UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,609,544 B2
APPLICATION NO. : 14/082040
DATED : March 28, 2017
INVENTOR(S) : Raleigh et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Add to the end of the first paragraph of item (60), page 2, Column 1:
, said application No. 12/695,019 is a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771, filed on Mar. 2, 2009, said application No. 12/695,020 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,445 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,451 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,455 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,021 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,980 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, said application No. 13/134,005, filed on May 25, 2011, is a continuation-in-part of application No. 12/380,759, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,779, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,758, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,768, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,767, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,780 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,755 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,756 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,770 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,772 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,782 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,783 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,757 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,781 filed on Mar. 2, 2009 and a continuation-in-part of application No. 12/380,774 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,773 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,769 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,777 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,020, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,445, filed on

Signed and Sealed this
Twenty-sixth Day of February, 2019

Andrei Iancu
Director of the United States Patent and Trademark Office

SAMSUNG 1002

Jan. 27, 2010, and a continuation-in-part of application No. 12/694,451, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,455, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,980, filed on Jan. 28, 2010.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh et al.	Patent No.: 9,609,544
Serial No.: 14/082,040	Issue Date: March 28, 2017
Filing Date: November 15, 2013	Conf. No.: 1015
Title: Device-Assisted Services for Protecting Network Capacity	

Commissioner for Patents
Office of Patent Publication
ATTN: Certificate of Correction Branch
P.O. Box 1450
Alexandria, VA 22313-1450

MISCELLANEOUS COMMUNICATION REGARDING CERTIFICATE OF CORRECTION

Applicant/Patentee (hereinafter, "Applicant") respectfully requests that the Office issue a Certificate of Correction for U.S. Patent No. 9,609,544 to correct the missing priority claims in "Related U.S. Application Data (60)" section of the patent. The errors being corrected are the Office's errors.

In the published patent, section (60) recites a priority claim that is incomplete. The complete priority claim is accurately reflected in the November 15, 2013 Application Data Sheet. The following information is missing and should be added to the end of the first paragraph of section (60), page 2, col. 1:

, said application No. 12/695,019 is a continuation-in-part of application No.12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No.12/380,771, filed on Mar. 2, 2009, said application No. 12/695,020 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,445 is a continuation-in-part of application No.

12/380,780, filed on Mar. 2, 2009, said application No. 12/694,451 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,455 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,021 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,980 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 2/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, said application No. 13/134,005, filed on May 25, 2011, is a continuation-in-part of application No. 12/380,759, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,779, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,758, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,768, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,767, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,780 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,755 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,756 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,770 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,772 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,782 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,783 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,757 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,781 filed on Mar. 2, 2009 and a continuation-in-part of application No. 12/380,774 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,773 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,769 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,777 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,020, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,445, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,451, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,455, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,980, filed on Jan. 28, 2010.

CONCLUSION

Applicant respectfully requests issuance of the Certificate of Correction to correct the errors in the priority claim. The Office is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: January 11, 2019 By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: January 11, 2019 By: /Jennifer Smith/
Jennifer Smith

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,609,544

APPLICATION NO.: 14/082,040

ISSUE DATE : March 28, 2017

INVENTOR(S) : Raleigh et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Add to the end of the first paragraph of section (60), page 2, col. 1:

, said application No. 12/695,019 is a continuation-in-part of application No.12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No.12/380,771, filed on Mar. 2, 2009, said application No. 12/695,020 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,445 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,451 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,455 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,021 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,980 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 2/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010,

[Continued on next page]

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,609,544

APPLICATION NO.: 14/082,040

ISSUE DATE : March 28, 2017

INVENTOR(S) : Raleigh et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

[Add to the end of the first paragraph of section (60), page 2, col. 1]:

said application No. 13/134,005, filed on May 25, 2011, is a continuation-in-part of application No. 12/380,759, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,779, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,758, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,768, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,767, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,780 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,755 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,756 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,770 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,772 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,782 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,783 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,757 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,781 filed on Mar. 2, 2009 and a continuation-in-part of application No. 12/380,774 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,773 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,769 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,777 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,020, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,445, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,451, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,455, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,980, filed on Jan. 28, 2010.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	34833138
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Jennifer Smith
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	11-JAN-2019
Filing Date:	15-NOV-2013
Time Stamp:	15:07:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	P032C1_ReqforCoC_RTF.pdf	426483 9cf033ca7d59ac8e55619da695361c82416ffd60	no	5

Warnings:

Information:	
Total Files Size (in bytes):	426483

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	03/28/2017	9609544	RALEP032C1	1015

106963 7590 03/08/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 338 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Headwater Partners I LLC, Redwood Shores, CA;
Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Change(s) applied to document, /D.D./ 2/22/2017

	229	7565141		2009-07-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 02/17/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
02/17/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com

Corrected Notice of Allowability	**Application No.** 14/082,040	**Applicant(s)** RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	**Art Unit** 3687	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the February 8, 2017 Information Disclosure Statements*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1,5,8-21 and 24-30*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE** "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Applicant cancelled claims 2-4, 6, 7, 22 and 23.

3. Applicant's January 31, 2014; May 22, 2014 and two February 8, 2017 Information Disclosure Statements (IDS's) have been reviewed. Note the attached IDS's.

Allowable Subject Matter

4. Claims 1, 5, 8-21 and 24-30 are allowed.

5. The following is an examiner's statement of reasons for allowance: Applicant's December 1, 2016 Amendment regarding claims 1, 5, 8-21 and 24-30 have been reviewed, along with the above aforementioned IDS's. Claims 1, 5, 8-21 and 24-30 are now allowed as all the cited prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Claims 1, 5, 8-21 and 24-30 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claims 1, 5, 8-21 and 24-30 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified abstract idea.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Fahd A. Obeid can be reached on 571-270-3324. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6115823	A	2000-09-05	Velasco et al.	
	2	9326173	B2	2016-04-26	Luft, Achim	
	3	7203721	B1	2007-04-10	Ben-Efraim et al.	
	4	7219123	B1	2007-05-15	Fiechter et al.	
	5	7505795	B1	2009-03-17	Lim et al.	
	6	7389412		2008-06-17	Sharma et al.	
	7	7466652		2008-12-16	Lau et al.	
	8	7512131		2009-03-31	Svensson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7526541		2009-04-28	Roese et al.	
	10	8539544		2013-09-17	Garimella et al.	
	11	9111088		2015-08-18	Ghai et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090065571	A1	2009-03-12	Jain, Deepak	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6879825	B1	2005-04-12	Daly, Brian Kevin	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050163320	A1	2005-07-28	Brown et al.	
	2	20060114821	A1	2006-06-01	Willey et al.	
	3	20070201502	A1	2007-08-30	Abramson, Nathan	
	4	20080168275	A1	2008-07-10	DeAtley et al.	
	5	20080178300	A1	2008-07-24	Brown et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	6	20090049156	A1	2009-02-19	Aronsson et al.	
	7	20090320110	A1	2009-12-24	NICOLSON et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1289326	EP	A1	2003-03-05	Motorola, Inc.		
	2	2006041989	JP		2006-02-09	Fujitsu Ltd.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	Raleigh, Gregory G.
Attorney Docket Number	RALEP032C1

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5774532	A	1998-06-30	Gottlieb et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040225898	A	2004-11-11	Frost, D. et al.	
	2	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	3	20060114832	A	2006-06-01	Hamilton et al.	
	4	20060156398	A	2006-07-13	Ross et al.	
	5	20060173959	A	2006-08-03	Mckelvie et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

	6	20070033194	A	2007-02-08	Srinivas et al.	
	7	20080070550	A	2008-03-20	Hose, David Alan	
	8	20080201266	A	2008-08-21	Chua et al.	
	9	20100284327	A	2010-11-11	Miklos, Gyorgy	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	2	7320029	B2	2008-01-15	Rinne et al.	
	3	7539132	B2	2009-05-26	Werner et al.	
	4	7805606	B2	2010-09-28	Birger et al.	
	5	8175574	B1	2012-05-08	Panda et al.	
	6	8180881	B2	2012-05-15	Seo et al.	
	7	8191124	B2	2012-05-29	Wynn et al.	
	8	8275415	B2	2012-09-25	Huslak, Nicholas S.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8300575	B2	2012-10-30	Willars, Per	
	10	8315593	B2	2012-11-20	Gallant et al.	
	11	8347378	B2	2013-01-01	Merkin et al.	
	12	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	13	8527410	B2	2013-09-03	Markki et al.	
	14	8539561	B2	2013-09-17	Gupta et al.	
	15	8554876	B2	2013-10-08	Winsor, Gerald W.	
	16	8666395	B2	2014-03-04	Silver, Andrew	
	17	8391834	B2	2013-03-05	Raleigh, Gregory G.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	1	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	2	20040170191	A	2004-09-02	Guo et al.	
	3	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	4	20050186948	A	2005-08-25	Gallagher et al.	
	5	20070147317	A	2007-06-28	Smith et al.	
	6	20080025230	A	2008-01-31	Patel et al.	
	7	20080056273	A	2008-03-06	Pelletier et al.	
	8	20080270212	A	2008-10-30	Blight et al.	
	9	20100030890	A	2010-02-04	Dutta et al.	
	10	20110110309	A	2011-05-12	Bennett, James D.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1310401	CN	A	2001-08-29	Wang, Di Xing		☐
	2	2466831	EP	A1	2012-06-20	Openet Telecom Ltd. - Mcnamee et al.		☐
	3	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
	4	1999027723	WO	A1	1999-06-03	Telefonaktiebolaget LM Ericsson		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 01/31/2017
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Ann Taylor	(Depositor's name)
	(Signature)
February 9, 2017	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

TITLE OF INVENTION: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/01/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	709-224000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 James E. Harris
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Headwater Research LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Tyler TX

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 505876 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date February 9, 2017
Typed or printed name James E. Harris Registration No. 40013

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal				
Application Number:	14082040			
Filing Date:	15-Nov-2013			
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY			
First Named Inventor/Applicant Name:	Gregory G. Raleigh			
Filer:	James E. Harris/Ann Taylor			
Attorney Docket Number:	RALEP032C1			
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt	
EFS ID:	28314187
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	09-FEB-2017
Filing Date:	15-NOV-2013
Time Stamp:	15:49:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	021017INTEFSW00002181505876
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P032C1_IssueFee.pdf	139849 b37dd6057c2b0c203de2a34530aadfbb1c6b9cf6	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30280 80bd9b96d9b3cf463a2cd714296c4c138b1424f4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	170129		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6115823	A	2000-09-05	Velasco et al.	
	2	9326173	B2	2016-04-26	Luft, Achim	
	3	7203721	B1	2007-04-10	Ben-Efraim et al.	
	4	7219123	B1	2007-05-15	Fiechter et al.	
	5	7505795	B1	2009-03-17	Lim et al.	
	6	7389412		2008-06-17	Sharma et al.	
	7	7466652		2008-12-16	Lau et al.	
	8	7512131		2009-03-31	Svensson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7526541		2009-04-28	Roese et al.	
	10	8539544		2013-09-17	Garimella et al.	
	11	9111088		2015-08-18	Ghai et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090065571	A1	2009-03-12	Jain, Deepak	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

If you wish to add additional non-patent literature document citation information please click the Add button	Add		
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-02-08
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6879825	B1	2005-04-12	Daly, Brian Kevin	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050163320	A1	2005-07-28	Brown et al.	
	2	20060114821	A1	2006-06-01	Willey et al.	
	3	20070201502	A1	2007-08-30	Abramson, Nathan	
	4	20080168275	A1	2008-07-10	DeAtley et al.	
	5	20080178300	A1	2008-07-24	Brown et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	6	20090049156	A1	2009-02-19	Aronsson et al.	
	7	20090320110	A1	2009-12-24	NICOLSON et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1289326	EP	A1	2003-03-05	Motorola, Inc.		
	2	2006041989	JP		2006-02-09	Fujitsu Ltd.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-02-08
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 2006041989
PUBLICATION DATE : 09-02-06

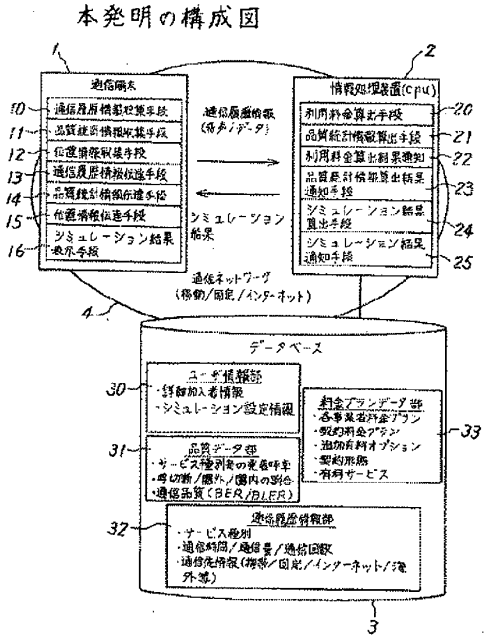
APPLICATION DATE : 28-07-04
APPLICATION NUMBER : 2004219784

APPLICANT : FUJITSU LTD;

INVENTOR : KATAOKA KOSUKE;

INT.CL. : H04M 15/16 (2006.01)

TITLE : CHARGING PLAN NOTIFICATION SYSTEM



ABSTRACT : PROBLEM TO BE SOLVED: To provide a charging plan notification system for calculating the lowest optimum charging plan corresponding to a utilization state of a communication terminal user from charging plans provided by all carriers.

SOLUTION: The charging plan notification system is provided with: a communication terminal for transmitting communication history information concerned with communication; a database 3 for storing the communication history information, all contract information between communication terminal users and communication carriers and all charging plans for communication service provided by all the carriers; and an information processor 2 for calculating utilization charges. The information processor 2 respectively calculates accurate utilization charges in the charging plans provided from respective carriers on the basis of the communication history information of each communication terminal user, the contract information and all the charging plans and notifies the communication terminal user of the calculated results.

COPYRIGHT: (C)2006,JPO&NCIPI

BNSDOCID: <JP_____2006041989A_AJ_>

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-41989
(P2006-41989A)
(43)公開日　平成18年2月9日(2006.2.9)

(51)Int.Cl.	F I	テーマコード（参考）
H04M 15/16 (2006.01)	H04M 15/16	5K025

審査請求 未請求　請求項の数 5　OL　（全 15 頁）

(21)出願番号　特願2004-219784 (P2004-219784)
(22)出願日　平成16年7月28日 (2004.7.28)

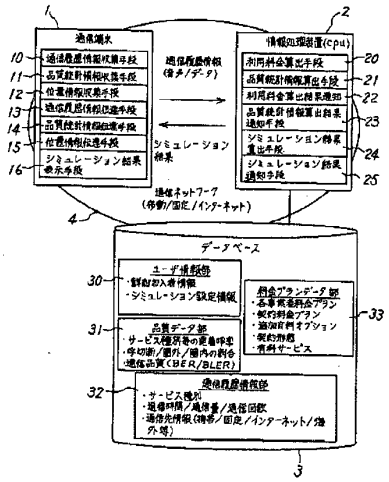
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100083297
弁理士　山谷　晧榮
(74)代理人　100087848
弁理士　小笠原　吉義
(72)発明者　友松　聖詞
東京都品川区南大井６丁目２２番７号　富士通ネットワークソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】料金プラン通知装置

(57)【要約】
【課題】全通信事業者の料金プランの中から通信端末ユーザの利用状態に応じた最も安い最適の料金プランを算出する料金プラン通知装置を提供すること。
【解決手段】このため本発明では、通信に関する通信履歴情報を送信する通信端末１と、通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベース３と、利用料金を算出する情報処理装置２を具備する料金プラン通知装置であって、通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置２により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知する。
【選択図】図１

本発明の構成図



BNSDOCID: <JP_____2006041989A__I_>

【特許請求の範囲】
【請求項1】
通信に関する通信履歴情報を送信する通信端末と、
通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベースと、
利用料金を算出する情報処理装置を具備する料金プラン通知装置であって、
通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知する料金プラン通知装置。
【請求項2】
前記通信端末は、全通信における発着呼率、通信途中での切断、待受け時における圏内・圏外の割合・データ伝送速度等、全ての品質情報を通信履歴情報、通信端末が取得できる位置情報とをデータベースに送信する伝達手段を持ち、
上記データベースは品質情報を蓄積する蓄積手段を持ち、
上記情報処理装置は、品質情報を基に各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出する算出手段を持ち、通信サービスの品質情報を全料金プランの正確な利用料金と共に通信端末ユーザに通知できる通知手段を具備したことを特徴とする請求項１記載の料金プラン通知装置。
【請求項3】
上記情報処理装置は、予めデータベースに登録されている、通信端末ユーザが通信事業者と契約している料金プラン、追加有料オプション、契約時期、契約形態、有料サービス、全通信事業者が提供している全料金プラン、及び有料オプション、割引情報等の情報を利用して正確な利用料金を算出することを特徴とする請求項１記載の料金プラン通知装置。
【請求項4】
上記情報処理装置は、サービス種別、通信時間、量、回数、通信先、位置情報等の詳細な通信履歴情報を利用して、正確な利用料金を算出することを特徴とする請求項１記載の料金プラン通知装置。
【請求項5】
通信端末ユーザが利用を想定した任意の利用条件をデータベースに設定し、ユーザの要求に応じて情報処理装置は、それらの情報と、データベースに登録してある通信端末ユーザの詳細加入者情報及び料金プランに関連する情報を利用して、各料金プランにおいてシミュレーションし、正確に料金算出し、結果を通信端末ユーザに通知することを特徴とする請求項１記載の料金プラン通知装置。

【発明の詳細な説明】
【技術分野】
【0001】
本発明は、通信端末の利用料金を算出し、通信端末ユーザに通知するサービスを行う料金プランを考慮した料金シミュレーションを実施し、最適な料金プランをユーザおよび事業者に通知する料金プラン通知システムに関する。
【背景技術】
【0002】
従来、携帯電話の如き通信端末では、基本使用料と一定金額の無料通話分の設定や、平日昼間や夜間、土日祝日等通話時間帯毎の通話料割引倍率、パケット料金の割引など様々な割引プランが設定されている。
【0003】
通信事業者は、これらの組み合せによりバリエーションを持たせた料金プランを準備している。
【0004】
ユーザは、あらかじめ１つの料金プランを選択し、そのプランに設定された割引率と実

BNSDOCID: <JP____2006041989A__I_>

際の月々の利用料金により算出された金額を契約した通信事業者からの請求により支払う。

【0005】

ユーザが自己の通信に対して最適な料金プランによる通信サービスを受けることができるように、ユーザに対して通話終了毎に、契約された契約料金プランと準備された全ての料金プランとを比較して、得られる最適な料金プランをリアルタイムで通知することが提案されている。

【特許文献1】特開２００１－３６６７３号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

上記従来技術では、ユーザが現在契約している通信事業者が提供しているサービスの中における最適な料金プランの提供であり、他社の通信事業者の提供しているものを含めた料金プランにおける最適なものの提供ではない。

【0007】

したがってユーザが、現在契約している料金システムが自己にとって最適なプランであるかどうかを判断するために、ユーザ自身が月々の利用状態を分析し、検討し、現在の契約通信事業者のみならず他の契約通信事業者の料金プランと比較することが必要である。

【0008】

しかるに各社の料金プランは多様・複雑化しており、ユーザ自らが分析・検討するのは困難である。したがって、各社の料金プランの中からユーザの通信端末の利用状態に応じた、最適の料金プランを提供するサービスが求められている。

【課題を解決するための手段】

【0009】

上記課題を解決するため、本発明では、下記（１）～（５）の料金プラン通知装置を提供する。

【0010】

（１）通信に関する通信履歴情報を送信する通信端末と、通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベースと、利用料金を算出する情報処理装置を具備する料金プラン通知装置であって、通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知することを特徴とする料金プラン通知装置。

【0011】

（２）上記（１）の料金プラン通知装置において、前記通信端末は、全通信における発着呼率、通信途中での切断、待受け時における圏内・圏外の割合・データ伝送速度等、全ての品質情報を通信履歴情報、通信端末が取得できる位置情報とをデータベースに送信する伝達手段を持ち、上記データベースは品質情報を蓄積する蓄積手段を持ち、上記情報処理装置は、品質情報を基に各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出する算出手段を持ち、通信サービスの品質情報を全料金プランの正確な利用料金と共に通信端末ユーザに通知できる通知手段を具備したことを特徴とする。

【0012】

（３）上記（１）の料金プラン通知装置において、上記情報処理装置は、予めデータベースに登録されている、通信端末ユーザが通信事業者と契約している料金プラン、追加有料オプション、契約時期、契約形態、有料サービス、全通信事業者が提供している全料金プラン、及び有料オプション、割引情報等の情報を利用して正確な利用料金を算出することを特徴とする。

【0013】

（４）上記（１）の料金プラン通知装置において、上記情報処理装置は、サービス種別

BNSDOCID: <JP_____2006041989A__I_>

、通信時間、量、回数、通信先、位置情報等の詳細な通信履歴情報を利用して、正確な利用料金を算出することを特徴とする。

【0014】

（５）上記（１）の料金プラン通知装置において、通信端末ユーザが利用を想定した任意の利用条件をデータベースに設定し、ユーザの要求に応じて情報処理装置は、それらの情報と、データベースに登録してある通信端末ユーザの詳細加入者情報及び料金プランに関連する情報を利用して、各料金プランにおいてシミュレーションし、正確に料金算出し、結果を通信端末ユーザに通知することを特徴とする。

【発明の効果】

【0015】

本発明により下記の効果を奏する。

【0016】

（１）通信端末が通信端末ユーザの詳細な通信履歴情報をサービス提供業者の料金プラン通知装置のデータベースに登録し、情報処理装置において、前記データベースに登録された詳細な通信履歴情報と料金プラン情報を使用して、ユーザが契約していない他の通信事業者のプランも含めて全料金プランについて正確な通信料金を算出し、通信端末ユーザに通知するので、通信端末ユーザは前記契約外の通信事業者のプランも含めた一番安い料金プランを正確に知ることができる。

【0017】

（２）通信端末に、通信履歴情報と共に通話品質に関連する情報をサービス提供業者の料金プラン通知装置のデータベースに送信し、情報処理装置に、データベースに登録されている通信品質に関連する情報を使用して各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出し、通信端末ユーザに通知するので、通信端末ユーザは契約していない通信事業者のつながり易さ、音声品質等の通信品質を含め、全通信事業者の通信品質情報を知る事が出来るので、通信端末ユーザは、一番通信品質の良い通信事業者を選択することができる。

【0018】

（３）通信端末ユーザは、料金プランや契約形態等の詳細な加入者情報、契約情報をサービス提供者の料金プラン通知装置のデータベースに登録し、それらを利用料金算出に使用することにより、利用形態に沿った正確な一番安い利用料金プランを算出することが可能となる。

【0019】

（４）現在の通信端末は音声通話終話単位で表示される通信履歴情報とパケット数情報を確認できるが、これらは各通信事業者の標準的なプランを基にした情報であり必ずしも正確な情報ではなかったが、本発明では通信端末ユーザからの実用的な詳細情報の収集は、通話時間、パケット数だけでなく、通信量、通話回数、接続通話先、データ量、利用回数等通信履歴情報の詳細を用いてデータベースに登録し、それらを利用料金算出に使用できるので、情報処理装置での正確な利用料金算出を可能とする。

【0020】

（５）通信端末ユーザが自分の利用形態を想定した条件をデータベースに登録し、データベースに登録した詳細な加入者情報、各種料金プランを利用することで大雑把な料金シミュレーションではなく、正確なシミュレーションの実現が可能となり、また前月の履歴情報を流用する手段を持たせることで、シミュレーションに必要な情報を前月と同じ状態で算出することができ、ユーザオペレーションを低減させた正確なシミュレーションの実現が可能となる。

【発明を実施するための最良の形態】

【0021】

自己の通信履歴情報を、サービス業者に送信する通信端末と、多数の通信事業者の料金プランと前記通信履歴情報を保持するデータベースと、前記通信履歴情報にもとづき前記多数の通信事業者の料金プランを使用して通信を行ったときの料金を算出する情報処理装

BNSDOCID: <JP_____2006041989A__I_>

置を設け、前記通信履歴情報にもとづき前記多数の通信事業者の料金プランを使用して通信を行ったときもっとも安いものを前記情報処理装置で算出して、このうちのもっとも安い料金システムを通信端末ユーザに通知する料金プラン通知装置を提供する。これにより、通信端末ユーザは、このサービス業者からの通知により、自己が契約している通信事業者以外の他の通信事業者を含めた全通信事業者の料金プランのうちより、自己に適したもっとも安い料金プランを認識することができる。

【実施例】

【0022】

本発明の実施例１を図１～図３にもとづき説明する。図１は本発明の構成図、図２は本発明の品質統計情報説明図、図３は時間毎の品質統計情報説明図である。

【0023】

図中、１は通信端末、２は情報処理装置、３はデータベース、４は通信ネットワーク、１０は通信履歴情報収集手段、１１は品質統計情報収集手段、１２は位置情報収集手段、１３は通信履歴情報伝達手段、１４は品質統計情報伝達手段、１５は位置情報伝達手段、１６はシミュレーション結果表示手段、２０は利用料金算出手段、２１は品質統計情報算出手段、２２は利用料金算出結果通知手段、２３は品質統計情報算出結果通知手段、２４はシミュレーション結果算出手段、２５はシミュレーション結果通知手段、３０はユーザ情報部、３１は品質データ部、３２は通信履歴情報部、３３は料金プランデータ部である。

【0024】

通信端末１は、ユーザが通信相手と音声やデータを送受信するものであり、例えば携帯端末である。

【0025】

情報処理装置２は、通信端末１から送信された通信履歴情報と、データベース３に保持された多くの通信事業者Ａ、Ｂ、Ｃ・・・の料金プランデータに基づいてシミュレーション演算を行い、そのうちもっとも安いものを送出するものであり、ＣＰＵで構成される。

【0026】

データベース３は通信端末１から送信された通信履歴情報や、多くの通信事業者Ａ、Ｂ、Ｃ、Ｄの料金プランデータが保持されており、外部メモリで構成されている。そしてデータベース３と情報処理装置２はサービス提供業者側の料金プラン通知装置に設置されている。

【0027】

通信ネットワーク４は、移動端末用ネットワーク、固定端末用ネットワーク、インターネットの如き、通信ネットワークである。

【0028】

通信端末１には、通信履歴情報収集手段１０、品質統計情報収集手段１１、位置情報収集手段１２、通信履歴情報伝達手段１３、品質統計情報伝達手段１４、位置情報伝達手段１５、シミュレーション結果表示手段１６等を有する。

【0029】

通信履歴情報収集手段１０は、通信端末１が通信相手に送信した送信データの種別データ量、送信時刻、送信時間、サービス種別等の履歴情報を一定期間保持するものである。

【0030】

品質統計情報収集手段１１は、通信相手から受信したデータの品質を通信相手が使用している通信事業者Ａ、Ｂ、Ｃ・・・毎に、例えば公知の５段階評価し、これを保持するものである。

【0031】

品質情報は、例えば前記受信データの５段階評価の外に、発着呼率、通信途中での切断、圏内・圏外の割合、通信品質（ビットエラーレートＢＥＲ、ブロックエラーレートＢＬＥＲ）、データ伝送レート等である。

【0032】

品質情報の例を図２、図３に示す。図２、図３は、通信事業者Ａ、Ｂ、Ｃ、Ｄの４者における品質統計情報を示すもので、図２（Ａ）は各通信事業者の平均の呼接続率、圏内の割合を示し、図２（Ｂ）は各通信事業者の平均の通信品質を示し、図２（Ｃ）は各通信事業者の平均データ伝送レートを示し、図３は各通信事業者の時間毎の呼接続率、圏内の割合を示す図である。

【0033】

なお図２（Ａ）における呼接続率（平均）Ｍ１と圏内の割合（平均）Ｍ２は下式により算出されるものである。

【0034】

Ｍ１＝（完了呼－不完了呼）／発呼

Ｍ２＝（圏内の時間－圏外の時間）／電源を入れていた時間

図２、図３のデータは、サービス業者に加入している通信事業者Ａ、Ｂ、Ｃ、Ｄを利用しているユーザの通信端末より送信されたデータにもとづく統計情報である。

【0035】

図２（Ａ）に示す如く、呼接続率は通信事業者Ａが約９０％、通信事業者Ｂが約９５％、通信事業者Ｃが約８０％、通信事業者Ｄが約９８％であることを示す。またノイズの少ない安定した状態で通信可能であることを示す圏内の割合は通信事業者Ａが約９５％、通信事業者Ｂが約７６％、通信事業者Ｃが約８５％、通信事業者Ｄが約９７％であることを示す。

【0036】

通信品質は、５段階評価で通信事業者Ａ、Ｂ、Ｄが５、通信事業者Ｃが４であることを示し、平均データ伝送レートは通信事業者Ａが約２５ｋｂｐｓ、通信事業者Ｂが約１７ｋｂｐｓ、通信事業者Ｃが約２３ｋｂｐｓ、通信事業者Ｄが約２４ｋｂｐｓであることを示す。

【0037】

品質情報には通信端末ユーザの住所が記入されているので、サービス装置側では各通信事業者についてこれらの住所を解析することにより例えば通信事業者Ｃが横浜駅周辺では通信品質があまりよくない等の品質統計情報を得ることができ、このような情報をユーザに提供することもできる。

【0038】

位置情報収集手段１２はサービス業者を利用している通信端末ユーザと通信先の通信端末ユーザの位置情報（住所）を収集し、これを保持するものである。

【0039】

通信履歴情報伝達手段１３は、通信履歴情報収集手段１０が収集した通信端末１が行った通信データを、通信ネットワーク４を経由してサービス業者側の情報処理装置２に送出するものである。

【0040】

品質統計情報伝達手段１４は、品質統計情報収集手段１１が収集したデータの品質情報をサービス業者側の情報処理装置２に通信ネットワーク４を経由して送出するものである。

【0041】

位置情報伝達手段１５は、位置情報収集手段１２で収集した、通信端末１と通信した相手端末のユーザの位置情報（住所）を通信ネットワーク４を経由してサービス業者側の情報処理装置２に送出するものである。

【0042】

シミュレーション結果表示手段１６は、情報処理装置２が算出したシミュレーション結果が通信ネットワーク４を経由して通信端末１に伝達されたとき、これを通信端末ユーザに表示する表示手段である。

【0043】

情報処理装置２は、通信端末から送信された通信履歴情報とデータベース４に蓄積され

BNSDOCID: <JP____2006041989A__I_>

ている全通信事業者の料金プランを使用して、全通信事業者の各料金プランについて正確な通信料金を算出し、通信端末の要求に応じて算出した通信料金を通信端末に通知したり、通信端末から受信した通信品質情報をデータベースに送信したり、データベースに登録してある通信品質情報を使用し、地域、時間帯通信事業者毎に品質統計情報を算出し通信端末の要求に応じて品質統計情報を通信端末に通知するものである。

【0044】

このため、情報処理装置２には、利用料金算出手段２０、品質統計情報算出手段２１、利用料金算出結果通知手段２２、品質統計情報算出結果通知手段２３、シミュレーション結果算出手段２４、シミュレーション結果通知手段２５等を有する。

【0045】

利用料金算出手段２０は、通信端末１から伝達された音声、データ等の通信履歴情報や、データベース部３に保持された各通信事業者の料金プランを使用して通信端末１のユーザに対する利用料金を算出するものである。

【0046】

品質統計情報算出手段２１は、通信端末１から受信されデータベース３に登録した通信品質情報を使用し、地域、時間帯、通信事業者毎における発着呼率、通信品質情報等を算出し、通信端末１の要求に応じて品質統計情報を通信端末１に通知するものである。

【0047】

利用料金算出結果通知手段２２は、利用料金算出手段２０で算出された全通信事業者の料金プランにもとづく通信料金のうち、もっとも安い料金を通信端末１に通知するものである。

【0048】

シミュレーション結果算出手段２４は、通信端末１のユーザが指定した任意の利用条件にもとづき、各通信事業者の料金プランを使用してもっとも安い利用料金を算出するものである。

【0049】

シミュレーション結果通知手段２５は、このシミュレーション結果算出手段２４から通知されたシミュレーション結果を、シミュレーション要求を行った通信端末に対し通知するものである。

【0050】

データベース３は、通信事業者に対する通信端末の加入者の詳細な契約情報、全通信事業者が提供する各種料金プラン、追加有料オプション情報、割引情報等の全ての課金に関する情報、及び本発明のサービスを制御するための、通信料金の通知回数や通知するタイミング等の設定情報、通信端末が送信した通信履歴情報を蓄積するもので、ユーザ情報部３０、品質データ部３１、通信履歴情報部３２、料金プランデータ部３３等を有し、前記情報処理装置２とともにサービス業者の料金プラン通知装置を構成する。

【0051】

ユーザ情報部３０は、通信端末１の加入者が現在契約している通信業者との詳細な契約情報である詳細加入者情報や、この加入者が料金のシミュレーション演算を求めるシミュレーション設定情報を保持するものである。

【0052】

品質データ部３１は、通信端末より送出されるサービス種別毎の発着呼率、呼切断の割合、圏内と圏外の割合、ビットエラーレート（ＢＥＲ）、ブロックエラーレート（ＢＬＥＲ）等の通信品質を保持するものである。

【0053】

通信履歴情報部３２は、通信端末より伝達された、通信端末が実際に通信を行った結果の情報を保持するもので、サービス種別、通信時間、通信量、通信回数、通信先が携帯端末か、固定端末か、インターネットか、海外か等を示す通信先情報を保持するものである。

【0054】

BNSDOCID: <JP____2006041989A__I_>

料金プランデータ部３３は、通信端末が加入しているか否かにかかわらず、全通信事業者の提供する各事業者料金プラン、契約料金プラン、追加有料オプション、契約形態、有料サービス等の課金に関する料金データを保持するものである。これらの料金データは、通信事業者がインターネットで公開したり、通信端末販売業者に郵送したりしているので、容易に入手できるものである。

【0055】

実施例１において、通信端末１は、通信履歴情報収集手段１０が収集したこの通信端末１が実際に通信した通信履歴情報を、通信履歴情報伝達手段１３が電子情報に変換し、移動通信網、固定通信網、インターネットの如き通信ネットワーク４を経由して、サービス業者の料金プラン通知装置を構成する情報処理装置２に送信する。

【0056】

情報処理装置２では、これを受信し、データベース３の通信履歴情報部３２に通信端末毎に、サービス種別、通信時間、通信量、通信回数、通信先情報等に識別して保持する。

【0057】

なお、サービス業者の料金プラン通知装置のデータベース３には、通信端末の加入者の料金プラン、オプション、契約期間等の詳細加入者情報やシミュレーション設定情報がそのユーザ情報部３０に保持され、また各通信事業者の料金プラン、契約料金プラン、追加有料オプション、契約形態、有料サービス等が料金プランデータ部３３に保持されている。

【0058】

したがって、通信端末の加入者が、例えば過去１ヶ月の通信履歴情報にもとづき、全通信事業者の料金プランにしたがって料金算出を求めたとき、情報処理装置２では、利用料金算出手段２０がデータベース３よりこの加入者の通信端末が過去１カ月に実際に通信を行った履歴情報にもとづき、料金プランデータ部３３に保持されている全通信事業者の各料金プランにより料金を算出し、これを利用料金算出結果通知手段２２に伝達する。

【0059】

利用料金算出結果通知手段２２では、この伝達された料金のうちもっとも安いものを選択してこれを通信端末１に送信する。

【0060】

通信端末１ではこれをシミュレーション結果表示手段１６が受信して表示出力し、加入者はこれにより、どの通信事業者の料金プランが自己の過去１ヶ月の通信履歴に対しもっとも安かったか認識し、現在の契約が適切か否かの判定が可能となる。勿論履歴情報は過去１ヶ月ではなく、１週間とか、適宜選択できる。

【0061】

実施例２においては、通信品質情報を算出通知するものである。通信端末１では通信毎の通信品質情報、例えば発着呼率、通信品質、通信時間、位置情報等を品質統計情報収集手段１１が算出し、これを収集する。

【0062】

品質統計情報伝達手段１４はこれらの情報を電子情報に変換し、任意のタイミングで移動通信網、固定通信網、インターネットの如き通信ネットワーク４を経由して、情報処理装置２に送信する。

【0063】

情報処理装置２は、通信端末１から受信した受信品質情報をデータベース３の品質データ部３１に送信し、通信品質情報を蓄積する。

【0064】

そして情報処理装置２は、通信端末１のユーザの要求に応じて、データベース３に登録してある通信品質情報を使用し、その品質統計情報算出手段２１が、地域毎、時間帯毎、通信事業者毎に、各時間帯毎、地域毎、事業者毎における発着呼率、呼切断、圏外・圏内の割合、ＢＥＲ、ＢＬＥＲ等の通信品質情報等を算出し、通信端末１のユーザの要求に応じて品質統計情報算出結果通知手段２３がこの品質統計情報を通信端末１に通知する。通

BNSDOCID: <JP____2006041989A_I_>

信端末１はこれをシミュレーション結果表示手段１６で受信してユーザに表示する。通信端末１のユーザは例えば図２、図３に示す如き、各通信事業者のサービス品質情報を取得することにより、通信サービスの品質を比較することができる。

【0065】

実施例３においては、有料オプション、契約期間等の詳細な加入者情報と、全通信事業者の提供する全料金プラン、追加オプション、割引制度情報から料金を比較算出するようにしたものである。

【0066】

データベース３のユーザ情報部３０には、情報処理装置２が通信端末ユーザの利用料金を算出する際に使用する、データベースに登録されている詳細な加入者情報が保持されている。

【0067】

この詳細な加入者情報としては、通信端末ユーザが通信事業者と契約している料金プラン情報すなわち、月額基本料金、無料通話時間、音声・データ・メール（Ｅメール、通信事業者網内向けメール、送受信料）等のサービス種別の通信料、自他国内キャリア、海外キャリア、国内・海外の固定電話、通信電話等の通信先毎の通信料、有料オプション、割引情報、契約期間、個人契約、法人契約（複数回線割引）等の契約形態等が登録されている。

【0068】

有料オプションの代表的なものとしては、通信事業者が提供する、留守番電話サービス、三者通話、海外ローミングサービス、国際通話等、その他ニュース、天気情報等の料金や条件等の詳細情報が登録される。

【0069】

割引情報の代表的なものとしては、家族割引、指定番号割引等の特定番号割引、時間帯割引、年齢・学生割引、長期契約割引、パケット割引の如きサービス種別毎の割引等の詳細情報が登録される。

【0070】

また、データベースの料金プランデータ部３３には、全通信事業者が提供している全料金プラン及び有料オプション、割引情報等の課金対象サービスの全ての詳細情報、条件が登録されており、これらの情報により情報処理装置２の利用料金算出手段２０が、例えば履歴情報に対して正確な利用料金を算出し、通信端末ユーザの契約料金と比較検討することができる。

【0071】

実施例４においては、通信履歴情報の詳細を示す。

【0072】

通信端末１がデータベース３に送信する通信履歴情報には、下記のような通信料金を算出するために必要な詳細情報が含まれている。

【0073】

音声、伝送速度・ＷＥＢアクセス・メール等のデータ、動画等のサービス種別。

【0074】

通信時間、パケット数等の量、回数。

【0075】

通信電話又は固定電話・フリーダイヤル・特定番号・ＵＲＬ・Ｅメール・国内又は海外等の通信先。

【0076】

緯経度等の位置情報。

【0077】

通信端末１は、これらの情報を電子情報に変換し、データベース３に送信する。情報処理装置２ではこれらの情報を利用料金の算出に使用する。

【0078】

BNSDOCID: <JP____2006041989A__I_>

実施例５においては、ユーザの任意の設定により、各料金プランにおいて使用料金をシミュレーション可能とするものである。

【0079】

このために、通信端末にユーザが例えば後述するサービス提供者のホームページより利用方法を想定したシミュレーション条件例えば音声通話時間、メール送受信回数、Ｗｅｂアクセス頻度、データ転送頻度、シミュレーション結果通知項目等を情報処理装置２に送信し、データベース３のユーザ情報部３０にこれらシミュレーション設定情報を登録する。

【0080】

情報処理装置２では、シミュレーション結果算出手段２４がこのシミュレーション条件と、データベース３の料金プランデータ部３３に登録ずみの全通信事業者の料金プランを利用してシミュレーション結果を算出し、シミュレーション結果通知手段２５がそのうちのもっとも安いものを通信端末１に送信し、シミュレーション結果表示手段１６がこれを表示してユーザにシミュレーション結果を知らせることができる。

【0081】

シミュレーション条件としてユーザの設定によるもののみでなく、例えばデータベースに蓄積されている前月の使用明細などの以前の通信履歴情報やデータベース３のユーザ情報部３０に予め用意してある代表的なシミュレーション条件を利用して設定することもできる。

【0082】

以前の通信履歴情報を利用する場合、本発明の料金プラン通知装置を設置するサービス提供者が作成したホームページの入力フォームにこの通信履歴情報を読み込ませるようにしてもよく、定形のファイルに以前の通信履歴情報を入力して通信端末等に送信し、通信端末は以前の通信履歴情報が記載された定形のファイルを編集し、データベースに送信することによっても実現できる。

【0083】

本発明では、通信端末ユーザは任意の利用条件を指定し、各料金プランにおいて通信料金をシミュレーションすることができる。

【0084】

通信端末は、ホームページの利用など公知の手段を使用して任意の利用条件をデータベースに設定する。任意の利用条件は、データベースに蓄積されている以前の通信履歴情報を流用することも可能である。

【0085】

データベースは通信端末から送信されてくる通信履歴情報を蓄積する。

【0086】

情報処理装置は、通信端末ユーザが指定した任意の利用条件、又はデータベースに蓄積されている以前の通信履歴情報、料金プラン、契約情報、割引情報を使用し、通信料金をシミュレーションし、通信端末ユーザに通知することができる。

【0087】

このシミュレーションとは、過去何時間とか特定の日等任意の期間の利用条件を元に、１ヶ月、１年分等の利用料金を全料金プランにおいて試算できる。これにより通信端末ユーザは種々の利用形態における利用料金を知ることができる。

【0088】

本発明では、通信端末ユーザは、情報処理装置で算出した、各料金プランの正確な使用料金、シミュレーション結果、及びサービス種別、通信先、通信時間、回数、情報量等の個別通信毎の料金内訳、品質統計情報等を下記に示す手段で入手することができる。

（１）電子データ：情報処理装置は通信端末ユーザの要求に応じて前記算出情報を、データベースから収集し、データファイル（テキスト、ＨＴＭＬ形式等）に変換して、Ｅメール、データファイルを通信端末ユーザのＥメールアドレスに送信する。また情報処理装置が前記算出情報をホームページに変換し、通信端末ユーザにホームページのアドレスを送

BNSDOCID: <JP____2006041989A__I_>

信し、通信端末ユーザはそのホームページのアドレスにアクセスして閲覧することにより前記情報を見ることができる。また情報処理装置が前記算出情報をデータファイルに変換して通信端末ユーザに送信し、通信端末ユーザはそのデータファイルを閲覧することにより前記算出情報を見ることができる。

【0089】

（２）前記以外の手段：情報処理装置は通信端末ユーザの要求に応じて、前記算出情報をデータベースから収集し、音声ガイダンスに変換することで通信端末ユーザに聞かせることができる。またその他に、明細書を作成して郵送したり、オペレータによる対応等により通信端末ユーザは前記算出情報を入手することができる。

【0090】

本発明では、通信端末ユーザは、情報処理装置が行う全ての処理、情報を伝送するタイミングを任意に設定することができる。これにより、通信料が安い時間帯での送信や、日、週、月、年単位等のある期間の通信履歴情報を送信するタイミング、自動又は手動、月に何回等の回数を設定することができる。これにより通信端末は、任意のタイミングで通信履歴情報をデータベースに送信することができる。

【0091】

また通信端末は、利用料金をシミュレーションさせるタイミング、シミュレーション結果を通知するタイミング等の各種タイミングをデータベースに登録することができる。

【0092】

情報処理装置は、前記タイミングで利用料金算出、シミュレーションを行い、通信端末ユーザに利用料金や、シミュレーション結果を通知する。

【0093】

本発明では、通信履歴情報や品質情報及び情報処理装置が送信するデータに優先度をつけることができ、これによりトラフィックを制御することができる。

【0094】

通信端末や情報処理装置では、公知の手段によりそれぞれが送信すべきデータの形式を変換して送信することができる。通信事業者は一般的に許容される伝送遅延を、映像＞音声＞パケットデータ（ＷＥＢアクセス、ファイル転送、Ｅメール等）の順に設定していることが多いので、通信履歴情報や品質情報、使用料金シミュレーション等の通信端末と情報処理装置で送受信する全ての情報を映像のフォーマットに変換して送れば、遅延時間は最小で送信できるが、その分トラフィックを圧迫することになる。反対にパケットデータに変換して送れば、遅延時間は多くなるが、その分トラフィックの隙間を利用して送信できるので、通信ネットワークのトラフィックに負担をあまりかけないようにできる。

【0095】

本発明では、使用料金算出、シミュレーションや品質情報を提供するのに通信費がかかるので、通信端末ユーザは、使用料金算出やシミュレーションに関連する情報を使用料金算出、シミュレーションする際に料金に含むか、含まないかをデータベースに設定することができる。もし「含まない」を選択した場合、情報処理装置は、純粋な通信にかかった使用料金を算出し、通信端末ユーザに送信する。このように通信端末ユーザは、純粋に通信にかかった料金のみを知ることができる。

【0096】

本発明では、通信端末ユーザは、情報処理装置で算出する通信先、通信時間、回数、情報量等の詳細な通信履歴毎の料金、事業者内・事業者間、比較プラン数、通知プラン数等のシミュレーション結果、料金プラン、通信履歴情報、割引情報等のシミュレーション条件の内容を、ユーザが任意に設定できる。

【0097】

これにより使用料金算出、シミュレーションにかかる通信費や情報処理装置がシミュレーションに要する時間を調整できる。

【0098】

通信端末ユーザは、使用料金算出、シミュレーション結果、シミュレーション条件の項

目のうち、任意の項目をデータベースに設定できる。これにより通信端末ユーザはどこまで正確に使用料金を算出するか設定することができる。当然、条件が多ければ通信履歴情報やシミュレーション結果等のデータ量は多くなり、その分通信費、情報処理装置が処理に要する時間は多くなる。

【0099】

情報処理装置は通信端末ユーザがデータベースに設定された条件を使用して使用料金算出、シミュレーションを行い通信端末ユーザに結果を送信する。

【0100】

本発明では、個人情報の秘密を保護するため、通信端末ユーザが送信する通信履歴情報及び情報処理装置において算出する使用料金算出、シミュレーション結果、品質情報等全てを暗号化して送信することができる。例えば通知端末では公知の暗号化機能を有するソフトを使用することができ、また情報処理装置は自身で暗号化機能を持つ。

【0101】

暗号化・復号化手段には一般に使用されている公開鍵暗号方式、秘密暗号方式等の暗号化手段や、ＩＤ、パスワード、電子署名等の認証機能手段が考えられる。

【0102】

暗号化手段を使用する場合は、通信端末のアプリケーションソフトと情報処理装置で同じ暗号化・復号化手段を持つ。また認証機能を使用する場合は、通信端末ユーザはデータベースにＩＤ、パスワード、電子署名等を登録しておき、情報処理装置はそれらの認証情報が一致していることが確認できたら通信端末ユーザからの情報を受信する。

【0103】

また通信端末ユーザは、情報処理装置から送信される認証情報と、予め情報処理装置から入手しておいた認証情報が一致していることが確認できたら、情報処理装置からの情報を受信する。

【0104】

本発明では、通信端末ユーザが設定する任意の使用料金設定を超えた、又は下回っている時に、通信端末ユーザにその旨を通知する機能を持つ。

【0105】

通信端末ユーザは、任意の使用料金と、その設定した使用料金を超えた、又は下回っている時に通知するようデータベースに設定する。情報処理装置はそれらの設定を認識し、通信端末ユーザから送信されてくる通信履歴情報から使用料金を算出し、データベースに設定されている使用料金を超えた、又は下回っている時に、通信端末ユーザに設定金額をいくら上回った、または下回っているかを通知する。

【0106】

本発明では、通信端末ユーザが契約している料金プランにおいて、無料通信料金が設定されている場合、通信端末ユーザに無料通信料金の残高、残り時間、残りパケットを通知する機能を持つ。

【0107】

通信端末ユーザは、データベースに無料通信料金の残高、残り時間、残りパケット数を通知させる時間、ベアラ毎の残高、残り時間、残りパケット数の割合等の内容を設定する。

【0108】

情報処理装置はそれらの設定を認識し、通信端末ユーザから送信されてくる通信履歴情報から使用料金を算出し、通信端末ユーザに、残高、残り時間、残りパケット数を通知する。

【0109】

通信端末ユーザは本発明が提供する、使用料金算出、シミュレーション、品質情報のうち、任意のサービスを選択することができる。

【0110】

通信端末ユーザは、シミュレーション内容、無料通信料金の算出、比較プラン数等デー

BNSDOCID: <JP____2006041989A__I_>

タベースに希望するサービスの種類、シミュレーション回数、品質情報等を受け取る回数、タイミングを設定する。

【0111】

情報処理装置はそれらの設定を認識し、通信端末ユーザから送信してくる通信履歴情報から使用料金、品質情報を算出し、通信端末ユーザの設定した日時に通信端末ユーザが要求した情報を送信する。

【0112】

本発明では、通信端末ユーザの加入者情報は公知のアプリケーションソフトやサービス提供者が作成するホームページを利用することでデータベースに登録、修正することができる。

【0113】

通信端末ユーザは、アプリケーションソフトを使用する場合は、アプリケーションソフトが提供するフォーマットに設定項目を入力し、データベースに送信する。ホームページを使用する場合は、通信端末ユーザが本サービス提供者が提供する加入者情報のホームページにアクセスし、必要事項を記入することで、データベースに通信端末ユーザの加入者情報を登録することができる。修正も同様の手段で可能である。

【0114】

本発明を使用すれば、通信端末ユーザは料金とサービス品質の両面から最適な料金プラン、通信事業者を選択することができる。また通信事業者は各ユーザの使用状況を詳細に把握することができ、適切な料金プランを検討する際に有効なデータや、サービスエリア拡充時に参考になる情報を得ることができる。

【図面の簡単な説明】

【0115】

【図1】本発明の一実施例構成図である。

【図2】本発明の品質統計情報説明図である。

【図3】本発明の時間毎の品質統計情報説明図である。

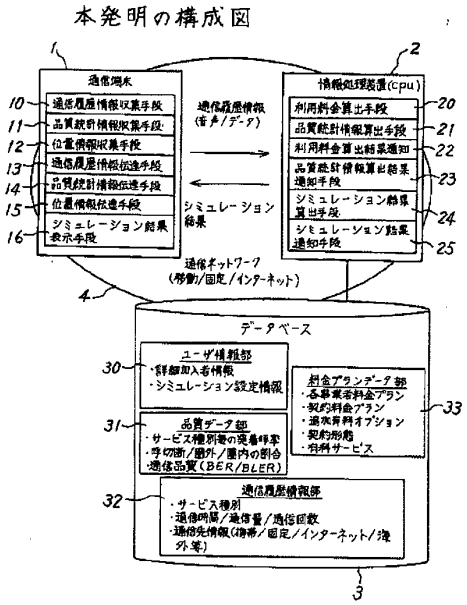
【符号の説明】

【0116】

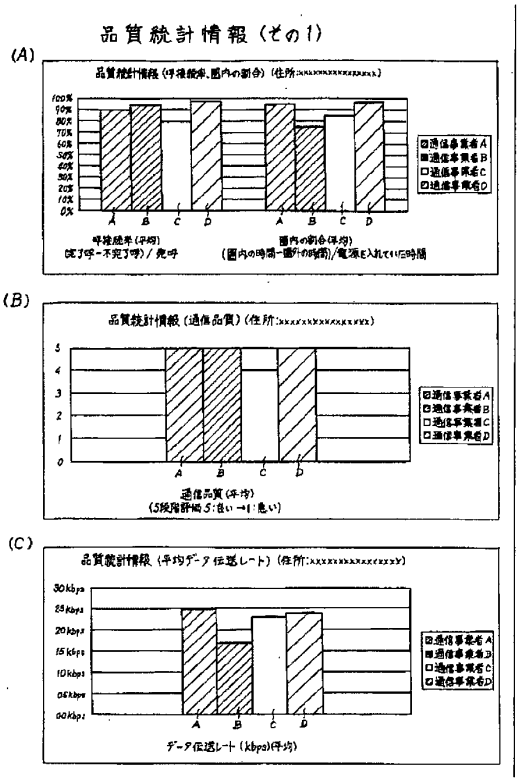
1　通信端末
2　情報処理装置
3　データベース
4　通信ネットワーク

BNSDOCID: <JP_____2006041989A__I_>

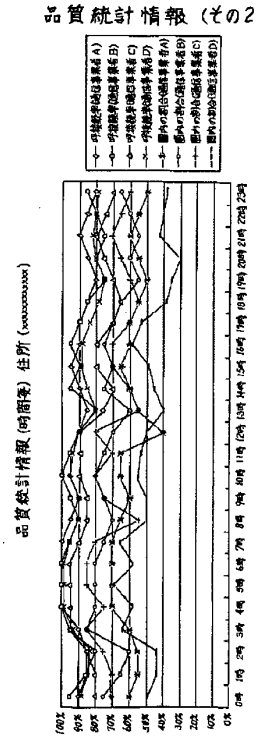
【図1】



【図2】



【図3】



BNSDOCID: <JP_____2006041989A__I_>

(72)発明者　片岡　康祐
東京都品川区南大井６丁目２２番７号　富士通ネットワークソリューションズ株式会社内

Ｆターム(参考) 5K025 AA08　BB06　CC01　JJ02　JJ16　JJ18

BNSDOCID: <JP_____2006041989A__I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 289 326 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.03.2003 Bulletin 2003/10

(51) Int Cl.7: **H04Q 7/32**

(21) Application number: **01402259.4**

(22) Date of filing: **30.08.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Deloume, Pascal**
  31170 Tournefeuille (FR)
- **Garani, Pradeep**
  31000 Toulouse (FR)

(74) Representative: **Litchfield, Laura Marie et al**
Motorola European Intellectual Property Operations,
Midpoint - Alencon Link
Basingstoke, Hampshire RG21 7PL (GB)

(54) Method of verifying downloaded software and corresponding device

(57) The present invention relates to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software. Thus the security of the keys and calculations involving the secure keys are kept secure. Preferably root security keys stored in the smart card can be updated using communication system messaging protocols.

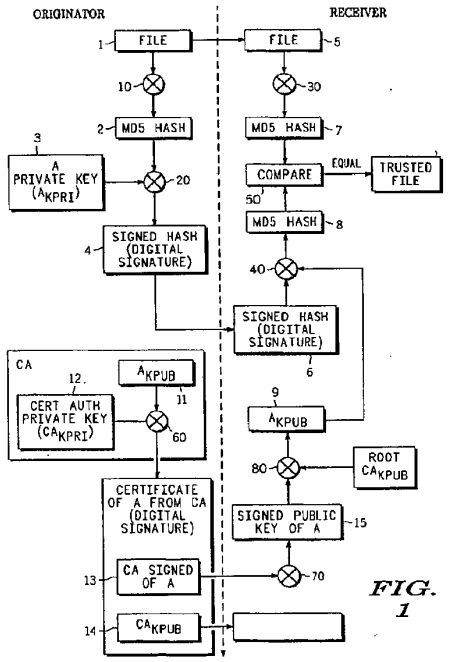


FIG. 1

EP 1 289 326 A1

Printed by Jouve, 75001 PARIS (FR)

BNSDOCID: <EP_____1289326A1_I_>

Description

[0001] The present invention relates to a method of verifying software downloaded from an originator to a device, and to a corresponding device. In particular, the invention relates to download verification in standardised execution environments such as the Mobile Execution Environment (MExE) and Java.

[0002] Increasingly it is becoming desirable for software to be downloaded to a portable device over the air. This allows the device to be upgraded with newly released software or enables new applications to be added to the device as these become available.

[0003] It is desirable that the device checks the authenticity of the downloaded software to determine whether, for example, the downloaded software has indeed been received from a trusted sender. In addition, it is desirable that the downloaded software should be restricted to a given domain, to avoid permission violation for the rest of the device.

[0004] This security can be ensured by keys, which are stored securely in the device such that they cannot be read or tampered with by applications except the security-checking environment. In addition it is desirable to update the keys periodically, and this must be done using a secure method.

[0005] Previously, it has been suggested to implement the security algorithms in software/hardware and then to protect them by hardware control on the processor of the terminal with memory management unit. However, this results in increased cost. In addition, the development of separate security hardware is undesirable.

[0006] The Mobile Execution Environment (MExE), which enables software download, is currently under standardisation. Three class marks are defined in the MexE environment. Class mark 1 relates to devices utilizing the Wireless Application Protocol (WAP); class mark 2 relates to devices, such as personal digital assistants (pda) or laptops using standard edition JAVA™ (J2SE); and class mark 3 relates to small devices, such as mobile telephones, using micro-edition JAVA™ (J2ME).

[0007] J2ME is being proposed as an environment for class mark 3 devices in MExE because of its small size, which makes it suitable for environments, such as the mobile communication environment for example, in which the available memory or processing power is limited and the size of files must be limited.

[0008] However, the security model for J2ME requires server-based pre-verification, in which a server inserts basic run-time security information in the software prior to download. The receiving device can then use the run-time security information to check the security of the download and verify the sender.

[0009] It is desirable to increase the security provided for software download, particularly in a MExE class mark 3 environment, so that server-based verification is avoided and software can be downloaded from a greater variety of sources.

[0010] According to a first aspect of the present invention, there is provided a method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising: receiving software and security information relating to the received software; obtaining in the smart card a first calculation result from the security information using at least one secure key; obtaining in the device a second calculation result from calculations performed on the received software; and comparing in the device first and second calculation results to verify the received software.

[0011] According to a second aspect of the invention, there is provided a device comprising: communication means for receiving software and security information relating to the received software; smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key; means for obtaining a second calculation result from calculations performed on the received software; means for comparing first and second calculation results to verify the received software.

[0012] For a better understanding of the present invention, and to show how it may be brought into effect reference will now be made, by way of example to the accompanying drawings in which:

Figure 1 illustrates a known file transfer verification procedure;
Figure 2 shows a communication device;
Figure 3 illustrates a download verification procedure in accordance with the invention;
Figure 4 illustrates message creation for transfer of the root key in accordance with the invention;
Figure 5 illustrates update of the root key in accordance with the invention

[0013] The present invention is described with reference to the use of RSA cryptography. The RSA cryptography algorithm and principle are well known and therefore will not be explained in detail in this document. As will be apparent to a skilled person, other cryptography techniques may also be used in accordance with the invention.

[0014] Figure 1 illustrates a known file transfer verification procedure, for verifying the authenticity of a file transferred from an originator to a receiver. The principle behind this procedure is that in addition to the transfer of the file 1 a second piece of information which is related to both the file 1 and the originator is also transferred between the originator and the receiver, which information enables the receiver to confirm that the file comes from the originator. In addition, the receiver possesses or is passed a third piece of information, which enables

BNSDOCID: <EP_____1289326A1_I_>

the receiver to confirm that the originator can be trusted and that it is therefore safe to execute the downloaded file.

[0015] In the illustrated procedure the originator generates the second piece of information by performing an MD5 hash operation 10 on the file 1 to be transferred to create an MD5 hash result 2. The MD5 hash operation is well known and will not be explained further. The MD5 hash result 2 is uniquely dependent on the file 1 and can be used to verify file 1.

[0016] Next the originator performs an RSA algorithm operation 20 on the MD5 hash result 2 using the private key of the originator (A_{KPRI}) 3 to generate a signed hash (or digital signature) 4. The signed hash 4 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 1 and the signed hash 4 are transferred to the receiver resulting in a received file 5 and a received signed hash 6.

[0017] In order to verify the received file, the receiver independently generates two versions of the MD5 hash result. The first MD5 hash result 7 is generated from the received file 5 using a MD5 hash operation 30, and the second MD5 hash result 8 is obtained from the received signed hash 6 by performing an RSA operation 40 on the received signed hash 6 using the public key of the originator A (A_{Kpub}) 9 held by the receiver. The first MD5 hash result 7 and the second MD5 hash result 8 are compared in a comparison operation 50 and if they are found to be equal, the received file 5 is authenticated and can be executed.

[0018] In order for the above authentication scheme to work, the receiver must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure through the use of a certification authority. The certification authority is trusted by the receiver, such that received information signed by the certification authority is trusted by the receiver.

[0019] Therefore, as shown the certification authority performs an RSA algorithm operation 60 on the public key of the originator (A_{KPub}) 11 using the private key of the certification authority (CA_{KPRI}) 12 resulting in a signed key 13 of the originator A. The signed key 13 and the certification authority public key (CA_{Kpub}) 14 are transferred to the receiver. As shown, if necessary the signed key 13 undergoes a certificate chain analysis operation 70 to obtain the received signed public key 15 of the originator A.

[0020] A certificate chain analysis operation is required if the certificate authority CA is not known by the receiver. In this case, the certificate authority is requested to provide its public key signed by a further certificate authority using the private key of the further certificate authority. If the further certificate authority is trusted by the receiver, the receiver will be able to use the public key of the further signature authority to verify that the public key of the signed authority has been signed by the private key of the further signature authority. The receiver can then trust the certificate authority and can use the received certificate authority public key. If the further certificate authority is not trusted by the receiver, use must be made of an additional certificate authority.

[0021] The receiver has stored therein a root certification authority public key. The root certification authority is the most trusted by the receiver, and ultimately the stored public key of the root certification authority can be used to verify all other certification authorities in a certificate chain situation.

[0022] The receiver then performs an RSA operation 80 on the resulting signed public key of the originator (A_{KPub}) (15) using the root certification authority public key (Root CA_{KPub}) to obtain the public key of the originator (A_{KPub}) 9. The public key of the originator (A_{KPub}) 9 is then used in the RSA operation 40 as described above.

[0023] The present invention is described below with reference to a communication device, such as a mobile telephone. However, it will be clear to a skilled person that the present invention is also applicable to other devices. An exemplary communication device 200 is now described with reference to Figure 2.

[0024] The communication device 200 shown in Figure 2 comprises a communication interface 210 coupled to an antenna 220 and to a processor 230. The processor 230 and the communication interface 210 are also coupled to volatile memory 240 and to a non-volatile memory 250. A smart card 260 is coupled to a smart card interface 270, which is also coupled to the processor 230. The smart card is equipped with its own processor 280 and memory 290.

[0025] The communication interface 210 comprises the necessary components to convert radio frequency signals for the communication device 200 received by the antenna 220 to digital signals to be stored in volatile memory 240 and/or non-volatile memory 250 and/or to be processed by processor 230, and to convert digital signals from the memories 240 and 250 and/or the processor 230 to radio frequency signals to be transmitted by the antenna 220. Thus communication interface 210 comprises radio frequency transmitter and receiver means and signal processor means, for example.

[0026] The volatile memory 240 and non-volatile memory 250 are used for storing program and other data for operation of the communication device 200.

[0027] The smart card is preferably a subscriber smart card (SIM) holding subscriber information used by the communication device 200, for example a Subscriber Identity Module card as currently used in the Global System for Mobile Communications (GSM system) and in use or proposed for other communication systems. However, it is possible that the smart card 260 may be another type of smart card received in the communication device instead of, or preferably in addition to a SIM card, for example an electronic commerce smart card.

[0028] As indicated above, the smart card is equipped with its own processor 280 and memory 290, and is capable of storing information therein and is also capable of carrying out operations or calculations on data received from the processor 230 via smart card interface 270 and of providing data or the results of such calculation to the processor 230 via smart card interface 270.

[0029] The smart card is preferably removably receivable in the communication device, for example by means of the provision of a slot in the housing of the communication device 200.

[0030] It will be appreciated by a skilled person that other components or arrangements of components within the communication device 200 are possible within the scope of the invention.

[0031] The secure download procedure in accordance with the invention will now be described with reference to Figure 3. In Figure 3 operations or data corresponding to operations or data in Figure 1 have been given similar reference numerals.

[0032] Figure 3 illustrates the download of an executable J2ME file in a MExE environment from an originator A to a device such as the communication device 200 described above with reference to Figure 2. As shown in Figure 3, box 3260 represents operations carried out and data stored in the smart card 260 of the communication device 200 shown in Figure 2, and the remaining operation and data storage is carried out in the rest of the communication device 200 shown in Figure 2.

[0033] As illustrated in Figure 2, the smart card 260 has no direct communications capability. Instead, the relevant data received by the communication device is passed by the processor 230 to the smart card 260 for storage therein and operation thereon.

[0034] In the procedure illustrated in Figure 3, the originator A performs an MD5 hash operation 310 on a file 31 to be transferred to create an MD5 hash result 32. As explained above, the MD5 hash result 32 is uniquely dependent on the file 31 and can be used to verify file 31.

[0035] Next the originator A performs an RSA algorithm operation 320 on the MD5 hash result 32 using the private key of the originator (A_{KPRI}) 33 to generate a signed hash 34. The signed hash 34 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 31 and the signed hash 34 are then sent to the communication device 200 resulting in a received file 35 and a received signed hash 36. File 35 is received using antenna 220 and communication interface 210 and is stored by the processor 230 in the volatile memory 240. In contrast, the signed hash 34 is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290.

[0036] As described above, in order to verify the received file, two versions of the MD5 hash result must be independently generated and compared. The first MD5 hash result 37 is generated by the communication device processor 230 from the received file 35 using a MD5 hash operation 330.

[0037] The second MD5 hash result 38 is obtained by the smart card from the received signed hash 36. The smart card processor 280 performs an RSA operation 340 on the received signed hash 36 stored in the smart card memory 390 using the public key of the originator A (A_{Kpub}) 39 stored in the smart card memory 290, as will be explained later.

[0038] The second MD5 hash result 38 is passed by the smart card processor 280 to the communication device processor 230 and the communication device processor 230 compares the first MD5 hash result 37 and the second MD5 hash result 38, calculated in the smart card 260, in a comparison operation 350. If the first MD5 hash result 37 and the second MD5 hash result 38 are found to be equal, the received file 35 is authenticated and can be executed.

[0039] In this arrangement, the smart card 260 must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure according to Figure 3 through the use of the root certification authority public key stored in the smart card memory 290. The root certification authority is trusted by the communications device, such that received information signed by the certification authority is trusted.

[0040] In this context, there may be more than one root certification authority. For example in the context of a mobile telephone the manufacturer and/or the operator can act as a root authority. In addition, it is possible to specify one or more trusted third parties as root certification authorities. The public key for each of the root certification authorities (eg the operator public root key (OPRK); the manufacturer public root key (MPRK); and third party public root key (TPRK)) is stored in the smart card of the communication device 200, for example during provisioning of a mobile telephone SIM card.

[0041] In order that the smart card 260 has authenticated access to the public key of the originator A (A_{Kpub}), as shown the root certification authority performs an RSA algorithm operation 360 on the public key of the originator (A_{KPub}) 311 using the private key of the certification authority ($RootCA_{KPRI}$) 312 resulting in a certificate from A 321 signed by the root certification authority. This certificate 321 is sent to the communications device 200, is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290 as certificate 322.

[0042] The Root certification authority public key ($RootCA_{KPub}$) 332 is already stored in the smart card memory 290, as indicated above. The smart card processor can perform an RSA operation 380 on the received certificate 322 using the Root Certification Authority public key ($RootCA_{KPub}$) 332 to obtain the public

BNSDOCID: <EP_____1289326A1_I_>

key of the originator A (A_{Kpub}) 39. The smart card processor can then use the obtained public key of the originator A (A_{Kpub}) 39 and the received signed hash 36 in RSA operation 340 to obtain the smart card MD5 hash value 38, as outlined above.

[0043] Also shown in Figure 3 is the transfer of the Root Certification Authority public key ($RootCA_{KPub}$) 331 to the communications device for storage in the smart card memory as Root Certification Authority public key ($RootCA_{KPub}$) 332. It is desirable to update the root certification authority keys periodically in a secure manner otherwise the security of the system will be compromised.

[0044] A preferred mechanism for the secure transfer of a Root public key (for example OPRK, MPRK, TPRK) using communication system messaging technology will now be explained with reference to Figures 4 and 5.

[0045] Figure 4 illustrates message creation for transfer of a root key, for example the operator public root key (OPRK), to the smart card 360 in accordance with the invention. In this exemplary arrangement, the update is achieved using a SMS message as provided in the GSM/UMTS systems, although other messaging techniques could be used.

[0046] An RSA operation is performed on the new OPRK 41 with the operator's private root key 42 corresponding to the old OPRK stored in the smart card 360. As mentioned earlier, the old OPRK may have been stored in the smart card 360 during provisioning, or during a previous update of the root key. The resulting signed new operator public root key 44 is included in an SMS message 45 to be sent to the communication device. The SMS message 45 has an SMS header portion 451 and SMS download command 452 in addition to the signed new operator public root key 44. The SMS message in encrypted by the communication system prior to being sent to the communication device.

[0047] Figure 5 illustrates update of the root key in the communication device in accordance with an embodiment of the invention. In this exemplary embodiment of the invention, the SMS message 45 sent by the network 500 to the communication device 200 is passed to the smart card 260. Once the encrypted SMS message 45 is received in the smart card 260, the smart card 260 undertakes an SMS message analysis and memory update procedure 51.

[0048] In the SMS message analysis and memory update procedure 51 the SMS message is initially decrypted and the SMS message is analysed. The download command 452 instructs the smart card 260 that a new OPRK is being sent to the smart card 260. The smart card 260 performs an RSA operation on the received signed new OPRK using the old OPRK already stored in the smart card 260 to verify the identity of the sender. The OPRK stored in the smart card can then be updated using the new value. Preferably a confirmation message 52 is sent from the smart card 260 to the network using the communication interface 210 of the communication device 200.

[0049] Although the update of the operator public root key (OPRK) has been described above, it would be possible to update any root key stored in the smart card in the same way.

[0050] In accordance with an alternative embodiment of the invention, the manufacturer root public key may be stored partially in the smart card memory and partially in the communications device memory. This arrangement is more secure since the communication device then contributes to ensuring the security of download in the manufacturer domain using the manufacturer root public key. This helps to prevent an insecure smart card from changing the manufacturer public root key via download authorization.

[0051] Thus the present invention proposes a solution to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software.

[0052] Since the secure keys are stored on the smart card and calculations involving the secure keys are performed by the smart card, the security of the secure keys can be ensured. In addition, the result of the calculation performed on the received file by the device is not passed to the smart card.

[0053] As will be apparent to a skilled person, the invention could be implemented in a different form from that shown herein, and so the invention is intended to encompass all arrangements and variations within the scope of the appended claims.

Claims

1. A method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising:

   receiving software and security information relating to the received software;
   obtaining in the smart card a first calculation result from the security information using at least one secure key;
   obtaining in the device a second calculation result from calculations performed on the received software; and
   comparing in the device first and second calculation results to verify the received software.

2. The method as claimed in claim 1, further comprising the steps of;

   receiving additional signed originator key infor-

BNSDOCID: <EP_____1289326A1_I_>

mation;
obtaining, in the smart card, originator key information from the received signed originator key information using a root security key stored therein; and
obtaining in the smart card the first calculation result from the security information using the originator key information.

3. The method as claimed in claim 2 wherein the root security key stored in the smart card is updated by
receiving a root security key update message containing a new root security key;
verifying the new root security key using the existing root security key stored in the smart card;
storing the new root security key in the smart card.

4. The method as claimed in claim 2 or 3, wherein part of the root security key is stored in the smart card and part of the root security key is stored in the device.

5. The method as claimed in any preceding claim, wherein the smart card is a Subscriber Identity Module (SIM) card

6. A device comprising
communication means for receiving software and security information relating to the received software;
smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key;
means for obtaining a second calculation result from calculations performed on the received software;
means for comparing first and second calculation results to verify the received software.

7. The device as claimed in claim 6 wherein
the communications means also receives additional signed originator key information; and
the smart card interface also passes the additional signed originator key information to the smart card, which obtains originator key information from the received signed originator key information using a root security key stored therein; and obtains the first calculation result from the security information using the originator key information.

8. The device as claimed in claim 7 wherein
the communications means also receives a root security key update message containing a new root security key; and
the smart card interface passes the root security key update message to the smart card, which verifies the new root security key using the existing root security key stored in the smart card; and stores the new root security key in the smart card.

9. The device as claimed in claim 7 or 8, wherein the device comprises storage means and part of the root security key is stored in the smart card and part of the root security key is stored in the storage means.

10. The device as claimed in one of claims 6-9, wherein the smart card is a Subscriber Identity Module (SIM) card.

BNSDOCID: <EP_____1289326A1_I_>

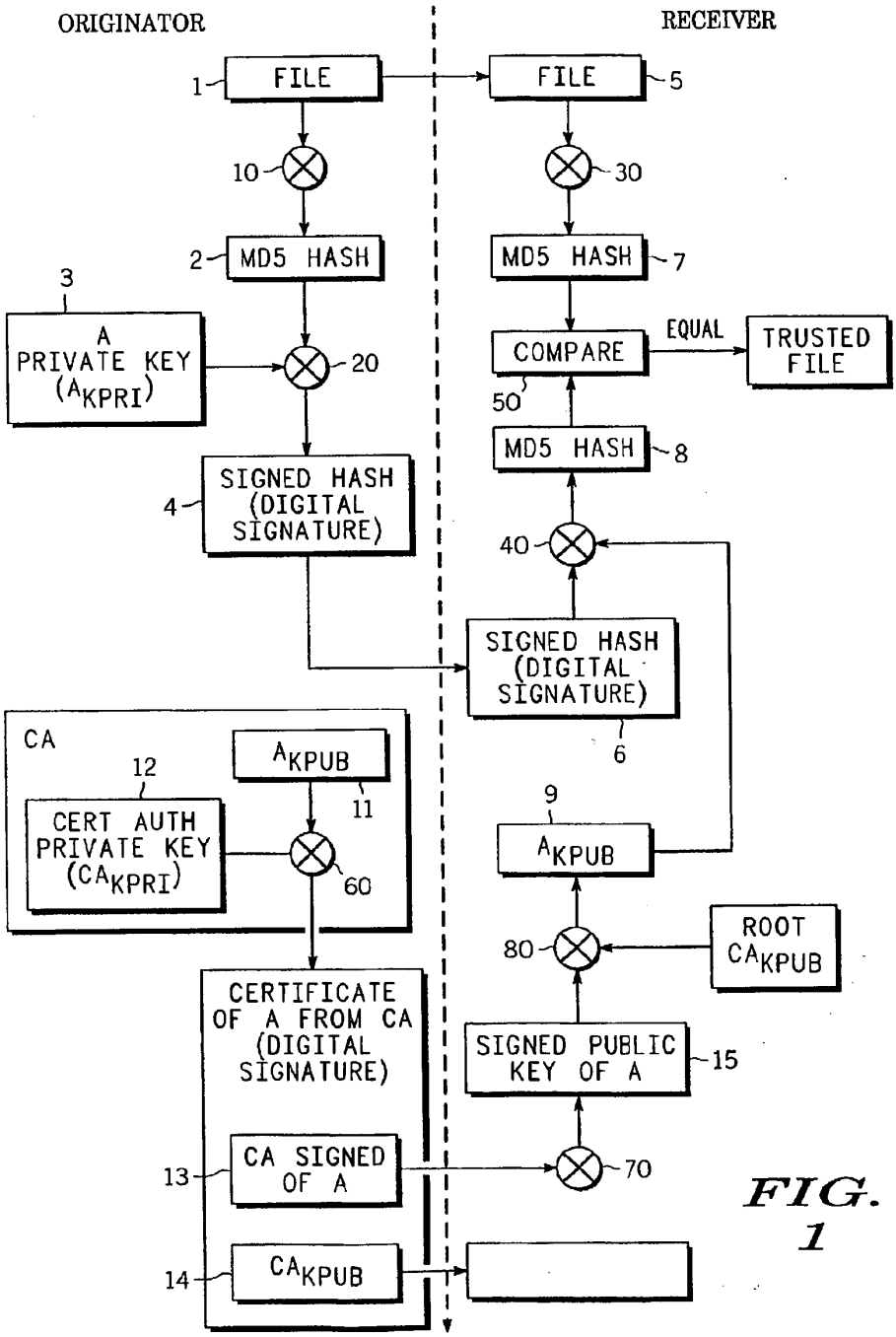


FIG. 1

BNSDOCID: <EP_____1289326A1_I_>

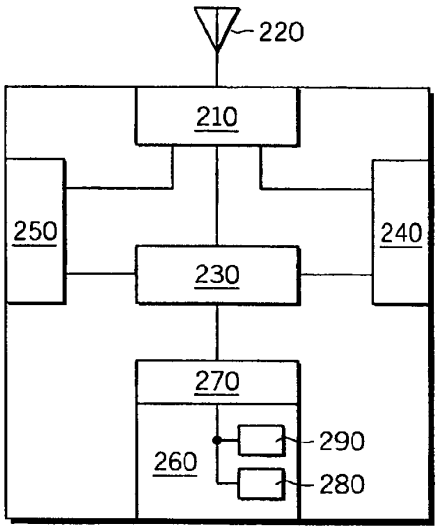


FIG. 2

BNSDOCID: <EP_____1289326A1_I_>

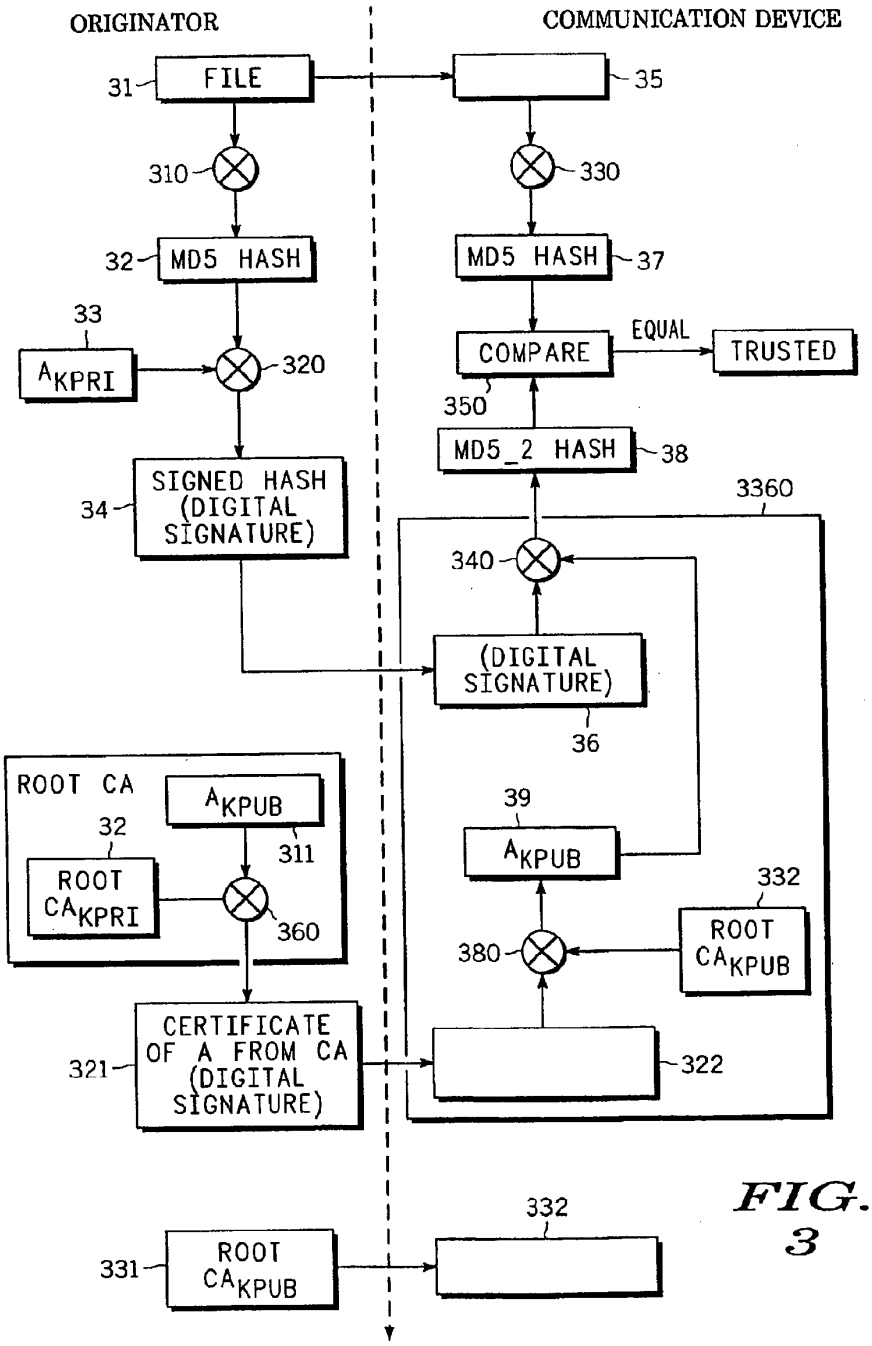


FIG. 3

BNSDOCID: <EP_____1289326A1_I_>

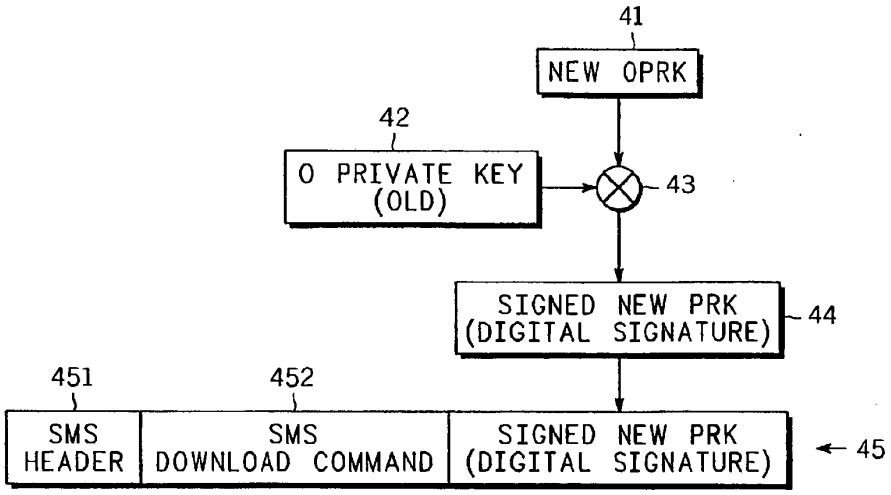
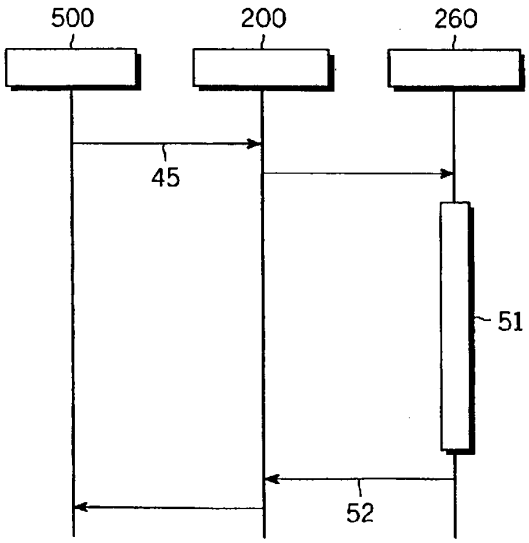


FIG. 4

FIG. 5



BNSDOCID: <EP_____1289326A1_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 40 2259

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 124 799 A (PARKER JOHN PATRICK) 26 September 2000 (2000-09-26) * the whole document *	1-4,6-9	H04Q7/32
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 (1993-09-29) * column 4, line 30 - column 5, line 32 *	1,6	
A	EP 1 124 401 A (LUCENT TECHNOLOGIES INC) 16 August 2001 (2001-08-16) * paragraphs '0002!-'0019! * * abstract; claims 1-13 *	2-4,7-9	
A	EP 0 977 452 A (LUCENT TECHNOLOGIES INC) 2 February 2000 (2000-02-02) * the whole document *	2-4,7-9	
A	EP 0 463 384 A (CIT ALCATEL) 2 January 1992 (1992-01-02) * the whole document *	1,6	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 February 2002	Coppieters, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1289326A1_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 40 2259

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-02-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6124799 A	26-09-2000	US 5864757 A	26-01-1999
		AU 715488 B2	03-02-2000
		AU 1409997 A	03-07-1997
		CA 2239550 A1	19-06-1997
		EP 0867099 A2	30-09-1998
		JP 11501182 T	26-01-1999
		JP 3080409 B2	28-08-2000
		WO 9722221 A2	19-06-1997
EP 0562890 A	29-09-1993	AT 193965 T	15-06-2000
		DE 69328847 D1	20-07-2000
		DE 69328847 T2	07-12-2000
		EP 0562890 A1	29-09-1993
		ES 2149801 T3	16-11-2000
EP 1124401 A	16-08-2001	AU 1828001 A	16-08-2001
		BR 0100191 A	09-10-2001
		CN 1308472 A	15-08-2001
		EP 1124401 A2	16-08-2001
		JP 2001251292 A	14-09-2001
EP 0977452 A	02-02-2000	US 6243811 B1	05-06-2001
		BR 9902942 A	09-05-2000
		CN 1249588 A	05-04-2000
		EP 0977452 A2	02-02-2000
		JP 2000083017 A	21-03-2000
		TW 428409 B	01-04-2001
EP 0463384 A	02-01-1992	FR 2662878 A1	06-12-1991
		AT 135519 T	15-03-1996
		CA 2043290 A1	01-12-1991
		DE 69117814 D1	18-04-1996
		DE 69117814 T2	25-07-1996
		EP 0463384 A1	02-01-1992
		ES 2084726 T3	16-05-1996
		FI 912548 A	01-12-1991
		JP 3054225 B2	19-06-2000
		JP 4233341 A	21-08-1992
		NO 178597 B	15-01-1996
		US 5303285 A	12-04-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1289326A1_I_>

Electronic Patent Application Fee Transmittal					
Application Number:	14082040				
Filing Date:	15-Nov-2013				
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY				
First Named Inventor/Applicant Name:	Gregory G. Raleigh				
Filer:	James E. Harris/Ann Taylor				
Attorney Docket Number:	RALEP032C1				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	28303504
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	08-FEB-2017
Filing Date:	15-NOV-2013
Time Stamp:	16:42:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	020917INTEFSW00003409505876
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS1.pdf	1054319 df545a16ff0cfdca7b2df576f47352779352ab6d	no	5
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS2.pdf	1054265 198570e13407c6acaebf438f0b56af72fc1ac71a	no	5
Warnings:					
Information:					
3	Foreign Reference	2091.pdf	4030163 9f5a695d3972f432ff9791f8b2ac99ef7cbca74d	no	16
Warnings:					
Information:					
4	Foreign Reference	2092.pdf	2382529 5c57dc228f491cd9301830aad5e4493f4c99b261	no	12
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30661 c7deb7f3a4f4111c4cd28f870c15d1a839ffc674	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	8551937		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 01/31/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 01/31/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

TITLE OF INVENTION: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/01/2017

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 01/31/2017
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

TITLE OF INVENTION: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/01/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	709-224000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
❑ Issue Fee
❑ Publication Fee (No small entity discount permitted)
❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
❑ A check is enclosed.
❑ Payment by credit card. Form PTO-2038 is attached.
❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
❑ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 01/31/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 01/31/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/082,040	Applicant(s) RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *December 1, 2016 Amendment*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1,5,8-21 and 24-30*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Applicant cancelled claims 2-4, 6, 7, 22 and 23.

3. Further pertinent references of interest are noted on the attached PTO-892.

4. Applicant's December 1, 2016 Information Disclosure Statement (IDS) has been reviewed. Note the attached IDS.

Allowable Subject Matter

5. Claims 1, 5, 8-21 and 24-30 are allowed.

6. The following is an examiner's statement of reasons for allowance: Applicant's December 1, 2016 Amendment regarding claims 1, 5, 8-21 and 24-30 have been reviewed. Claims 1, 5, 8-21 and 24-30 are now allowed as all the cited prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Claims 1, 5, 8-21 and 24-30 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claims 1, 5, 8-21 and 24-30 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified abstract idea.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Fahd A. Obeid can be reached on 571-270-3324. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

Notice of References Cited	Application/Control No. 14/082,040	Applicant(s)/Patent Under Reexamination RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,115,823 A	09-2000	Velasco; Francisco	G06F1/3203	710/16
*	B	US-7,505,795 B1	03-2009	Lim; Vincent Cheekiat	H04W52/0232	340/7.38
*	C	US-9,326,173 B2	04-2016	Luft; Achim	H04W4/00	1/1
*	D	US-2009/0065571 A1	03-2009	Jain; Deepak	G06K19/07739	235/379
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5617539	A	1997-04-01	Ludwig et al.	
	2	6141565	A	2000-10-31	Feuerstein et al.	
	3	6401113	B2	2002-06-04	Lazaridis et al.	
	4	6510152	B1	2003-01-21	Gerszberg et al.	
	5	6535855	B1	2003-03-18	Cahill et al.	
	6	6542500	B1	2003-04-01	Gerszberg et al.	
	7	6546016	B1	2003-04-08	Gerszberg et al.	
	8	6570974	B1	2003-05-27	Gerszberg et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6601040	B1	2003-07-29	Kolls, H. Brock	
	10	6636721	B2	2003-10-21	Threadgill et al.	
	11	6654786	B1	2003-11-25	Fox et al.	
	12	6690918	B2	2004-02-10	Evans et al.	
	13	6959393	B2	2005-10-25	Hollis et al.	
	14	7082422	B1	2006-07-25	Zirngibl et al.	
	15	7095754	B2	2006-08-22	Benveniste, Mathilde	
	16	7133386	B2	2006-11-07	Holur et al.	
	17	7136361	B2	2006-11-14	Benveniste, Mathilde	
	18	7151764	B1	2006-12-19	Heinonen et al.	
	19	7177919	B1	2007-02-13	Truong et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7191248	B2	2007-03-13	Chattopadhyay et al.	
	21	7272660	B1	2007-09-18	Powers et al.	
	22	7369848	B2	2008-05-06	Jiang, Yue Jun	
	23	7369856	B2	2008-05-06	Ovadia, Shlomo	
	24	7409569	B2	2008-08-05	Illowsky et al.	
	25	7428750	B1	2008-09-23	Dunn et al.	
	26	7440433	B2	2008-10-21	Rink et al.	
	27	7486658	B2	2009-02-03	Kumar, Rajneesh	
	28	7562213	B1	2009-07-14	Timms, Natalie	
	29	7577431	B2	2009-08-18	Jiang, Yue Jun	
	30	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7602746	B2	2009-10-13	Calhoun et al.	
	32	7610047	B2	2009-10-27	Hicks III et al.	
	33	7643411	B2	2010-01-05	Andreasen et al.	
	34	7657920	B2	2010-02-02	Arseneau et al.	
	35	7660419	B1	2010-02-09	Ho, Jin-Meng	
	36	7661124	B2	2010-02-09	Ramanathan et al.	
	37	7664494	B2	2010-02-16	Jiang, Yue Jun	
	38	7719966	B2	2010-05-18	Luft et al.	
	39	7724716	B2	2010-05-25	Fadell, Anthony M.	
	40	7770785	B2	2010-08-10	Jha et al.	
	41	7817983	B2	2010-10-19	Cassett et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	7873001	B2	2011-01-18	Silver, Andrew	
	43	7979069	B2	2011-07-12	Hupp et al.	
	44	8036387	B2	2011-10-11	Kudelski et al.	
	45	8044792	B2	2011-10-25	Orr et al.	
	46	8065365	B2	2011-11-22	Saxena et al.	
	47	8085808	B2	2011-12-27	Brusca et al.	
	48	8125897	B2	2012-02-28	Ray et al.	
	49	8132256	B2	2012-03-06	Bari, Farooq	
	50	8140690	B2	2012-03-20	Ly et al.	
	51	8145194	B2	2012-03-27	Yoshikawa et al.	
	52	8151205	B2	2012-04-03	Follmann et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8191106	B2	2012-05-29	Choyi et al.	
	54	8194549	B2	2012-06-05	Huber et al.	
	55	8194581	B1	2012-06-05	Schroeder et al.	
	56	8195153	B1	2012-06-05	Frencel et al.	
	57	8219134	B2	2012-07-10	Maharajh et al.	
	58	8271025	B2	2012-09-18	Brisebois et al.	
	59	8291439	B2	2012-10-16	Jethi et al.	
	60	8307095	B2	2012-11-06	Clark et al.	
	61	8320902	B2	2012-11-27	Moring et al.	
	62	8325906	B2	2012-12-04	Fullarton et al.	
	63	8340628	B2	2012-12-25	Taylor et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	8363799	B2	2013-01-29	Gruchala et al.	
	65	8380247	B2	2013-02-19	Engstrom	
	66	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	67	8412798	B1	2013-04-02	Wang, Frank C.	
	68	8418168	B2	2013-04-09	Tyhurst et al.	
	69	8448015	B2	2013-05-21	Gerhart, David	
	70	8494559	B1	2013-07-23	Malmi	
	71	8503358	B2	2013-08-06	Hanson et al.	
	72	8505073	B2	2013-08-06	Taglienti et al.	
	73	8521775	B1	2013-08-27	Poh et al.	
	74	8531954	B2	2013-09-10	McNaughton et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	75	8538421	B2	2013-09-17	Brisebois et al.	
	76	8543814	B2	2013-09-24	Laitinen et al.	
	77	8600895	B2	2013-12-03	Felsher, David Paul	
	78	8639215	B2	2014-01-28	McGregor et al.	
	79	8670752	B2	2014-03-11	Fan et al.	
	80	8675852	B2	2014-03-18	Maes, Stephane H.	
	81	8700729	B2	2014-04-15	Dua, Robin	
	82	8719397	B2	2014-05-06	Levi et al.	
	83	8731519	B2	2014-05-20	Flynn et al.	
	84	8744339	B2	2014-06-03	Halfmann et al.	
	85	8787249	B2	2014-07-22	Giaretta et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	86	8811338	B2	2014-08-19	Jin et al.	
	87	8819253	B2	2014-08-26	Simeloff et al.	
	88	8837322	B2	2014-09-16	Venkataramanan et al.	
	89	8838686	B2	2014-09-16	Getchius, Jeffery M.	
	90	8838752	B2	2014-09-16	Lor et al.	
	91	8855620	B2	2014-10-07	Sievers et al.	
	92	8862751	B2	2014-10-14	Faccin et al.	
	93	8898748	B2	2014-11-25	Burks et al.	
	94	8908516	B2	2014-12-09	Tzamaloukas et al.	
	95	8943551	B2	2015-01-27	Ganapathy et al.	
	96	8971841	B2	2015-03-03	Menezes et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	97	8971912	B2	2015-03-03	Chou et al.	
	98	8995952	B1	2015-03-31	Baker et al.	
	99	9030934	B2	2015-05-12	Shah et al.	
	100	9032427	B2	2015-05-12	Gallant et al.	
	101	9173090	B2	2015-10-27	Tuchman et al.	
	102	9282460	B2	2016-03-08	Souissi, Slim Salah	
	103	9325737	B2	2016-04-26	Gutowski et al.	
	104	9344557	B2	2016-05-17	Gruchala et al.	
	105	9367680	B2	2016-06-14	Mahaffey et al.	
	106	9413546	B2	2016-08-09	Meier et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020120370	A1	2002-08-29	Parupudi et al.	
	2	20020138599	A1	2002-09-26	Dilman et al.	
	3	20030184793	A1	2003-10-02	Pineau, Richard A.	
	4	20040054779	A1	2004-03-18	Takeshima et al.	
	5	20040176104	A1	2004-09-09	Arcens, Suzanne	
	6	20040225561	A1	2004-11-11	Hertzberg et al.	
	7	20040243680	A1	2004-12-02	Mayer, Georg	
	8	20040267872	A1	2004-12-30	Serdy et al.	
	9	20050091505	A1	2005-04-28	Riley et al.	
	10	20050108075	A1	2005-05-19	Douglis et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20060099970	A1	2006-05-11	Morgan et al.	
	12	20060182137	A1	2006-08-17	Zhou et al.	
	13	20070130283	A1	2007-06-07	Klein et al.	
	14	20070255797	A1	2007-11-01	Dunn et al.	
	15	20070297378	A1	2007-12-27	Poyhonen et al.	
	16	20080089303	A1	2008-04-17	Wirtanen et al.	
	17	20080096559	A1	2008-04-24	Phillips et al.	
	18	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
	19	20080320497	A1	2008-12-25	Tarkoma et al.	
	20	20090006229	A1	2009-01-01	Sweeney et al.	
	21	20090016310	A1	2009-01-15	Rasal, Digambar L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	22	20090042536	A1	2009-02-12	Bernard et al.	
	23	20090047989	A1	2009-02-19	Harmon et al.	
	24	20090132860	A1	2009-05-21	LIU et al.	
	25	20090217364	A1	2009-08-27	Salmela et al.	
	26	20090307696	A1	2009-12-10	Vals et al.	
	27	20100190469	A1	2010-07-29	Vanderveen et al.	
	28	20120144025	A1	2012-06-07	Melander et al.	
	29	20120166364	A1	2012-06-28	Ahmad et al.	
	30	20130072177	A1	2013-03-21	Ross et al.	
	31	20140241342	A1	2014-08-28	Constantinof, Cristian	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1345154	CN	A	2002-04-17	Datang Microelectronics Tech. Co.		
	2	1545114	EP	A1	2005-06-22	Alcatel		
	3	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	4	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		
	5	2005339247A	JP		2005-12-08	Secured Communications		
	6	2006155263A	JP		2006-06-15	NEC Corporation		
	7	2006197137	JP		2006-07-27	NTT Docomo Inc.		
	8	2006344007	JP	A	2006-12-21	Hitachi Ltd.		
	9	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	10	2002093877	WO	A1	2002-11-21	Nokia Corp.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	2003017063	WO	A2	2003-02-27	Apogee Networks		
	12	2003017065	WO	A2	2003-02-27	Apogee Networks		
	13	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.		
	14	2006004784	WO	A1	2006-01-12	Japan Communications Inc.		
	15	2007120310	WO		2007-10-25	Qualcomm Inc.		
	16	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		
	17	2011002450	WO	A1	2011-01-06	Alcatel-Lucent USA Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)," Release 9, Document No. 3GPP TS 24.312, V9.1.0, March 2010	
	2	3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offload; Stage 2," Release 10, Document No. 3GPP TS 23.261, V1.0.0, March 2010	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	Ahmed et al., "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS)," 2010 IEEE	
	4	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	5	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	6	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	7	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	8	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	
	9	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	10	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	11	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	12	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	
	13	Quintana, David, "Mobile Multitasking," April 14, 2010	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	14	Roy et al., "Energy Management in Mobile Devices with the Cinder Operating System", Stanford University, MIT CSAIL, June 3, 2010	
	15	Windows7 Power Management, published April 2009	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	01/24/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

CPC							
Symbol						Type	Version
H04W		28	/	0289		F	2013-01-01
H04W		24	/	00		A	2013-01-01
H04W		36	/	14		A	2013-01-01
H04L		41	/	0893		I	2013-01-01
H04L		41	/	5054		I	2013-01-01
H04L		47	/	803		I	2013-01-01
H04L		47	/	822		I	2013-01-01
H04L		47	/	824		I	2013-01-01
H04L		43	/	0882		I	2013-01-01
H04W		4	/	001		I	2013-01-01
H04W		52	/	0212		I	2013-01-01
H04W		84	/	12		I	2013-01-01
H04L		47	/	20		I	2013-01-01
H04W		28	/	0215		I	2013-01-01
H04W		28	/	12		I	2013-01-01
H04W		84	/	042		A	2013-01-01
H04L		43	/	08		I	2013-01-01
H04L		47	/	12		I	2013-01-01
H04L		47	/	14		I	2013-01-01
H04L		47	/	19		I	2013-01-01
H04L		47	/	801		I	2013-01-01
H04L		47	/	805		I	2013-01-01
H04W		28	/	021		I	2013-01-01
H04W		28	/	0221		I	2013-01-01
H04W		28	/	0268		I	2013-01-01
H04L		41	/	5051		I	2013-01-01
H04L		47	/	808		I	2013-01-01
H04W		28	/	0257		I	2013-01-01
H04L		63	/	10		I	2013-01-01
H04L		63	/	102		I	2013-01-01
H04L		63	/	20		I	2013-01-01

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	1/26/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

H04W		12	/ 08	I	2013-01-01
H04W		48	/ 16	I	2013-01-01
H04W		80	/ 04	I	2013-01-01
H04L		47	/ 2475	I	2013-01-01
H04W		48	/ 04	I	2013-01-01
H04W		52	/ 0264	I	2013-01-01
H04W		24	/ 08	I	2013-01-01
Y02B		60	/ 50	A	2013-01-01
H04L		47	/ 2425	A	2013-01-01
H04W		24	/ 02	I	2013-01-01
H04W		28	/ 0247	I	2013-01-01
H04W		28	/ 20	I	2013-01-01
H04W		48	/ 06	I	2013-01-01
H04L		12	/ 14	I	2013-01-01
H04M		15	/ 30	A	2013-01-01
H04M		15	/ 41	I	2013-01-01
H04M		15	/ 43	I	2013-01-01
H04M		15	/ 44	I	2013-01-01
H04M		15	/ 66	I	2013-01-01
H04M		15	/ 8016	I	2013-01-01
H04M		15	/ 8055	I	2013-01-01
H04M		15	/ 81	I	2013-01-01
H04W		4	/ 26	A	2013-01-01
H04L		41	/ 5006	I	2013-01-01
H04L		41	/ 5022	A	2013-01-01
H04L		41	/ 5029	I	2013-01-01
H04L		12	/ 1492	I	2013-01-01
H04L		12	/ 1496	I	2013-01-01
H04L		41	/ 0896	I	2013-01-01
H04W		28	/ 0284	I	2013-01-01

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	1/26/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 25

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC Combination Sets				
Symbol	**Type**	**Set**	**Ranking**	**Version**
/				
/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	1/26/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

U.S. Patent and Trademark Office

Part of Paper No. 20170126

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
709	224	G	0	6	F	15 / 173 (2006.01.01)						
CROSS REFERENCE(S)		H	0	4	M	3 / 42 (2006.01.01)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
455	414.1											

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	1/26/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 25

U.S. Patent and Trademark Office

Part of Paper No. 20170126

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	24	18	18												
3	25	19	19												
4	26	20	20												
5	5	21	21												
6	27	22	29												
7	28	23	30												
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	1/26/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 25

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	14/082,040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

SEARCHED			
Class	Subclass	Date	Examiner
prior			
search	updated	1/25/2017	AJR
455	405,414.1	1/25/2017	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
709	**224**	**1/26/2017**	**AJR**
455	414.1	1/26/2017	AJR
H04L	29/08072	1/26/2017	AJR
H04I 29/08108		1/26/2017	AJR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	1/23/2017	AJR

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/082,040	Filing Date 11/15/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/01/2016	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 23	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
JASON B. EADDY

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	Rudy, Andrew J.
Serial No.:	14/082,040	Art Unit:	3687
Filed:	November 15, 2013	Conf. No.:	1015
Title:	Device-Assisted Services for Protecting Network Capacity		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

In response to the Office Action dated June 1, 2016, the no-fee deadline for response being September 1, 2016, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 7.

AMENDMENTS TO THE CLAIMS

Without prejudice and without surrender of any subject matter, please amend the claims as follows:

1. (Currently Amended) A wireless end-user device ~~system~~, comprising:

a wireless modem to communicate data for network service usage activities between the device and a wireless network;

a processor that executes instructions ~~of a communications device configured~~ to[[:]]

~~monitor a network service usage activity of the communications device in network communication;~~

~~classify the network service usage activity for differential network access control for protecting network capacity; and~~

associate [[the]] network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy, ~~based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity~~

set an application state indicating whether the first device application, associated with a particular network service usage activity, is in the foreground of user interaction, and

dynamically determine whether to apply the network service usage control policy to the particular network service usage activity, based on the application state and based on a power control state; and

a memory coupled to the processor ~~and configured~~ to provide the processor with the instructions.

2-4. (Canceled).

5. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

implement the network service usage control policy at least in part via communication with the first device application through ~~differential network access for the network service usage~~

~~activity for protecting network capacity using~~ an emulated network access API that indicates to the first device application that an available wireless network is unavailable when a dynamic determination applies the network service usage control policy to the particular network service usage activity.

6-7. (Canceled).

8. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user ~~communications~~ device.

9. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user ~~communications~~ device; and

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of wireless end-user ~~communications~~ devices in communication with one or more base stations.

10. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user ~~communications~~ device;

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of wireless end-user ~~communications~~ devices in communication with one or more base stations; and

receive router traffic control instructions from the service controller, wherein the service controller provides the router traffic control instructions to assist in dynamically managing network capacity usage for the plurality of wireless end-user ~~communications~~ devices in

communication with the one or more base stations ~~for protecting network capacity of one or more access networks~~.

11. (Currently Amended) The wireless end-user device recited in claim 1, wherein [[the]] dynamically determining whether to apply the network service usage control policy to the particular network service usage activity ~~classifying~~ is further based on a current wireless ~~access~~ network and/or the network service usage control policy is based on a current wireless ~~access~~ network.

12. (Currently Amended) The wireless end-user device recited in claim 1, wherein dynamically determining whether to apply the network service usage control policy to the particular network service usage activity further includes dynamically assigning a network capacity controlled services priority level to the particular network service usage activity based on a network busy state.

13. (Currently Amended) The wireless end-user device recited in claim 1, wherein ~~classifying includes querying a network element for determining a network capacity controlled services classification and/or~~ associating includes querying a network element for determining an association of the first device application with the network service usage control policy.

14. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings, packet error rate, jitter and delay settings, queue settings, and tag settings.

15. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters, the filters comprising a first filter specifying applicability of the policy only when the first device application is not in the foreground of user interaction, and a second filter specifying applicability of the policy only in one or more specific power control states.

16. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters implemented as cascading filters.

17. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters using a network busy state and/or a time of day as an index into a traffic control setting.

18. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

differentially control the particular network service usage activity based on the network service usage control policy based on a network busy state~~, wherein the network service usage activity is classified as a network capacity controlled service~~.

19. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

differentially control the particular network service usage activity based on the network service usage control policy based on a user input and/or a current wireless ~~access~~ network~~,~~ ~~wherein the network service usage activity is classified as a network capacity controlled service~~.

20. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

modify or replace a network stack interface of the wireless end-user ~~communications~~ device to provide for intercept or discontinuance of network access messaging for implementing traffic control of the particular network service usage activity ~~for network capacity controlled services for protecting network capacity~~.

21. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

store a network capacity controlled service list, wherein the network capacity controlled service list is periodically updated based on monitored network service usage activities.

22-23. (Canceled).

24. (New) The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction when the user of the device is directly interacting with that application or perceiving any benefit from that application.

25. (New) The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction based on a state of user interface priority for the application.

26. (New) The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

27. (New) The wireless end-user device of claim 1, wherein the processor further executes the instruction to, for at least a second device application or service, allow network service usage activities without regard to the power control state.

28. (New) The wireless end-user device of claim 1, wherein the power control state is a power state of the device.

29. (New) The wireless end-user device of claim 1, wherein the power control state is a power save state of the device.

30. (New) The wireless end-user device of claim 1, wherein the power control state is a power state of the wireless modem.

REMARKS

Claims 1-23 were pending and rejected by the Office Action dated June 1, 2016. Applicant has amended claims 1, 5, and 8-21, canceled claims 2-4, 6-7, and 22-23, and added new claims 24-30. Accordingly, claims 1, 5, 8-21, and 24-30 are active in the application. In view of the amendments to the claims and the following remarks, Applicant respectfully requests reconsideration.

Claim Rejections – 35 U.S.C. § 101

In section 4, the Office Action rejected claims 1-23 under 35 U.S.C. § 101, indicating that the claimed invention is directed towards non-statutory subject matter.

Applicant has extensively reworked the claims to remove potentially abstract language and incorporate further elements from prior dependent claims 6 and 15 and from the specification (see, e.g., paragraphs [00256]-[00257] and [00265]-[00266]) into claim 1. Applicant submits that claim 1 and its dependents are now are within a statutorily permitted subject area, as the current claims are drawn to a device and include limitations that improve the functioning of the device itself. For instance, the device as recited in claim 1 contains features that allow network service usage policies to be directed to the network service usage activity of a particular application based on specific operational states, including the foreground state of the application and the power control state of the device and/or modem. Thus as exemplary but non-limiting enabled improvements to the device, such features allow an embodiment of the device to prevent applications that the user is not interacting with from further depleting an already-low battery, or allow an embodiment of the device to prevent applications that the user is not interacting with from cycling modem power. Applicant respectfully submits that, at least due to the inclusion of such features, the amended claims are directed to statutory subject matter. No new matter has been added.

Claim Rejections – 35 U.S.C. § 103

In section 6, the Office Action rejected claims 1-23 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 8,484,568 to Rados (hereinafter, "Rados"). Applicant respectfully

submits that Rados is not prior art to the current claims. It is Applicant's belief that the claims are each supported no later than May 25, 2010, the filing date of Provisional Patent Application 61/348,022, which is in the chain of priority for the current application. This priority date predates the filing date of Rados. Accordingly, Applicant respectfully requests that the rejection be withdrawn.

CONCLUSION

Applicant respectfully requests entry of these amendments as provided herein. The application is believed to be in condition for allowance, and a Notice of Allowance is hereby respectfully requested. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: December 1, 2016 By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: Dec. 1, 2016 By: /Ann Taylor/
Ann Taylor

Electronic Patent Application Fee Transmittal					
Application Number:	14082040				
Filing Date:	15-Nov-2013				
Title of Invention:	Device-Assisted Services for Protecting Network Capacity				
First Named Inventor/Applicant Name:	Gregory G. Raleigh				
Filer:	James E. Harris/Ann Taylor				
Attorney Docket Number:	RALEP032C1				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**790**

Electronic Acknowledgement Receipt	
EFS ID:	27671315
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	01-DEC-2016
Filing Date:	15-NOV-2013
Time Stamp:	18:56:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$790
RAM confirmation Number	120216INTEFSW00005609505876
Deposit Account	505876
Authorized User	Ann Taylor
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS.pdf	1059039 953834adfce4a09146cb780c6f5b39a175095d45	no	19
Warnings:					
Information:					
2	Foreign Reference	2074.pdf	7047386 8fcf0ca549f5be7aaa631006e8ff2b73a8defc71	no	40
Warnings:					
Information:					
3	Foreign Reference	2075.pdf	1121298 941f56ab8972334f740a42da0f64323e27525f22	no	46
Warnings:					
Information:					
4	Foreign Reference	2076.pdf	972543 b6cc2b50dfba5f9dafe28939427a6228d7218933	no	39
Warnings:					
Information:					
5	Foreign Reference	2077.pdf	1901018 6539164475086ad9ab3c492961440050eb14eb60	no	51
Warnings:					
Information:					
6	Foreign Reference	2078.pdf	1128425 34d3158d2965f487838e0079c67c3c6926679a7c	no	38
Warnings:					
Information:					

7	Foreign Reference	2079.pdf	1123981 085b25ad47976d8c5eaa309e384a85cf56ef2e6a	no	3
Warnings:					
Information:					
8	Foreign Reference	2080.pdf	877755 277dd25bee280796f81a1943a6d00e1e91ac213a	no	11
Warnings:					
Information:					
9	Foreign Reference	2081.pdf	975121 23277e1884ea272e116216d6e83b5c822a6a2d58	no	14
Warnings:					
Information:					
10	Foreign Reference	2082.pdf	7497094 1cab9a3e1917138dd03e255717030799796eafc5	no	45
Warnings:					
Information:					
11	Foreign Reference	2083.pdf	782462 2ce1ee70705ca2f54e4571f31517ddc96b1c19c4	no	8
Warnings:					
Information:					
12	Foreign Reference	2084.pdf	1397656 9e6a8957ad2e807f979431120ddbd1741e2acde7	no	57
Warnings:					
Information:					
13	Foreign Reference	2085.pdf	441333 e8defb411cdca2f87d3c0c97eae168e0c2960826	no	19
Warnings:					
Information:					

14	Foreign Reference	2086.pdf	232424 fbefdfe44bda45a08d0dfa2e2b40b5d0f577f976	no	29
Warnings:					
Information:					
15	Foreign Reference	2087.pdf	922375 5370f148f48d4def4ad535f2c2b1762f0ca57119	no	47
Warnings:					
Information:					
16	Foreign Reference	2088.pdf	255944 b4b8ef7ddc1f98c4716aaed35917fdb84c9be0fa	no	18
Warnings:					
Information:					
17	Foreign Reference	2089.pdf	172902 9025822de8f174376f282787af6b3524407be5db	no	13
Warnings:					
Information:					
18	Foreign Reference	2090.pdf	643809 f84e3fb9347dd0d758241de1f737fa384a62bebe	no	38
Warnings:					
Information:					
19	Extension of Time	P032C1_Ext.pdf	163581 8fcbd2e524be36d7274e429cb2e8415f513a43f5	no	2
Warnings:					
Information:					
20		P032C1_OAR.pdf	96821 c8a108013b6da6af953f66f267038f78454caaf3	yes	9
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	

	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	9	
Warnings:					
Information:					
21	Fee Worksheet (SB06)	fee-info.pdf	32680 ab7d11ad5138a1cc2b59c2406b971432c646b422	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	28845647		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5617539	A	1997-04-01	Ludwig et al.	
	2	6141565	A	2000-10-31	Feuerstein et al.	
	3	6401113	B2	2002-06-04	Lazaridis et al.	
	4	6510152	B1	2003-01-21	Gerszberg et al.	
	5	6535855	B1	2003-03-18	Cahill et al.	
	6	6542500	B1	2003-04-01	Gerszberg et al.	
	7	6546016	B1	2003-04-08	Gerszberg et al.	
	8	6570974	B1	2003-05-27	Gerszberg et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6601040	B1	2003-07-29	Kolls, H. Brock	
	10	6636721	B2	2003-10-21	Threadgill et al.	
	11	6654786	B1	2003-11-25	Fox et al.	
	12	6690918	B2	2004-02-10	Evans et al.	
	13	6959393	B2	2005-10-25	Hollis et al.	
	14	7082422	B1	2006-07-25	Zirngibl et al.	
	15	7095754	B2	2006-08-22	Benveniste, Mathilde	
	16	7133386	B2	2006-11-07	Holur et al.	
	17	7136361	B2	2006-11-14	Benveniste, Mathilde	
	18	7151764	B1	2006-12-19	Heinonen et al.	
	19	7177919	B1	2007-02-13	Truong et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7191248	B2	2007-03-13	Chattopadhyay et al.	
	21	7272660	B1	2007-09-18	Powers et al.	
	22	7369848	B2	2008-05-06	Jiang, Yue Jun	
	23	7369856	B2	2008-05-06	Ovadia, Shlomo	
	24	7409569	B2	2008-08-05	Illowsky et al.	
	25	7428750	B1	2008-09-23	Dunn et al.	
	26	7440433	B2	2008-10-21	Rink et al.	
	27	7486658	B2	2009-02-03	Kumar, Rajneesh	
	28	7562213	B1	2009-07-14	Timms, Natalie	
	29	7577431	B2	2009-08-18	Jiang, Yue Jun	
	30	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7602746	B2	2009-10-13	Calhoun et al.	
	32	7610047	B2	2009-10-27	Hicks III et al.	
	33	7643411	B2	2010-01-05	Andreasen et al.	
	34	7657920	B2	2010-02-02	Arseneau et al.	
	35	7660419	B1	2010-02-09	Ho, Jin-Meng	
	36	7661124	B2	2010-02-09	Ramanathan et al.	
	37	7664494	B2	2010-02-16	Jiang, Yue Jun	
	38	7719966	B2	2010-05-18	Luft et al.	
	39	7724716	B2	2010-05-25	Fadell, Anthony M.	
	40	7770785	B2	2010-08-10	Jha et al.	
	41	7817983	B2	2010-10-19	Cassett et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	7873001	B2	2011-01-18	Silver, Andrew	
	43	7979069	B2	2011-07-12	Hupp et al.	
	44	8036387	B2	2011-10-11	Kudelski et al.	
	45	8044792	B2	2011-10-25	Orr et al.	
	46	8065365	B2	2011-11-22	Saxena et al.	
	47	8085808	B2	2011-12-27	Brusca et al.	
	48	8125897	B2	2012-02-28	Ray et al.	
	49	8132256	B2	2012-03-06	Bari, Farooq	
	50	8140690	B2	2012-03-20	Ly et al.	
	51	8145194	B2	2012-03-27	Yoshikawa et al.	
	52	8151205	B2	2012-04-03	Follmann et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8191106	B2	2012-05-29	Choyi et al.	
	54	8194549	B2	2012-06-05	Huber et al.	
	55	8194581	B1	2012-06-05	Schroeder et al.	
	56	8195153	B1	2012-06-05	Frencel et al.	
	57	8219134	B2	2012-07-10	Maharajh et al.	
	58	8271025	B2	2012-09-18	Brisebois et al.	
	59	8291439	B2	2012-10-16	Jethi et al.	
	60	8307095	B2	2012-11-06	Clark et al.	
	61	8320902	B2	2012-11-27	Moring et al.	
	62	8325906	B2	2012-12-04	Fullarton et al.	
	63	8340628	B2	2012-12-25	Taylor et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	8363799	B2	2013-01-29	Gruchala et al.	
	65	8380247	B2	2013-02-19	Engstrom	
	66	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	67	8412798	B1	2013-04-02	Wang, Frank C.	
	68	8418168	B2	2013-04-09	Tyhurst et al.	
	69	8448015	B2	2013-05-21	Gerhart, David	
	70	8494559	B1	2013-07-23	Malmi	
	71	8503358	B2	2013-08-06	Hanson et al.	
	72	8505073	B2	2013-08-06	Taglienti et al.	
	73	8521775	B1	2013-08-27	Poh et al.	
	74	8531954	B2	2013-09-10	McNaughton et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	75	8538421	B2	2013-09-17	Brisebois et al.	
	76	8543814	B2	2013-09-24	Laitinen et al.	
	77	8600895	B2	2013-12-03	Felsher, David Paul	
	78	8639215	B2	2014-01-28	McGregor et al.	
	79	8670752	B2	2014-03-11	Fan et al.	
	80	8675852	B2	2014-03-18	Maes, Stephane H.	
	81	8700729	B2	2014-04-15	Dua, Robin	
	82	8719397	B2	2014-05-06	Levi et al.	
	83	8731519	B2	2014-05-20	Flynn et al.	
	84	8744339	B2	2014-06-03	Halfmann et al.	
	85	8787249	B2	2014-07-22	Giaretta et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	86	8811338	B2	2014-08-19	Jin et al.	
	87	8819253	B2	2014-08-26	Simeloff et al.	
	88	8837322	B2	2014-09-16	Venkataramanan et al.	
	89	8838686	B2	2014-09-16	Getchius, Jeffery M.	
	90	8838752	B2	2014-09-16	Lor et al.	
	91	8855620	B2	2014-10-07	Sievers et al.	
	92	8862751	B2	2014-10-14	Faccin et al.	
	93	8898748	B2	2014-11-25	Burks et al.	
	94	8908516	B2	2014-12-09	Tzamaloukas et al.	
	95	8943551	B2	2015-01-27	Ganapathy et al.	
	96	8971841	B2	2015-03-03	Menezes et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	97	8971912	B2	2015-03-03	Chou et al.	
	98	8995952	B1	2015-03-31	Baker et al.	
	99	9030934	B2	2015-05-12	Shah et al.	
	100	9032427	B2	2015-05-12	Gallant et al.	
	101	9173090	B2	2015-10-27	Tuchman et al.	
	102	9282460	B2	2016-03-08	Souissi, Slim Salah	
	103	9325737	B2	2016-04-26	Gutowski et al.	
	104	9344557	B2	2016-05-17	Gruchala et al.	
	105	9367680	B2	2016-06-14	Mahaffey et al.	
	106	9413546	B2	2016-08-09	Meier et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020120370	A1	2002-08-29	Parupudi et al.	
	2	20020138599	A1	2002-09-26	Dilman et al.	
	3	20030184793	A1	2003-10-02	Pineau, Richard A.	
	4	20040054779	A1	2004-03-18	Takeshima et al.	
	5	20040176104	A1	2004-09-09	Arcens, Suzanne	
	6	20040225561	A1	2004-11-11	Hertzberg et al.	
	7	20040243680	A1	2004-12-02	Mayer, Georg	
	8	20040267872	A1	2004-12-30	Serdy et al.	
	9	20050091505	A1	2005-04-28	Riley et al.	
	10	20050108075	A1	2005-05-19	Douglis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20060099970	A1	2006-05-11	Morgan et al.	
	12	20060182137	A1	2006-08-17	Zhou et al.	
	13	20070130283	A1	2007-06-07	Klein et al.	
	14	20070255797	A1	2007-11-01	Dunn et al.	
	15	20070297378	A1	2007-12-27	Poyhonen et al.	
	16	20080089303	A1	2008-04-17	Wirtanen et al.	
	17	20080096559	A1	2008-04-24	Phillips et al.	
	18	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
	19	20080320497	A1	2008-12-25	Tarkoma et al.	
	20	20090006229	A1	2009-01-01	Sweeney et al.	
	21	20090016310	A1	2009-01-15	Rasal, Digambar L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	22	20090042536	A1	2009-02-12	Bernard et al.	
	23	20090047989	A1	2009-02-19	Harmon et al.	
	24	20090132860	A1	2009-05-21	LIU et al.	
	25	20090217364	A1	2009-08-27	Salmela et al.	
	26	20090307696	A1	2009-12-10	Vals et al.	
	27	20100190469	A1	2010-07-29	Vanderveen et al.	
	28	20120144025	A1	2012-06-07	Melander et al.	
	29	20120166364	A1	2012-06-28	Ahmad et al.	
	30	20130072177	A1	2013-03-21	Ross et al.	
	31	20140241342	A1	2014-08-28	Constantinof, Cristian	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1345154	CN	A	2002-04-17	Datang Microelectronics Tech. Co.		
	2	1545114	EP	A1	2005-06-22	Alcatel		
	3	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	4	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		
	5	2005339247A	JP		2005-12-08	Secured Communications		
	6	2006155263A	JP		2006-06-15	NEC Corporation		
	7	2006197137	JP		2006-07-27	NTT Docomo Inc.		
	8	2006344007	JP	A	2006-12-21	Hitachi Ltd.		
	9	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	10	2002093877	WO	A1	2002-11-21	Nokia Corp.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	2003017063	WO	A2	2003-02-27	Apogee Networks		
	12	2003017065	WO	A2	2003-02-27	Apogee Networks		
	13	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.		
	14	2006004784	WO	A1	2006-01-12	Japan Communications Inc.		
	15	2007120310	WO		2007-10-25	Qualcomm Inc.		
	16	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		
	17	2011002450	WO	A1	2011-01-06	Alcatel-Lucent USA Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)," Release 9, Document No. 3GPP TS 24.312, V9.1.0, March 2010	
	2	3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offload; Stage 2," Release 10, Document No. 3GPP TS 23.261, V1.0.0, March 2010	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	Ahmed et al., "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS)," 2010 IEEE	
	4	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	5	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	6	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	7	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	8	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	
	9	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	10	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	11	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	12	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	
	13	Quintana, David, "Mobile Multitasking," April 14, 2010	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	14	Roy et al., "Energy Management in Mobile Devices with the Cinder Operating System", Stanford University, MIT CSAIL, June 3, 2010	
	15	Windows7 Power Management, published April 2009	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-12-01
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 July 2009 (23.07.2009)

PCT

(10) International Publication Number
WO 2009/091295 A1

(51) International Patent Classification:
H04Q 7/38 (2006.01) *H04Q 7/32* (2006.01)

(21) International Application Number:
PCT/SE2008/000031

(22) International Filing Date: 15 January 2008 (15.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: RUNE, Johan [SE/SE]; Terrängvägen 12, S-181 30 Lidingö (SE).

(74) Agent: MOSSMARK, Anders; Albihns AB, Box 142, S-401 22 Göteborg (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(54) Title: PRE-FETCHING OF INPUT DATA FOR ACCESS NETWORK SELECTION

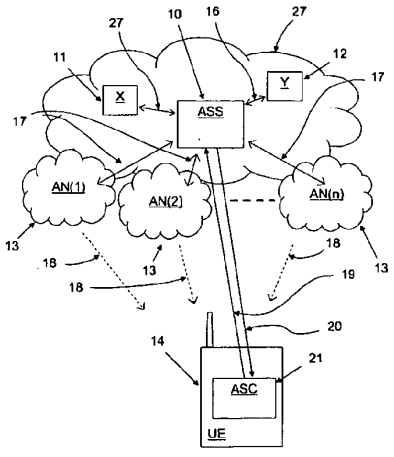


FIG 1

(57) Abstract: The present invention relates to a method, an Access Selection Server and a communication network 27 for network access selection 26. The network comprises an Access Selection Server (ASS) 10, at least one User Equipment (UE) 14, an Access Selection Client (ASC) 21 arranged in the UE 14 and communication nodes 11, 12. The ASS collects 23 access selection parameters used for the selection 26 of access network for the network access for the UE 14 in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE 14 and a first node. The ASS 10 forwards 25 the access selection parameters and/or processes 23 the access selection parameters and sends 25 the results of the processed parameters to the UE 14. The parameters forwarded 25 or the results sent 25 by the ASS 21 being access selection information, based on which the ASC 21 performs 26 activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow. What particularly characterizes the invention is that the ASS 10 controls at least the collection or the processing 23 of the access selection parameters, the collection or the processing 23 being performed at least when the UE 14 is disconnected from the communication network 27. Furthermore, the parameters collected or processed 23 when the UE 14 is disconnected from the communication network 27 are forwarded 25 and/or the results of the processed parameters are sent 25 as access selection information by the ASS 10 to the UE 14 when the UE 14 is again connected to the communication network 27.

WO 2009/091295 A1

TITEL

Pre-Fetching of Input Data for Access Network Selection

TECHNICAL FIELD

The present invention relates to a method and a communication system for network access selection and an access selection server in the system enabling said method.

BACKGROUND

Third generation mobile systems (3G), based on WCDMA (Wideband Code Division Multiple Access) radio access technology, are being deployed on a broad scale all around the world. However, as user and operator requirements and expectations will continue to evolve a new phase in the standard specification body called 3rd Generation Partnership Project (3GPP) has started to consider the next major steps in the evolution of the 3G standard. The terminals used in the network are having more functions integrated which means that an increasing number of access types such as e.g. LTE (Long Term Evolution), WiMAX (Worldwide Interoperability for Microwave Access) and WLAN (Wireless Local Area Network) and new services such as Voice over IP (VoIP) or IP-TV are added to the terminal.

In a multi-access environment the multi-interface terminal is often faced with a choice of potential access networks to connect to, either for a new connection or for a potential handover of an existing one or simply for being reachable through after power on.

These access networks may differ in various properties, such as access technology (e.g. 3G or WLAN), available operators (directly or indirectly) and roaming agreements, presence of NATs and/or firewalls, applicable policies (such as codec restrictions), access rate, supported QoS and current load. All these variable parameters make the choice of access network(s) potentially complex. The more data about the available access networks that

the access selection algorithm takes into account, the more sophisticated and accurate (and thus beneficial) the selection can be made.

Some of this information is available through scanning of system information that is broadcast from access points or base stations and that can be received by any terminal (equipped with a matching interface) without any type of prior association, registration, authentication or connection.

However, retrieval of other parts of the information, potentially most of it, requires IP level communication, which in turn implies that the terminal has to go through all the preceding procedures that are needed to establish IP level communication. In for example a WLAN network this means that the terminal first has to associate with the access point at the MAC layer, then in most cases go through the user authentication and authorization procedure, typically using Extensible Authentication Protocol (EAP), and finally request and receive IP configuration data through Dynamic Host Configuration Protocol (DHCP).

It is first after all these procedures that the terminal can retrieve some of the information that may be required to select which of the available access networks that it should connect to. That is, the terminal actually has to connect to an access network in order to retrieve access selection input data. This implies an additional effort, unless the terminal already is connected.

Furthermore, retrieving such information related to a particular access network may be difficult using IP communication via another access network. Instead the terminal may have to connect to the particular concerned access network. The reason is that with the currently proposed techniques for locating an access network's local network profile, in which much of the interesting information is expected to be stored, relies on information conveyed in DHCP option 15 during the DHCP configuration procedure.

The DCHP-related technique is for instance described in the internet-draft "A Framework for Session Initiation Protocol User Agent Profile Delivery",

written by D. Petrie and published October 2006. This document specifies a framework to enable configuration of Session Initiation Protocol (SIP) User Agents in SIP deployments. The framework provides a means to deliver profile data that terminals need to be functional, automatically and with minimal (preferably none) user and administrative intervention. The framework describes how SIP User Agents can discover sources, request profiles and receive notifications related to profile modifications.

Since DHCP relies on subnet broadcasting and hardware addresses, it is only available through the particular access network and not via routers from another access network. As an unfortunate consequence the terminal in practice has to connect to each available access network in order to retrieve the information that serves as input data to the selection of which access network to connect to. Even if workarounds would appear for the limitation of the DHCP-based local network profile retrieval, the terminal would still have to connect to at least one access network in order to retrieve the relevant information from all the available access networks to enable sophisticated access selection.

Consequently, connecting to an access network and establishing IP level communication (with all its preceding procedures) with subsequent information retrieval can be rather time consuming and could consequently make the access selection inconveniently slow. It is even worse if the terminal has to connect not only to one, but to all the available access networks. The problem is the most severe when the terminal is not already connected to an access network and the access selection concerns a new connection.

Previous access selection solutions are either terminal-controlled, network-controlled or a combination of both (or the trivial method: user-controlled access selection). Network-controlled access selection is typically used for controlling handover in cellular networks. More accurately this access selection is network-controlled but terminal-assisted – the network's decision

relies on reports of measured radio signal strengths from neighbouring base stations. In networks based on IETF protocols, relying on Mobile IP for mobility and session continuity, handovers and their associated access selection are typically entirely terminal-controlled. For access selection during the initial connection to a network, before any network connectivity is available, the solutions are inherently terminal-controlled, since no network-based functionality is available.

In one approach to access selection it is proposed to implement so called access awareness functionality (for support and execution of access selection) both in the terminal and in the network. It is implemented as a layer between the application layer and the transport layer (between applications and sockets). The functionality-related signalling is independent (not mixed with other signalling, in particular application control signalling). It assumes simultaneous accesses and applies to individual communication sessions without impact to the service performance. The network-based access awareness functionality is generic and system independent in the sense that it can be applied to Internet based systems as well as cellular systems, such as 3GPP and IP Multimedia Subsystem (IMS).

The applications interface an extended socket mechanism which makes decision about what accesses to use for connection establishment/handover influenced by a set of criteria or descriptions provided by the application at socket creation. The functionality is structured to have a clear separation between the actual decision making process and the actions resulting from access awareness decisions. The access awareness functionality is system wide which means that it is generally distributed between network entities and in particular an end-user terminal and the network side.

The Assumptions/high-level requirements for the functionality includes: support for any application, compatible with any mobility management, support of simultaneous use of different accesses, separated from

applications by an interface and extensible to cover other contexts than the current networking capabilities.

A prime task of the network-based functionality is to assist the terminal-based functionality by collecting network-based information on behalf of the terminal, which is filtered and possibly refined before it is sent to the terminal. The functionality collects events from the system that is needed for access awareness. In this way the terminal and the potentially resource-scarce access link are relieved from some of the potentially demanding information retrieval and processing.

Another potential task of the network-based access awareness functionality is to assist the terminal-based functionality in calculating choices, decisions and/or recommendation in order to offload the terminal of some of this processing, which is expected to be rather intensive. The access awareness assistant performs its tasks on explicit instructions from the terminal or by analyzing contextual information or, possibly in some cases, based on default instructions.

The communication session is per socket basis (individual communication sessions) and a socket request from the application in the terminal triggers the access awareness functionality. The access selection functionality identifies the application from the port numbers in the socket request (and/or possibly other information such as indications of the process originating the socket request) and infers the application's requirements on the communication quality. This, together with policies and other information, such as available accesses and possibly network load, is then used as input data to the access selection decision. The characteristics are provided to the access awareness functionality in the network as "application preferences". These preferences may express what the functionality is allowed to do on behalf of the application and within which limits it may act. For instance, "I need 128 kbps, but could stretch myself down to 64 kbps, but not lower".

The purpose of the network-based access awareness functionality is to let users and applications exploit the fact that accesses and access networks have different characteristics. That is to give applications the necessary tools to exploit differences or give the applications enough support so that they do not need to be aware of the different charactertics. Another purpose is to provide means to adapt to existing or changing conditions. That is, for instance to give recommendations to applications, make applications adapt to changing conditions, adapt communications to changing conditions and trigger mobility management actions. The user benefits can be summarized in increased service quality, reduced interference between applications, convenience and reduced costs. The Access Service Provided (ASP) benefits include more satisfied customers, a mechanism to improve service and a new, potential service offering. Benefits for application and contents providers are higher service penetration and usage take rate, more attractive services and potential for better services.

The 3GPP has also initiated activities to develop access selection functionality (also know as multi access terminal steering) for the evolving 3GPP systems being (or expected to be) deployed in an access network environment of increasing multitude and heterogeneity. The access selection work in 3GPP focuses on packet-switched services and on 3GPP context (access technologies such as EGPRS, WCDMA/HSPA and LTE). It works also for non-3GPP context (WLAN, WiMAX, etc.). The target is a (more or less) network-controlled solution, but there will also be some kind of terminal-based access selection functionality.

The 3GPP access selection provides new functionality in the 3GPP architecture with an Access Selection Discovery and Selection Function (ANDSF), which is separate or part of the Policy and Charging Rules Function (PCRF) in the network. The ANDSF has control of all available accesses for the terminal, current network load, RAT etc. The functionality also comprises an access selection function in the terminal, which based on

request or information from the network based access selection functionality (ANDSF) performs activation/deactivation/modification or changes of access (es). It finally comprises a reference point between the access selection functions in the terminal and the network and potentially new interfaces between the PCRF and the ANDSF and between the Proxy-Call Session Control Function - P-CFCS (application server) and the ANDSF.

An assumption (which is not valid for the initial phase of access selection in a 3GPP context but which is a natural continuation in future phases) is that the terminal may have multiple accesses that may be active in parallel, so called simultaneous multi-access. The ANDSF further gets access information from the access selection function in the terminal and information from the network (load status etc.). The ANDSF will also have session information on all active accesses for the terminal. An IP connection between the access selection function in the terminal and in the network will be established at activation of the default access network. The connection is used to communicate access selection information between the access selection function in the terminal and the ANDSF. The ANDSF will be able to send activation/deactivation/modification/change requests of an access network, or instructions, policies, rules or information as the basis for such decisions to the access selection function in the terminal.

The objectives of the 3GPP access selection are automated access selection, automated network discovery/selection, tariff-dependent access priorities, definition of preferred network and service-dependent priorities. Example of benefits for the operators are network load management, radio management capabilities, automatic access selection for the user, improved resource efficiency and system usage and minimized handover effects. User benefits are enablement to influence the access selection, reduction of energy consumption in the terminal, selection of zone per cost etc.

The choice of access network is consequently complex and time consuming. There are so many parameters to consider, e.g. access technology, available

operators, roaming agreements, presence of NATs, and/or firewalls, applicable policies, access rate, supported QoS, current load etc. The collection of these parameters takes long time. Some of this information is available through scanning of system information that is broadcast from access points or base stations and that can be received without any type of prior association, registration, authentication or connection. However, as described, retrieval of other parts of the information, potentially most of it, requires IP level communication between the terminal and the network. This in turn implies that the terminal has to go through all the preceding procedures that are needed to establish IP level communication. Normally the terminal must connect to each concerned access network in order to retrieve all access selection input data.

In the research community access selection schemes have been developed that rely on functionality in both the terminal and the network, typically with some kind of access awareness assistant or access selection wizard in the network helping the terminal by providing information or recommendations or even making decisions on behalf of the terminal in order to maintain operator control.

However, the network access awareness/access control function acts on explicit instructions from the terminal and/or current contextual information about the terminal's whereabouts and current activities. It is largely dependent on contextual information and/or the explicit instructions from the terminal and remains in a standby mode when the terminal is disconnected from the network. The advanced access selection schemes depend on information that requires IP communication to retrieve – scanning is not enough.

Moreover, gathering a multitude of information from potential access networks over resource scarce and error prone access link is time consuming. The network-based functionality off-loads the terminal-based access awareness/access control functionality, but still needs time to collect

and deliver the information. When the information is needed for an access selection decision, it will often take too long time to collect all the input data to enable a timely access selection decision.

Consequently, due to the time delay and the need for an IP communication, today's solutions do not allow swift, sophisticated access selection.

SUMMARY

The object of the present invention is to remove the above mentioned deficiencies of prior art solutions and to shorten the time for network access selection.

This object is enabled by means of a method for network access selection in a communication network. The network comprises an Access Selection Server (ASS), at least one User Equipment (UE), an Access Selection Client (ASC) arranged in the UE and communication nodes. The ASS collects access selection parameters used for the selection of access network for the network access for the UE in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE and a first node. The ASS forwards the access selection parameters and/or processes the access selection parameters and sends the results of the processed parameters to the UE. The parameters forwarded or the results sent by the ASS being access selection information, based on which the ASC performs activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow .

What particularly characterizes the method is that the ASS controls at least the collection or the processing of the access selection parameters, the collection or the processing at least being performed when the UE (14) is disconnected from the communication network. Furthermore, the parameters collected or processed when the UE is disconnected from the communication network are forwarded and/or the results of the processed parameters are

sent as access selection information by the ASS to the UE when the UE is again connected to the communication network.

This object is also enabled by means of an Access Selection Server (ASS) being adapted for network access selection. The ASS is arranged in a communication network further comprising at least one User Equipment (UE), an Access Selection Client (ASC) being arranged in the UE and communication nodes. The ASS is further adapted to collect access selection parameters used for the selection of access network for the network access for the UE in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE and a first node. The ASS further is adapted to forward the access selection parameters and/or process the access selection parameters and send the results of the processed parameters to the UE. The parameters forwarded or the results sent by the ASS being access selection information based on which the ASC performs activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow.

What particularly characterizes the ASS is that it is further adapted to control at least the collection or the processing of the access selection parameters. The ASS is further adapted to perform the collection or the processing at least when the UE is disconnected from the communication network. The ASS is further adapted to, when the UE (14) is again connected to the communication network, forward the parameters, collected or processed when the UE is disconnected from the communication network, and/or send the results of the processed parameters, as access selection information to the UE.

This object is finally enabled by means of a communication network for network access selection. The communication network comprises an Access Selection Server (ASS), at least one User Equipment (UE), an Access Selection Client (ASC) being arranged in the UE and communication nodes.

The ASS is adapted to collect access selection parameters used for the selection of access network for the network access for the UE in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE and a first node. The ASS further is adapted to forward the access selection parameters and/or process the access selection parameters and send the results of the processed parameters to the UE. The parameters forwarded or the results sent by the ASS being access selection information based on which the ASC performs activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow.

What particularly characterizes the ASS is that it is further adapted to control at least the collection or the processing of the access selection parameters. The ASS is further adapted to perform the collection or the processing at least when the UE is disconnected from the communication network. The ASS is further adapted to, when the UE (14) is again connected to the communication network, forward the parameters, collected or processed when the UE is disconnected from the communication network, and/or send the results of the processed parameters, as access selection information to the UE.

One advantage of the invention is that the solution enables swift, sophisticated access selection that takes data into account that cannot be retrieved from the respective candidate access networks through scanning from the terminal, but which requires established IP communication to retrieve. Another advantage it that it is general enough to be applicable in a variety of access selection solutions, including the ones being worked out in the research community_and in the 3GPP. Further advantages will be described in relation to the embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following text the invention will be described in detail with reference to the attached drawings. These drawings are used for illustration only and do not in any way limit the scope of the invention:

Figure 1 Schematically shows the communication system with the Access Selection functionality according to the present invention.

Figure 2 Schematically shows a flow diagram for the Access Selection functionality.

Figure 3 Shows a signalling diagram for the Access Selection functionality.

DETAILED DESCRIPTION

The invention will now be described in detail with reference to embodiments described in the detailed description and shown in the drawings.

The present invention focus on the problem that existing access selection solutions do not allow swift, sophisticated access selection that takes data into account that cannot be retrieved from the respective candidate access networks through scanning from the terminal. Instead it requires established IP communication to retrieve such data. Such network-based information is either gathered by network-based access selection functionality or by the terminal itself, potentially over a resource restricted and possibly delay prone radio connection. When the information is needed for an advanced access selection decision, it often, or even typically, takes too long to collect or process all the relevant input data to enable a timely access selection decision.

The embodiments refer to a method and a telecommunication system for network access selection, an Access Selection Server and an Access Selection Client, in the system enabling said method. The system, the server

and the client are adapted to perform the method steps as described in the method. It should be understood by a person skilled in the art that the fact that the system and in particular the system parts perform a method step means that it is adapted to perform said step.

The present invention relates to a method for network access selection comprising an Access Selection Server (ASS) 10 being arranged in a communication network 27, at least one User Equipment (UE) 14, an Access Selection Client (ASC) 21 being arranged in the UE and communication nodes 11, 12.

The communication network 27 is illustrated in figure 1. The term "node" is herein used in a general sense. It should be understood that different nodes may be integrated into a single node and that the functions represented/employed by a node could also be realized as separate nodes. The ASS 10 is located in the core network. Where it is located depends on which kind of access selection technology that is used (terminal- or network controlled). Examples of selection technologies are described in the background part. The communication nodes X 11 and Y 12 may for instance be databases, profile servers, Authentication/Authorization and Accounting (AAA) server, Home Subscriber Server (HSS), Session Initiation Protocol (SIP) proxies, Home Agents etc. What kind of nodes which are present depends on in which network/sub-network that the access selection function is located.

The functionality of the ASS 10, on which the invention is based, is illustrated in figure 2. The functionality comprises a learning stage 22 for the behaviour of a control of at least the collecting/receiving or processing of access selection parameters when the UE 14 is disconnected from the communication network 27. It further comprises a step 23 when the collecting/receiving or processing is performed. This is followed by a requesting stage 24 where the UE when being connected to the communication network requests the ASS to send/forward access selection

information. During step 25 the ASS sends/forwards the information and at step 26 the UE (the ASC in the UE) performs the access selection, handover or similar. The collecting/receiving is performed via connections 27, 16 and 17 from the nodes 11 – 12 and the access networks 13. The request is sent via connection 19 and the information is sent/forwarded via connection 20. The functionality will also be described step by step in the following text.

During operation the ASS collects 23 access selection parameters used for the selection 26 of access network for the network access for the UE 14 in a multi-access environment (more than one access network 13). What kind of parameters and how it is used (network or terminal controlled access selection 26) varies, and it should be understood that all kinds of access selection related parameters are included within the term "collected".

In particular, the ASS during operation receives 23, see figure 2, access selection parameters from the nodes 11,12 via the connections 27,16 established using reference points (not described further in this document) corresponding to a certain interfaces. Possible parameters received are e.g. node location information, connection information, disconnection information, network load information, policy-based restrictions and network-based information. The ASS further receives 23 network-based parameters from the different access networks 13 (1, 2 up to n) connected to the core network. This is enabled through a reference point 17. The interfaces referenced 18 – 20 will be described later.

The network access enables a traffic bearer for a traffic flow between an application in the UE 14 and a first node. A first node is for instance a peer node for peer-to-peer communication, e.g. Voice over IP communication, or an application server for client-server communication. The traffic preferably flows via a PDN-GW, which for instance could be a Systems Architecture Evolution (SAE) Gateway (GW)/Home Agent (HA) in a SAE network in a 3GPP domain or an access router. An application could for instance be VoIP or video calls. A first node is the receiver of the traffic flow from the UE.

The traffic bearer may be enabled between the UE 14 and a Packet Data Network Gateway (PDN GW) and the traffic flow between the application in the UE and a first node is then communicated via the PDN GW.

During operation the ASS 10 forwards 25 the access selection parameters and/or processes the access selection parameters and sends 25 the results of the processed parameters to the UE 14 using connection 20, see figure 1-2. The parameters forwarded or the results sent by the ASS are defined as access selection information. Results are network-based filtered and refined information.

From now on reference will be made to the UE 14 including the ASC 21. Since the ASC is included in the UE, the UE is able to perform activities in practise executed by the ASC.

Based on the access selection information, the UE 14, executed by the ASC 21, performs 26 activation of new network access and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow.

Access selection information is for instance instructions to the ASC to select 26 a certain access for the traffic bearer, the instruction being accompanied by for instance Quality of Service and Traffic Flow Template information. As another example the access selection information may be information that serves as input data to an access selection decision in the UE, e.g. rules guiding or directing such an access selection decision or input data in the form of information about the current state of the network(s) or access network(s).

What particularly characterizes the present invention is that the ASS 10 controls at least the collection or the processing 23 of the access selection parameters and that the collection or the processing 23 at least being performed when the UE 14 is disconnected from the communication network 27. The parameters collected or processed when the UE is disconnected

from the communication network are forwarded 25 and/or the results of the processed parameters are sent as access selection information by the ASS to the UE when the UE is again connected to the communication network.

In an access selection functionality it is an important task of the ASS 10 to feed 25 the UE 14 with relevant information collected from network-based sources 11, 12, and 13, which are not accessible through scanning from the UE 14. In addition to offloading the UE from some of the collection and processing 23 of information, the inventive solution proposes an adaptive feature in the ASS that allows it not only to provide the UE with relevant information, but also to prepare such information transfers while the UE is disconnected. This enables access selection 26 decisions that are both fast and sophisticated.

The ASS can collect and/or process 23 access selection parameters from various access networks 13. This is made through the reference point 17. What parameters to at least collect or process and from which access networks are normally determined by contextual information, such as the terminal's current point of connection, concerned applications, policy and profile data, etc. The problem with the known access selection technologies is that the ASS 10 can either itself analyze such contextual information received from the UE 14 or base its parameter collection on explicit instructions from the UE. The ASS is then largely dependent on the UE and remains in a standby mode when the terminal is disconnected from the communication network 27.

According to the characterizing part the present invention this dependency is partly removed by enabling the ASS 10 to maintain meaningful activity even when the UE 14 is disconnected from the communication network 27. During such time periods the ASS controls what parameters it should at least collect or process 23 and from which access networks 13 it should collect or process it. The purpose of collecting or processing parameters even when the UE is disconnected from the communication network is to be able to provide 25 the

ASC 21 in the UE with relevant access selection information without unnecessary delay as soon as the UE connects to the communication network 27 (and/or when requested by the UE). If the ASS has managed to collect or process parameters that actually turn out to be relevant, this method enables fast and sophisticated access selection 26.

According to one embodiment of the present invention the control by the ASS 10, comprising the control of at least the collection or the processing 23 of parameters by the ASS, is based on contextual information, historical records and/or statistics from the records for the communication network 27 location of the UE. An adaptive learning scheme is located in the ASS and controls at least the collection or the processing 23 of parameters. Also the sending and/or forwarding 25 of access selection information are preferably controlled by the adaptive learning scheme in the ASS.

To be able to adapt the control of at least the collection or processing 23 to the UE's history of movements, connections and disconnections the ASS has to be able to detect (and record) these actions from the UE which constitute the input data to the adaptive scheme.

A key component in the present invention is the control of at least the collection or the processing 23 behaviour by the ASS 10 (the adaptive learning scheme). According to the adaptive scheme the ASS continuously records relevant contextual information and learns 22 from historical records as well as statistics extracted from such records. The control behaviour is then continuously modified accordingly. There are different examples what kind of contextual information that the ASS can learn from:

According to a first example the time period between the disconnecting and the following connecting of the UE 14 to the communication network 27 is controlled. If the period exceeds a certain period value, the control of at least the collection or the processing 23 of parameters is at least based on:

1. Contextual information on where in the communication network 27 the UE is most likely to appear when connecting to the communication network, and

2. Which access network or networks the UE can select from when connecting to the communication network 27.

The statistics is based in information about the selectable access network or networks.

The ASS 10 consequently learns 22 where the UE 14 is most likely to "appear" after a significant period of disconnection and which access networks 13 that it then usually has to select between. The word "appear" is here used as a metaphor for connecting to the communication network 27. From the point of view of the ASS the UE is invisible as long as it is disconnected and visible only when it is connected to the communication network. Thus, in this context and with this "terminology" the word "appear" is a rather descriptive term for the event where the UE changes from being invisible to being visible.

Contextual data may take the shape of an access network 13, one or more access points/base stations, one or more cell(s)/zone(s) or even geographical data. The ASS 10 can learn 22 and maintain statistics about multiple such "locations of probable appearance". The knowledge acquired in this way allows the ASS 10 to proactively at least collect or process 23 data that is relevant for access selection 26 during initial connections.

In another example of what kind of contextual information that the ASS 10 can learn 22 from, the control of at least the collection the or processing 23 of parameters is at least based on movement pattern that reoccurs frequently. In this context movement pattern refers to movement between communication network 27 locations.

This means that the ASS 10 learns to which new location the UE 14 is likely to move from a certain current communication network 27 location. A "location" may in this context be an access network 13, an access point(s)/base station(s), one or more cell(s)/zone(s) or a geographical area (e.g. indicating the vicinity of a certain access network, a certain access point/base station or a certain cell/zone). The knowledge learnt 22 in this way allows the ASS to proactively at least collect or process 23 parameters that are relevant for access selection 26 during (potential) handovers. To refine its choice of information sources, the ASS may also take into consideration the currently used application(s).

The acquired knowledge may also be relevant for access selection 26 in a "camping" state, i.e. when the UE 10 is connected/associated with an access network 13, but not actively communicating. Optionally, the ASS 10 may maintain separate statistics on movement patterns for the UE 14 in the "camping" and actively communicating states respectively. An additional option for how to refine the statistics for movement patterns in an actively communicating state (i.e. for the purpose of handovers) is to take the currently used application(s) into account, such that movement pattern statistics per application or application type can be maintained.

In another example of what kind of contextual information that the ASS 10 can learn 22 from the time period between the disconnecting and the following connecting is below a certain period value. The control of at least the collection the or processing 23 of parameters is then at least based on the communication network 27 location where it was last connected.

According to this example, the ASS 10 learns 22 where the UE 14 is most likely to "reappear" after a brief (insignificant) period of disconnection based on the location where it was last connected. The word "reappear" is here used in a similar way as "appear". The purpose of the prefix "re" is to distinguish the situation where the UE has been "invisible" for the ASS for a limited period (below a certain period value) of time from the situation where

the UE has been "invisible" for a significant period (exceeds a certain period value) of time. The former case implies that the UE probably has not moved very long from the location where it was last "visible" for the ASS, whereas in the latter case the UE has had ample time to move even to locations far a way from the one where it was last "visible".

For instance, if the UE 14 was last disconnected from the communication network 27 in location α, then the ASS may have learnt 22 that if the UE connects to the communication network again within a certain limited period of time (implying a limited movement), it is likely to do this in location β (which may well be the same as location α). The definition of "location" in this context is the same as above. A more concrete or precise example could be that if a disconnected UE was last connected in cell X of access network A, then the ASS may have learnt that if the UE reconnects to the communication network within a certain limited period of time, then it will usually do this in cell Y in access network A with access networks B and C also within reach.

This means that when the UE 14 disconnects from cell X of access network A then, unless it is a handover, the ASS 10 starts at least collecting or processing 23 relevant parameters from access networks A (with focus on cell Y if applicable), B and C in order to be able to support quick access selection 26 if the UE 14 reappears (reconnects) as expected. However, if it takes too long before the UE reconnects, the ASS starts at least collecting or processing information according to the principles described above for the case where the UE is disconnected from the communication network 27 during a significant period of time, i.e. from the "location(s)" where the UE most commonly appears after a significant period of disconnection. Thus, the knowledge learnt in this way allows the ASS to proactively at least collect or process parameters that are relevant for access selection 26 during connection(s) in certain situations.

In accordance with one alternative of how the ASS 10 receives 23 information about the communication network 27 location of the UE, it gets information about the communication network location of the UE 14 explicitly. This means that the UE informs the ASS of its communication network location whenever it arrives in a location. The explicit information is the most important. The UE informs the ASS of its location with the detail/granularity needed, e.g. access network, cell, zone, access point, domain name, geographical data etc., whenever it arrives in a location (manifested as connection, handover, movement in idle mode or "camping" state). If the UE moves in a mode in which it is not configured for IP communication, IP configuration is required before explicitly informing the ASS of a new location. It may be argued that it is not beneficial to go to such lengths merely to inform the ASS of the new location of the UE, but it is at least a possible option.

In accordance with another alternative of how the ASS 10 receives information about the communication network 27 location of the UE 14, the ASS gets information about the network location of the UE implicitly. This means that the UE contacts the ASS for other purposes than to inform about its communication network location, during which contact the UE reveals its Internet Protocol address to the ASS.

In another alternative of how the ASS 10 receives information about the communication network 27 location of the UE it is also possible that the ASS can retrieve location information from other entities that possess knowledge about the location of a UE, such as a SIP proxy, a Mobile IP Home Agent, a AAA server or a HSS.

Within one embodiment of the present invention the Uniform Resource Identifier (URI) of an access network's local network profile is sent by the UE 14 to the ASS 10 when being connected to the communication network 27. The URI may be delivered to a UE in Dynamic Host Configuration Protocol (DCHP) option 15 during the DCHP configuration procedure. In some cases

it is possible that the relevant information cannot be located without prior information that is only available through scanning 18, see figure 1, or by connecting to a certain access link. One example is this retrieval of a local network profile located through a URI that is delivered in DHCP option 15. Since DHCP relies on link-local mechanisms like broadcast, this URI can only be retrieved by a device connected to the concerned access network. In cases like this, the UE will transfer to the ASS 10 the information that is required to locate certain relevant information, e.g. in the form of a URI for a local network profile or a domain name for information in general.

The UE 14 will do this opportunistically, i.e. any time that the UE has contact with the ASS 10 and concerning any information that may potentially be relevant for the ASS to retrieve. Out of the information of this type that the ASS receives from the UE, it may choose to retain only a selected part that turns out to be useful within a reasonable time. In other words, information of this type that the ASS does not use is eventually timed out and deleted.

Within one embodiment of the present invention the UE 14 subscribes to certain events from the ASS 10. The ASS continuously monitors the information sources that are relevant for the subscribed events and when a criteria for a subscribed event is fulfilled the ASS sends a notification to the UE. Such events may e.g. be changes in policies, Quality of Service support or load. The ASS continuously monitors the information sources that are relevant for the subscribed events and when the criteria for a subscribed event are fulfilled, the ASS sends a notification to the UE.

The sending and/or forwarding 25 of information are preferably controlled by the ASS 10. The access selection information is preferably sent/forwarded to the UE 14 through the interface 20. The access selection information is not available through scanning from the UE.

The notion of the ASS controlling the sending and/or forwarding 25 of information may constitute that the ASS determines which information and/or

which type of information that is appropriate to send/forward to the UE in each particular situation.

The notion of the ASS controlling the sending and/or forwarding 25 of information may also constitute that the access selection information is sent and/or forwarded 25 to the UE when requested by the UE. Such a request is sent when the UE is again connected to the communication network 27. The request may optionally be sent immediately when the UE connects to the communication network. The request is sent via a communication interface 19 between the ASS and the ASC. Figure 2 illustrates this alternative.

Proactively collected 23 parameters (as well as more reactively collected parameters) are typically transferred 25 to the UE 14 on request 24, i.e. the UE retrieves the access selection information from the ASS 10. When an access selection 26 situation arises in the ASC 21 in the UE 14 and the decision requires input data that can beneficially (or only) be collected by the ASS 10, then the UE requests the ASS to at least collect or process the concerned parameters and transfer it as access selection information to the UE.

If the ASS's adaptive, proactive behaviour has been successful and the requested 24 parameters consequently are already at least collected or processed 23, then the ASS can transfer 25 it as access selection information to the UE immediately. Otherwise, the ASS has to collect or process 23 the requested parameters before it can transfer 25 it to the UE. From the UE's point of view these two situations differ only in how quick the UE receives the requested access selection information from the ASS.

There are two major cases of access selection 26 in the context of the UE requesting access selection information from the ASS 10. In one case the UE 14 requests 24 the access selection information from the ASS via anyone of the access networks 13 that the UE is connected to. This for instance relate to access selection 26 for handover of a connection or access selection 26

for a new connection request from an application when the UE is already connected. If the UE is connected to one or more access network(s) when the access selection situation arises, it can use any one of the connected accesses to send its request 24 for access selection information to the ASS.

The other case relates to access selection when the UE is not connected to an access network, e.g. for access/cell selection in idle mode (also known as access selection for "camping") or access selection for a connection (socket) request from an application when the terminal is disconnected/idle.

If the UE 14 is not connected to an access network 13 when the access selection situation arises, it has to connect to one of the available access networks before requesting 24 the information from the ASS. Which one of the available accesses to choose for this communication may be governed by default policies (with information retrieved through scanning as input data, possibly enhanced with old, cached contextual data, such as application usage history and additional information about the discovered access networks). If the access selection 26 is only for idle mode (in the sense that no IP configuration is required) then it may not be considered worthwhile to connect to an access network (going through authentication and IP configuration etc.) merely to be able to retrieve information from the ASS and consequently it is an option to rely only on information that can be retrieved through scanning or from within the terminal in such situations.

The notion of the ASS controlling the sending and/or forwarding 25 of information may finally constitute in that the ASS (10) sends and/or forwards the access selection information to the UE (14) after receiving an indication from another network entity that the UE has connected to one of the available access networks. The ASS consequently transfers access selection information to the UE without a prior request, when it receives an indication from another network entity, e.g. an AAA server that the UE has connected to the communication network 27 (provided that the ASS has a means to appropriately address the UE with this information transfer).

Figure 3 shows a signalling diagram illustrating the Access Selection functionality according to the present invention. When the UE 14 is disconnected D from the communication network 27, the ASS 10 checks 1 historical records, statistics etc. in order to control at least the collection or processing of parameters. The ASS further requests 2 and receives 3 network-based information from the network based entity X 11 and receives 4 unsolicited network-based information from the network-based entity Y 12Y 12. The communication nodes X and Y may for instance be databases, profile servers, Authentication/Authorization and Accounting (AAA) server, Home Subscriber Server (HSS), Session Initiation Protocol (SIP) proxies, Home Agents etc.

When the UE 14 again connects C to for instance access node 1 (AN (1)) 13 it sends 5 location information and a request for access selection information to the ASS. The ASS 10 sends 6 back such information to the ASC 21 in the UE. Then ASC in the UE then processes 7 the access selection information.

Depending on the outcome of the processing 7 by the UE, certain actions 8 are performed. As a possibility the UE connects 8A to access node 2 (AN(2)) 13 and possibly disconnects 8B from AN(1) 13.

It will also be appreciated by a person skilled in the art that various modifications may be made to the above-described embodiments without departing from the scope of the present invention.

CLAIMS

1. A method for network access selection (26) in a communication network (27) comprising an Access Selection Server (ASS) (10), at least one User Equipment (UE) (14), an Access Selection Client (ASC) (21) being arranged in the UE (14) and communication nodes (11,12),

the ASS (10) collecting (23) access selection parameters used for the selection (26) of access network for the network access for the UE (14) in a multi-access environment

the network access enabling a traffic bearer for a traffic flow between an application in the UE (14) and a first node,

the ASS (10) forwarding (25) the access selection parameters and/or processing (23) the access selection parameters and sending (25) the results of the processed parameters to the UE,

the parameters forwarded or the results sent (25) by the ASS (10) being access selection information based on which the ASC (21) performs (26) activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow ,

characterized in that

the ASS (10) controls at least the collection or the processing (23) of the access selection parameters, the collection or the processing (23) at least being performed when the UE (14) is disconnected from the communication network (27),

the parameters collected or processed (23) when the UE (14) is disconnected from the communication network (27) are forwarded (25) and/or the results of the processed parameters are sent as access selection

information by the ASS (10) to the UE (14) when the UE (14) is again connected to the communication network (27).

2. Method according to claim 1 wherein the control by the ASS of at least the collection or the processing (23) of parameters is based on contextual information, historical records and/or statistics from the records for the communication network (27) location of the UE (14).

3. Method according to claim 2 wherein an adaptive learning scheme being located in the ASS (10) controls at least the collection or the processing (23) of parameters.

4. Method according to any of the claims 2 - 3 wherein if the time period between the disconnecting and the following connecting exceeds a certain period value, the control of at least the collection or the processing (23) of parameters is at least based on:

contextual information on where in the communication network (27) the UE (14) is most likely to appear when connecting to the communication network (27), and

which access network or networks the UE can select from when connecting to the communication network (27).

5. Method according to claim 4 wherein the statistics is based in information about the selectable access network or networks (13).

6. Method according to any of the claims 2 – 5 wherein the control of at least the collection or the processing (23) of parameters is at least based on movement patterns that reoccurs frequently, the patterns being movement between communication network (27) locations.

7. Method according to any of the claims 2 - 6 wherein if the time period between the disconnecting and the following connecting is below a certain period value the control of at least the collection or the processing (23) of

parameters is at least based on the communication network (27) location where it was last connected.

8. Method according to any of the claims 2 - 7 wherein the ASS (10) gets information about the communication network (27) location of the UE (14) explicitly, in which the UE (14) informs the ASS (10) of its communication network (27) location whenever it arrives in a location.

9. Method according to any of the claims 2 - 7 wherein the ASS (10) gets information about the communication network (27) location of the UE (14) implicitly, in which the UE (14) contacts the ASS (10) for other purposes than to inform about its communication network (27) location, during which contact the UE (14) reveals its Internet Protocol address to the ASS (10).

10. Method according to any of the preceding claims wherein the access selection information is not available through scanning from the UE (14).

11. Method according to any of the preceding claims wherein a Uniform Resource Identifier (URI) of an access network's local network profile, is sent by the UE (14) to the ASS (10) when being connected to the communication network (27).

12. Method according to any of the preceding claims wherein the UE (14) subscribes to certain events from the ASS (10), the ASS (10) continuously monitoring the information sources that are relevant for the subscribed events and when a criteria for a subscribed event is fulfilled the ASS (10) sends a notification to the UE (14).

13. Method according to any of the preceding claims wherein the access selection information is sent and/or forwarded (25) to the UE when requested (24) by the UE .

14. Method according to any of the preceding claims wherein the UE (14) requests (24) the access selection information from the ASS (10) via any of the access networks (13) that the UE (14) is connected to.

15. Method according to any of the preceding claims wherein the ASS (10) sends and/or forwards the access selection information after receiving an indication from another network entity that the UE has connected to one of the available access networks.

16 Access Selection Server (ASS) (10) being adapted for network access selection (26), the ASS (10) being arranged in a communication network (27) further comprising at least one User Equipment (UE) (14), an Access Selection Client (ASC) (21) being arranged in the UE (14) and communication nodes (11,12),

the ASS (10) further is adapted to collect (23) access selection parameters used for the selection (26) of access network for the network access for the UE (14) in a multi-access environment,

the network access enabling a traffic bearer for a traffic flow between an application in the UE (14) and a first node,

the ASS (10) further is adapted to forward (25) the access selection parameters and/or process (23) the access selection parameters and send (25) the results of the processed parameters to the UE,

the parameters forwarded or the results sent (25) by the ASS (10) being access selection information based on which the ASC (21) performs activation (26) of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow,

characterized in that

the ASS (10) is further adapted to control at least the collection or the processing (23) of the access selection parameters,

the ASS is further adapted to perform the collection or the processing (23) at least when the UE is disconnected from the communication network (27),

the ASS (10) is further adapted to, when the UE (14) is again connected to the communication network (27), forward (25) the parameters, collected or processed (23) when the UE (14) is disconnected from the communication network (27), and/or send the results of the processed parameters, as access selection information to the UE (14).

17. The ASS (10) according to claim 16 wherein the ASS is adapted to perform the control of at least the collection or the processing (23) of parameters on the basis of contextual information, historical records and/or statistics from the records for the communication network (27) location of the UE (14).

18. The ASS (10) according to claim 17 wherein an adaptive learning scheme located in the ASS (10) is adapted to control at least the collection or the processing (23) of parameters.

19. The ASS (10) according to any of the claims 17 - 18 wherein the ASS (10) is adapted to get information about the communication network (27) location of the UE (14) explicitly, in which the UE (14) informs the ASS (10) of its communication network (27) location whenever it arrives in a location.

20. The ASS (10) according to any of the claims 17 – 18 wherein the ASS (10) is adapted to get information about the communication network (27) location of the UE (14) implicitly, in which the UE (14) contacts the ASS (10) for other purposes than to inform about its communication network (27) location, during which contact the UE (14) reveals its Internet Protocol address to the ASS (10).

21. The ASS (10) according to any of the claims 16 – 20 wherein the UE (14) subscribes to certain events from the ASS (10), the ASS (10) is further adapted to continuously monitor the information sources that are relevant for

the subscribed events, and when a criteria for a subscribed event is fulfilled the ASS (10) is further adapted to send a notification to the UE (14).

22. The ASS (10) according to any of the claims 16 - 21 wherein the ASS (10) is further adapted to send and/or forward (25) the access selection information to the UE when requested (24) by the UE .

23. The ASS (10) according to any of the preceding claims wherein the ASS (10) is further adapted to send and/or forward the access selection information after receiving an indication from another network entity that the UE has connected to one of the available access networks.

24. A communication network (27) for network access selection (26), the communication network (27) comprising an Access Selection Server (ASS) (10), at least one User Equipment (UE) (14), an Access Selection Client (ASC) (21) being arranged in the UE (14) and communication nodes (11,12),

the ASS (10) is adapted to collect (23) access selection parameters used for the selection (26) of access network for the network access for the UE (14) in a multi-access environment,

the network access enabling a traffic bearer for a traffic flow between an application in the UE (14) and a first node,

the ASS (10) is further adapted to forward (25) the access selection parameters and/or process (23) the access selection parameters and send (25) the results of the processed parameters to the UE (14),

the parameters forwarded (25) or the results sent (25) by the ASS being access selection information based on which the ASC (21) is adapted to perform (26) activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow,

characterized in that

the ASS (10) is further adapted to control at least the collection or the processing (23) of the access selection parameters,

the ASS is further adapted to perform the collection or the processing (23) at least when the UE (14) is disconnected from the communication network (27),

the ASS is further adapted to, when the UE (14) is again connected to the communication network (27), forward (25) the parameters collected or processed (23) when the UE (14) is disconnected from the communication network (27), and/or send the results of the processed parameters, as access selection information to the UE (14).

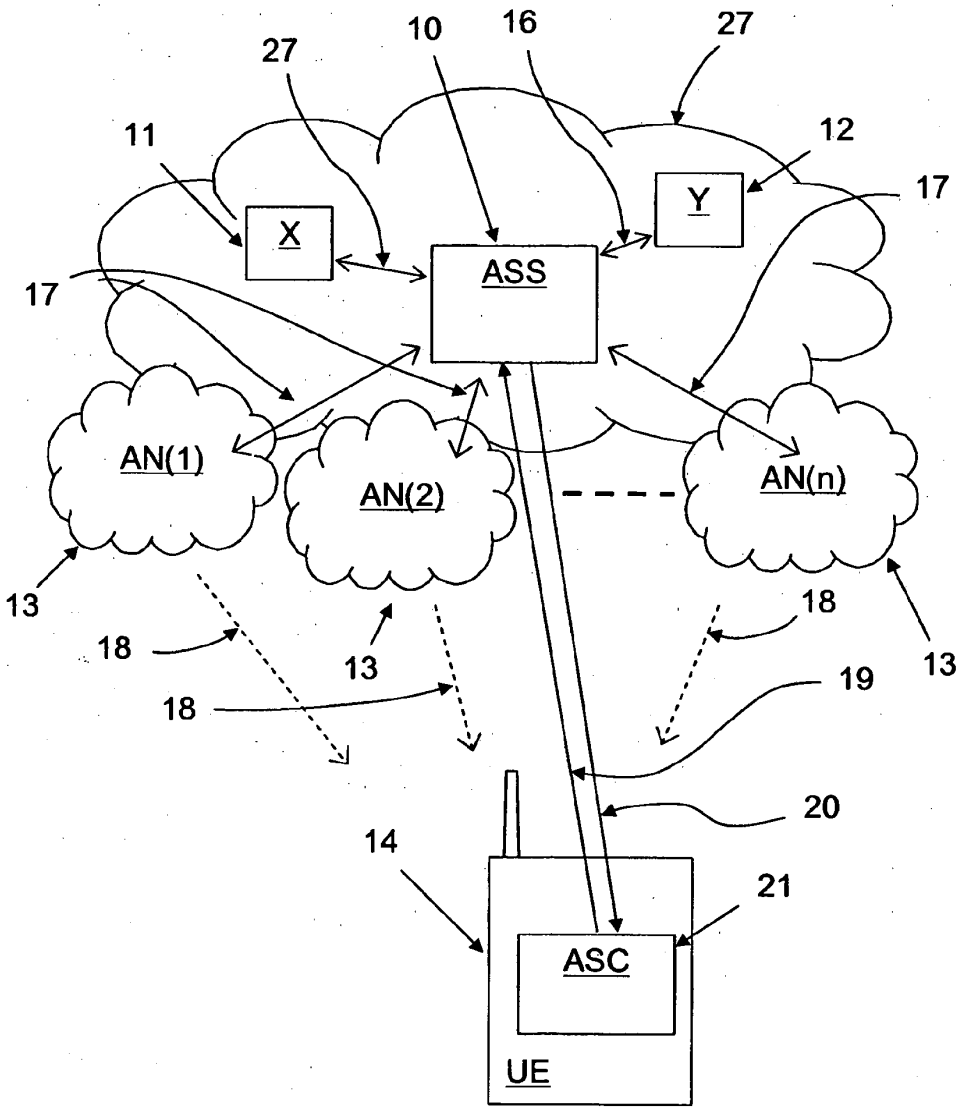

27
10
16
27
11
12
X
Y
17
ASS
17
AN(1)
AN(2)
AN(n)
13
18
13
18
13
18
19
20
14
21
ASC
UE

FIG 1

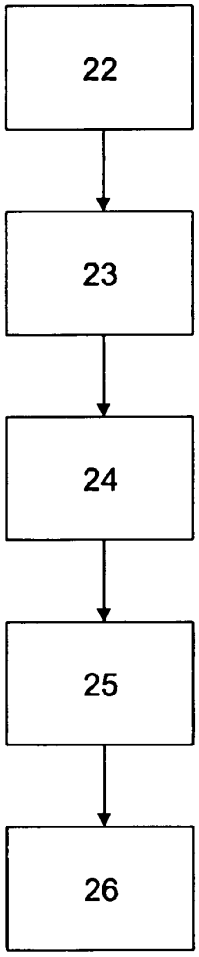


FIG 2

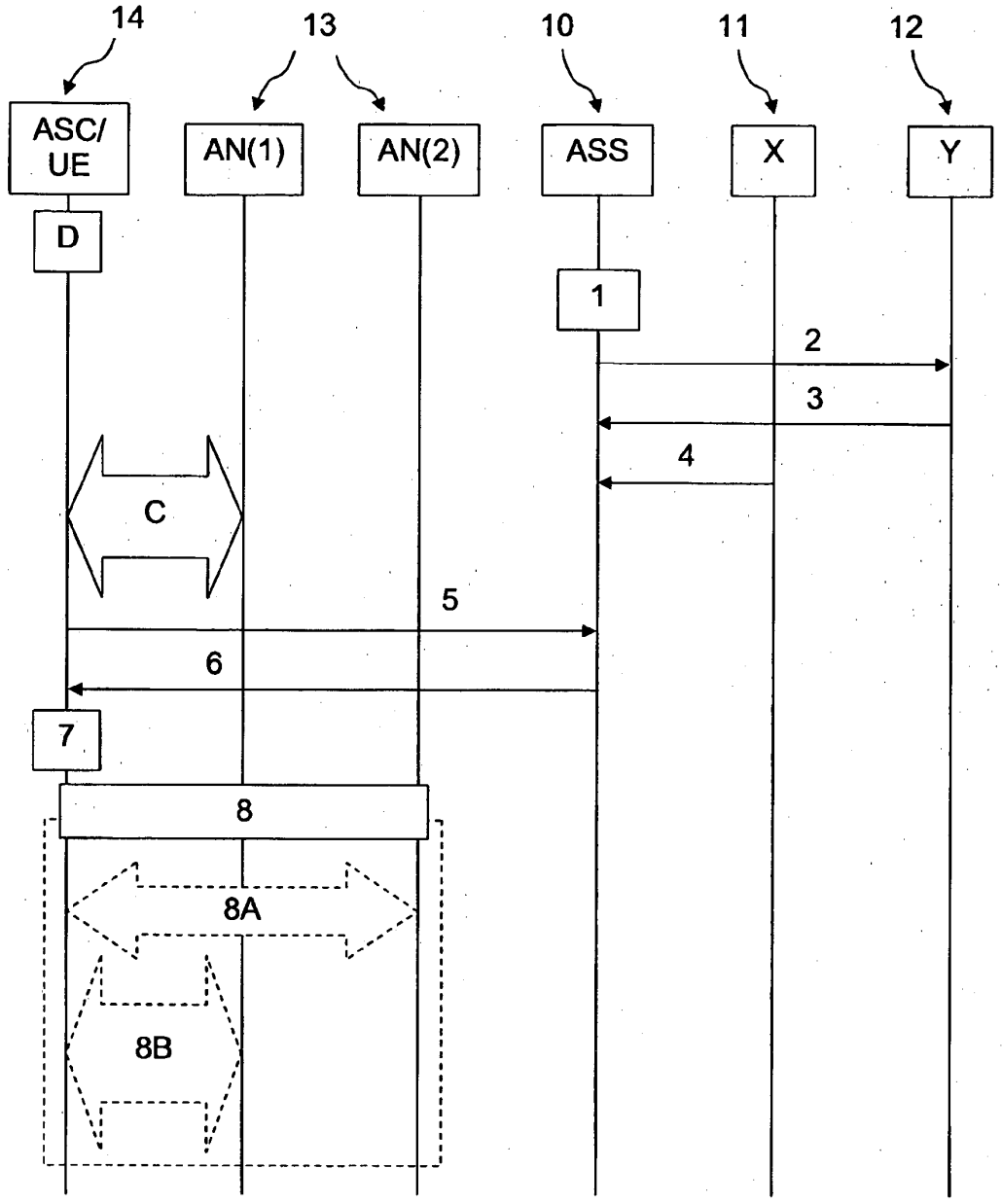


FIG 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000031

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005117463 A2 (NOKIA CORP.), 8 December 2005 (08.12.2005), figures 1-5, claims 1-26, paragraphs [0009] - [0041] --	1-24
A	XP005333980, Kaloxylos et al, "A flexible handover mechanism for seamless service continuity in heterogeneous environments", 20060331 ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL VOL - 29 NR - 6 PG - 717 - 729 See the whole document --	1-24

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 October 2008	06-11-2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Elisabet Åselius/PR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

BNSDOCID: <WO_____2009091295A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000031

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	WO 2008043970 A1 (FRANCE TELECOM), 17 April 2008 (17.04.2008), page 1, line 7 - page 5, line 15, figures 1-4, claims 1-10, abstract ---	1-24
A	US 20040218605 A1 (GUSTAFSSON ET AL), 4 November 2004 (04.11.2004), figures 1-8, claims 1-29, abstract, paragraphs [0013] - [0018] ---	1-24
A	WO 2006103402 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY), 5 October 2006 (05.10.2006), page 1, line 25 - page 2, line 35, figures 1-4, claims 1-13, abstract --- --------	1-24

Form PCT/ISA/210 (continuation of second sheet) (July 2008)

International patent classification (IPC)
H04Q 7/38 (2006.01)
H04Q 7/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **GLZJVOXTPZ.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

WO	2005117463	A2	08/12/2005	AU	2005330571	A	07/12/2006
				CN	1957634	A	02/05/2007
				EP	1749419	A	07/02/2007
				JP	2008500756	T	10/01/2008
				US	20080064393	A	13/03/2008
WO	2008043970	A1	17/04/2008	NONE			
US	20040218605	A1	04/11/2004	NONE			
WO	2006103402	A1	05/10/2006	EP	1708526	A	04/10/2006
				EP	1864533	A	12/12/2007

BNSDOCID: <WO_____2009091295A1_I_>

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2002 (21.11.2002)

PCT

(10) International Publication Number
WO 02/093877 A1

(51) International Patent Classification[7]: H04M 1/00, 3/00, 3/42, 11/10, H04B 1/38

(21) International Application Number: PCT/IB02/01550

(22) International Filing Date: 7 May 2002 (07.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/854,628 15 May 2001 (15.05.2001) US

(71) Applicants: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: **NYKÄNEN, Petri**; Lehdokkikatu 3, FIN-37120 Nokia (FI). **PALONIEMI, Jari**; Yliki-imingintie 169, FIN-90900 Kiiminki (FI). **KANGAS, Petri**; Pölkkytie 7A3, FIN-90800 Oulu (FI).

(74) Agent: **HOEL, John**; Morgan & Finnegan, LLP, 345 Park Avenue, New York, NY 10154 (US).

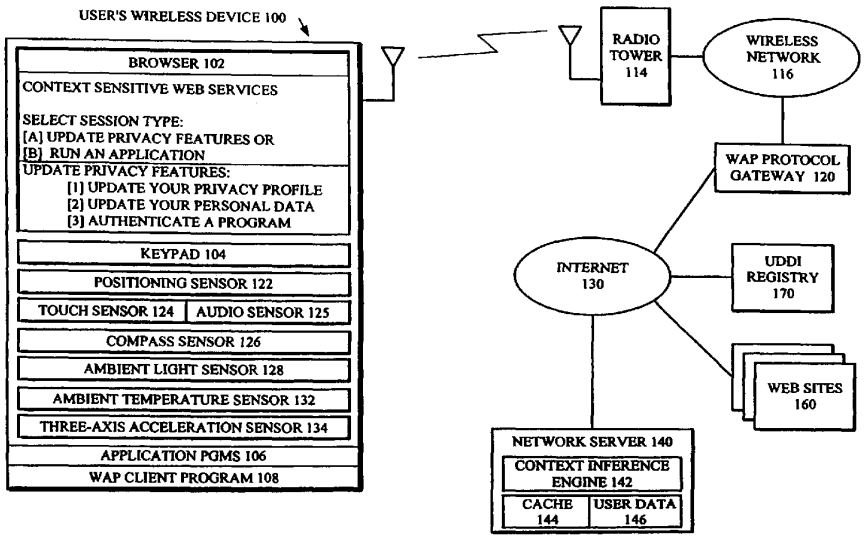
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: CONTEXT SENSITIVE WEB SERVICES



(57) Abstract: The context sensitive web services method enables a mobile phone or wireless device (100) to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. The method includes the steps of receiving sensor signals (122-134) characterizing a current environment of the wireless device (100); processing the sensor signals with a context inference engine (142); outputting a current context result from the processing by the context inference engine (142); and providing useful information to the user in response to the current context result.

WO 02/093877 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTEXT SENSITIVE WEB SERVICES

This application claims priority to U.S. Application Serial No. 09/857,628, filed May 15, 2001, entitled, "Context Sensitive Web Services, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention:

The invention disclosed broadly relates to methods for providing Internet services and more particularly relates to improvements in mobile device accessing of Internet services.

Background Art:

Mobile phones and wireless personal digital assistants (PDAs) are able to access the Internet using the Wireless Application Protocol (WAP). WAP-enabled wireless devices can now access Internet applications such as headline news, exchange rates, sports results, stock quotes, weather forecasts, multilingual phrase dictionaries, personal online calendars, online travel and banking services, or download distinctive ringing tones. Broadband wireless networks make it possible for WAP-enabled wireless devices to exchange multimedia messages that combine conventional text with much richer content types, such as photographs, images, voice clips, and video clips. WAP-enabled wireless devices can be used to pay bills online using the wireless device as a virtual wallet. WAP-enabled wireless devices can deliver useful and informative advertising and transaction services from online merchants. WAP-enabled wireless devices now also provide entertainment services, such as interactive adventure games, quizzes, and chess tournaments.

What is needed is the ability of a mobile phone or wireless PDA to use context inference techniques to sense the mobile user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. It would be even more useful to offload some of the computationally intensive computing necessary in context inference techniques, from the mobile user's wireless device to a server and to web sites on the Internet. It would be beneficial to maintain a personal

CONFIRMATION COPY

profile of the mobile user's personal preferences in an online server or web site. It would be important to provide the mobile user with the ability to control any access to the user's profile by the online server or web site.

SUMMARY OF THE INVENTION:

The context sensitive web services invention enables a mobile phone or wireless PDA to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment.

One aspect of the invention is a method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment. The method includes the steps of receiving sensor signals characterizing a current environment of the wireless device; processing the sensor signals with a context inference engine; outputting a current context result from the processing by context inference engine; and providing useful information to the user in response to the current context result. The processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device. In another aspect of the invention, the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device. The server can access files from a web server, for selective forwarding to the user's wireless device. A personal profile of the user can be maintained by the server.

A further aspect of the invention provides user control of access by application programs to the user's private data. This can also include providing user control of access by application programs to the user's private data in the server. Still further, this can also include providing user control of access by application programs in a web server, to the user's private data.

Another aspect of the invention is providing the current context result to an application program in response to the user control and receiving the useful information from the application program. The invention enables the user to grant access permission to the application program to access the current context result. This can be performed in

the user's wireless device or in the network server. The network server can carry out the control of access by application programs in web servers, in response to a user privacy profile received from the user's wireless device.

DESCRIPTION OF THE FIGURES:

Figure 1 is a network diagram of the invention, showing an example relationship between the user's Wireless Application Protocol (WAP)-enabled portable wireless device, the WAP protocol gateway to the Internet, the network server, the Universal Description, Discovery and Integration (UDDI) registry, and a plurality of web sites.

Figure 1A shows the user's wireless device with the UPDATE PRIVACY FEATURES: sub-menu of the Context Sensitive Services menu, enabling the user to UPDATE YOUR PRIVACY PROFILE or UPDATE YOUR PERSONAL DATA.

Figure 1B shows the user's wireless device with the UPDATE PRIVACY FEATURES: sub-menu of the Context Sensitive Services menu, enabling the user to AUTHENTICATE A PROGRAM and REGISTER A PROGRAM.

Figures 1C and 1D show the user's wireless device with the RUN AN APPLICATION sub-menu of the Context Sensitive Services menu, enabling the user to RUN AN APPLICATION.

Figure 2 is a functional block diagram of the wireless device 100, showing its various components and programs.

Figure 2A is a functional block diagram of the wireless device 100, the server 140, and the web server 160, and their interaction when exchanging a metadata vector 138 and privacy control data 150.

Figure 3 is a network process flow diagram of the interaction of the wireless device 100, network server 140, and web server 160 when carrying out the determination of the current context of the wireless device 100.

Figure 4 is a functional block diagram of the network server 140, showing the memory storing the application services software programs needed to perform the operations of the invention.

DISCUSSION OF THE PREFERRED EMBODIMENT:

The context sensitive web services invention enables a mobile phone or wireless PDA to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. The invention offloads some of the computationally intensive computing necessary in context inference techniques, from the mobile user's wireless device to a server and to web sites on the Internet. The context sensitive web services invention maintains a personal profile of the mobile user's personal preferences in an online server or web site. The mobile user is provided with the ability to control access by application programs in the wireless device, to the user's private data. The context sensitive web services invention provide the mobile user with the ability to control any access to the user's profile by the online server or web site.

The mobile user's wireless device is equipped with a context inference engine for providing and awareness of the mobile user's context to application programs, including third party applications. Since the processing power and storage capacity is limited in typical wireless devices, the computational load and storage requirements of the context inference engine are distributed to a context inference server capable of processing the context data. The invention enables the mobile user to control which application programs in the wireless device are granted access to the user's private context information. A privacy control block in the wireless device grants or revokes access by application programs to the private context information, based on the mobile user's preferences stored in a privacy profile. The same privacy control and privacy profile is extended to the context inference server, thereby enabling the extension of the user's privacy control to any web server connected to the context inference server. The invention thus enables building an infrastructure for context sensitive applications and services within the wireless device and the server, while providing to the mobile user control over the privacy user's context information.

The invention is applied to wireless telephones and wireless personal digital assistants (PDAs) implementing the Wireless Application Protocol (WAP) standard. Figure 1 is a network diagram of an embodiment of the invention, showing an example relationship between the user's Wireless Application Protocol (WAP)-enabled portable wireless device 100, a WAP protocol gateway 120, and the server 140. The user's WAP-enabled portable wireless device 100 can be a wireless mobile phone, pager, two-way

radio, smartphone, personal communicator, or the like. The user's WAP-enabled portable wireless device 100 accesses a small file called a deck which is composed of several smaller pages called cards which are small enough to fit into the display area of the device's microbrowser 102. The small size of the microbrowser 102 and the small file sizes accommodate the low memory constraints of the portable wireless device 100 and the low-bandwidth constraints of a wireless network 116. The cards are written in the Wireless Markup Language (WML) which is specifically devised for small screens and one-hand navigation without a keyboard. The WML language is scaleable from two-line text displays on the microbrowser 102 of a cellular telephone, up through large LCD screens found on smart phones and personal communicators. The cards written in the WML language can include programs written in WMLScript, which is similar to JavaScript, but makes minimal demands on memory and CPU power of the device 100 because it does not contain many of the unnecessary functions found in other scripting languages.

The Nokia WAP Client Version 2.0 is a software product containing the components necessary to implement the WAP client 108 on the wireless device 100. These components include a Wireless Markup Language (WML) Browser, WMLScript engine, Push Subsystem, and Wireless Protocol Stack. The Nokia WAP Client is a source-code product that can port and integrate into wireless devices such as mobile phones and wireless PDAs. Application programs 106 stored in the wireless device 100 interact with the WAP Client 108 to implement a variety of communications applications. Details of the Nokia WAP Client Version 2.0 can be found in the online paper: Nokia WAP Client Version 2.0, Product Overview, Nokia Internet Communications, 2000, www.nokia.com/corporate/wap.

The WAP Client 108 includes the Wireless Public Key infrastructure (PKI) feature, providing the infrastructure and the procedures required for authentication and digital signatures for servers and mobile clients. Wireless PKI is a certificate-based system that utilizes public/private key pairs associated with each party involved in a mobile transaction. Wireless Identity Module (WIM) is a security token feature of the WAP Client 108, which includes security features, such as the public and private keys and service certificates, needed for user authentication and digital signatures. Additionally, it has the ability to perform cryptographic operations to encrypt and decrypt messages.

The wireless device 100 of Figure 1 also has a plurality of sensors for sensing the mobile user's ambient conditions. The sensors shown include POSITIONING SENSOR 122, TOUCH SENSOR 124, AUDIO SENSOR 125, COMPASS SENSOR 126, AMBIENT LIGHT SENSOR 128, AMBIENT TEMPERATURE SENSOR 132, and THREE-AXIS ACCELERATION SENSOR 134. The audio sensor 125 can be a microphone, for example, which can detect speech or environmental sounds. The positioning sensor can be, for example, a GPS receiver integrated in the device. The positioning sensor can also be, for example, a radio beacon triangulation sensor that determines the location of the wireless device by means of a network of radio beacons, base stations, or access points, as is described for example, in Nokia European patent EP 0 767 594 A2, entitled "Mobile Station Positioning System". These sensors provide inputs which are sampled by the wireless device 100 to infer a current context, as will be described below.

The WAP protocol gateway 120 links the Internet 130 and the wireless network 116. The WAP protocol gateway 120 includes the Wireless Public Key infrastructure (PKI) feature to help provide a secure Internet connection to the wireless device 100. The WAP protocol gateway 120 enables the WAP-enabled wireless device 100 to access Internet applications such as headline news, exchange rates, sports results, stock quotes, online travel and banking services, or to download distinctive ringing tones.

The user's WAP-enabled portable wireless device 100 communicates with the radio tower 114 and can exchange messages for distances up to several kilometers. The types of wireless networks 116 supported by the WAP standard include Cellular Digital Packet Data (CDPD), Code-Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), Time Division Multiple Access (TDMA), GPRS, 3G-Broadband, and the like.

The overall process of communication between the user's WAP-enabled wireless device (the client) 100, through the WAP protocol gateway 120, to the server 140 resembles the way Web pages are served on the Internet using the HyperText Transfer Protocol (HTTP) or World Wide Web protocol:

[1] The user presses a phone key on the user's device 100 related to the Uniform Resource Locator (URL) of the server 140.

[2] The user's device 100 sends the URL, via the radio tower 114 and the wireless network 116, to the gateway 120 using WAP protocols.

[3] The gateway 120 translates the WAP request into an HTTP request and sends it over the Internet 130 to the server 140, via Transmission Control Protocol/ Internet Protocol (TCP/IP) interfaces.

[4] The server 140 handles the request just like any other HTTP request received over the Internet. The server 140 either returns a WML deck or a HyperText Markup Language (HTML) page back to the gateway 120 using standard server programs written, for example in Common Gateway Interface (CGI) programs, Java servlets, or the like.

[5] The gateway 120 receives the response from the server 140 on behalf of the user's device 100. If the response is an HTML page, it gets transcoded into WML if necessary. Then the WML and WMLScript coding is encoded into a byte code that is then sent to the user's device 100.

[6] The user's device 100 receives the response in the WML byte code and displays the first card in the deck on the microbrowser 102 to the user.

In Figure 1, the protocol gateway 120 includes a WAP protocol stack organized into five different layers. An application layer is the wireless application environment, which executes portable applications and services. A session layer is the wireless session protocol, which supplies methods for the organized exchange of content between client/server applications. A transaction layer is the wireless transaction protocol, which provides methods for performing reliable transactions. A security layer is the wireless transport layer security, which provides authentication, privacy, and secure connections between applications. The transport layer is the wireless datagram protocol, which shelters the upper layers from the unique requirements of the diverse wireless network protocols, such as CDPD, CDMA, GSM, etc. Additional information about the WAP standard and the WAP protocol stack can be found in the book by Charles Arehart, et al. entitled, "Professional WAP", published by Wrox Press Ltd., 2000 (ISBN 1-861004-04-1).

In Figure 1, the user's portable wireless device 100 includes the microbrowser 102 displays the Context Sensitive Services menu, to enable the user to navigate through the cards being displayed and to select options that are programmed by the application

programs 106. The user's device 100 also includes the WAP client program 108 which has been previously discussed.

The Context Sensitive Services menu displayed by the microbrowser 102 in Figure 1 is rendered by the WAP client program 108 under the control of the application programs 106, which are shown in Figures 2 and 2A. The user can select the session type with Context Sensitive Services menu, either [A] UPDATE PRIVACY FEATURES or [B] RUN AN APPLICATION. If the UPDATE PRIVACY FEATURES session type is selected by the user, the Context Sensitive Services menu of Figure 1 then presents to the user the UPDATE PRIVACY FEATURES sub-menu from which the user can select the following options:

[A] UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[2] UPDATE YOUR PERSONAL DATA
[3] AUTHENTICATE A PROGRAM

Option [1] of UPDATE YOUR PRIVACY PROFILE, leads to a second sub-menu shown in Figure 1A, which has the following options:

[1] UPDATE YOUR PRIVACY PROFILE
[a] Add a local program to permissions list
[b] Remove a local program from list
[c] Add a server program to permissions list
[d] Remove a server program from list
[e] Add a network program to permissions list
[f] Remove a network program from list.

Option [2] of UPDATE YOUR PERSONAL DATA, leads to a another sub-menu shown in Figure 1A, which has the following options:

[2] UPDATE YOUR PERSONAL DATA
[a] Update server database
[b] Update network database.

Option [3] of AUTHENTICATE A PROGRAM, leads to a another sub-menu shown in Figure 1B, which has the following options:

[3] AUTHENTICATE A PROGRAM
[a] Request program's public key certificate
[b] Verify certificate signatures

[c] Verify validity time
[d] Verify revocation status
[e] Check if certificate authority on trust list
[f] Flag program as authenticated.

The AUTHENTICATE A PROGRAM option calls the privacy control 150 of the wireless device 100 in Figure 2. If an application program A, B, X, or Y has been verified for its acceptability by a trusted authority, then the trusted authority will have issued a digital certificate on a message authentication code (MAC) it has computed for the application program, which can be checked by the privacy control 150. As long as the privacy control 150 trusts the trusted authority issuing the digital certificate, authentication of the application program is straight forward.

Once the mobile user has verified the program's digital certificate and is satisfied that the application program will not subvert the integrity or security of the user's private data, the user can register the program. Registration is the granting by the user of access permission to the program, to access the current context of the user's wireless device and/or to access other portions of the user's private data. There are several levels of permission that can be granted by the user in two categories, [a] when can the accesses take place and [b] what data can be accessed.

Option [4] of REGISTER A PROGRAM, leads to a another sub-menu shown in Figure 1B, which has the following options:

[4] REGISTER A PROGRAM
[a] When can the accesses take place
[b] What data can be accessed

For the first category of [a] when can the accesses take place, the highest level of permission in this category is that access can occur anytime and without notice. The lowest level of permission in this category is that access can only occur at specified times or under specified conditions, and only after notice to the user and specific authorization by the user. For the second category of [b] what data can be accessed, the highest level of permission in this category is to access unlimited datasets in the user's private data, including current context information, personal data entered by the user, the user's Internet usage history data, the user's Internet cookie data, and the user's application program usage data. The lowest level of permission in this category is that access of any data can

only occur after notice to the user and specific authorization by the user. The user can configure any levels of permission in between the highest and lowest and make that the basis for the registration. The user can include the terms of registration in a digital certificate signed by the user and appended to the application program. This registration certificate can be presented by the program to the privacy control 150 prior to a proposed access event, the privacy control 150 to automatically verify the registration status of the program. The registration certificate can be constructed as follows.

The privacy control 150 can compute a message authentication code (MAC) and its own digital signature and append it as a certificate to an acceptable application program A, B, X, or Y. The privacy control 150 can include the terms of registration in the digital certificate. Then when the program requests access to the user's private data, the privacy control 150 can automatically check the MAC and its own digital signature to verify that the program has not been changed and the privacy control 150 can also automatically verify the registration status of the program. This is achieved by the privacy control 150 computing a hash value for the entire application program A, B, X, or Y (or some portion of it) and the terms of registration, and then forming a message authentication code (MAC) from the hash value. The privacy control 150 then uses its PKI private key to digitally sign the message authentication code (MAC). The terms of the registration, the MAC and the privacy control's digital signature are appended to the application program A, B, X, or Y as a registration certificate.

Then, whenever the application program A, B, X, or Y requests access to the user's context data or private data, the privacy control 150 will require the application program to present the registration certificate so that the privacy control 150 can check that the presented MAC compares with a computed MAC and that the presented digital signature is genuine. The privacy control 150 can then automatically grant access permission to the application program, in accordance with the terms of the registration.

Methods to generate and evaluate message authentication codes to insure the integrity of data are described in the book by Stephen Thomas entitled "SSL and TLS", published by John Wiley and Sons, 2000. Two example algorithms for message authentication are RSA's Message Digest (MD5) and the Secure Hash Algorithm (SHA),

both of which are described in the book by Stephen Thomas. Another reference that goes into greater detail in its discussion of data integrity methods is the book by Bruce Schneier entitled "Applied Cryptography - 2nd Edition" published by John Wiley and Sons, 1996. Methods to generate and evaluate digital signatures to insure the source of the digital program are described in the book by Richard E. Smith entitled "Internet Cryptography", published by Addison Wesley, 1997.

What has been described here for the privacy control 150 in the wireless device 100, is equally applicable to the privacy control 164 in the network server 140 of Figure 2A. The privacy control 164 in the network server 140 can compute the message authentication code (MAC) and its own digital signature and append it, with the terms of the registration, as a registration certificate to an acceptable application program in the web server 160. Privacy control 164 has a cached copy 144 of the Privacy Profile 152 of the wireless device 100. This enables automatically processing the privacy check in the network Server 140 for access requests from web server 160. When the application program in the web server 160 requests access to the user's private data in the network server 140 or in the wireless device 100, the privacy control 164 in the network server 140 will require the application program in the web server 160 to present the registration certificate so that it can check the MAC and its own digital signature to verify that the application program has not been changed. The privacy control 164 can then automatically grant access permission to the application program in the web server 160, in accordance with the terms of the registration.

If the [B] RUN AN APPLICATION session type is selected by the user, the Context Sensitive Services menu of Figure 1C then presents to the user the RUN AN APPLICATION sub-menu from which the user can select the following options:

[1] MESSAGING
[a] exchange multimedia messages

[2] MOBILE COMMERCE
[a] personal online calendar
[b] exchange rates
[c] banking services
[d] pay bills online using virtual wallet
[e] useful and informative advertising

[f] online merchant transaction services

The Context Sensitive Services menu of Figure 1D presents to the user the RUN AN APPLICATION sub-menu from which the user can select the following options:

[3] ENTERTAINMENT
[a] headline news
[b] sports results
[c] stock quotes
[d] weather forecasts
[e] multilingual phrase dictionaries
[f] online travel
[g] download distinctive ringing tones
[h] interactive games

The RUN AN APPLICATION option calls one of the application programs A, B, X, or Y of the wireless device 100 in Figure 2.

Figure 2 is a functional block diagram of the wireless device 100, showing its various components and programs. The wireless device 100 has context sensitive applications A, B, X, and Y, either downloaded, or in firmware. The wireless device 100 does not need to utilize external functionality in the network for the initial sampling and digitization of the sensor inputs. The sampled and digitized values of the sensor inputs are POSITIONING METADATA 122', TOUCH METADATA 124', AUDIO METADATA 125', COMPASS METADATA 126', AMBIENT LIGHT METADATA 128', AMBIENT TEMPERATURE METADATA 132', and THREE-AXIS ACCELERATION METADATA 134'. The sampled and digitized values of the sensor inputs are loaded into a metadata vector 138.

Figure 2 shows the memory 202 of the wireless device 100, connected by the bus 204 to the keypad 104, the radio 206, the sensor interface 208, the central processor 210, and the display 212. The memory 202 stores programs which are sequences of executable instructions which, when executed by the processor 210, carry out the methods of the invention. The memory 202 stores the WAP client program 108, the context inference engine 136, the privacy control 150, the privacy profile 152, the context aware API 154, the motion/gesture API 156, the location API 158, and other APIs 162. The context inference engine 136 processes the metadata vector 138 to produce the current context.

Application programs 106 stored in the memory 202 include the application programs A and B which are part of the software system SS1, and the application programs X and Y which are contained in the execution environment "Exec. Env."

If sufficient computational power and storage capacity are available in the wireless device 100, further processing of the metadata vector 138 can take place in the context inference engine 136, toward the objective of producing the result of an inferred current context. However, if at some point in the computation, the context inference engine 136 needs the processing power or storage capacity available at the network server 140, the metadata vector 138 is sent from the wireless device 100 to the context inference engine 142 in the network server 140 of Figure 2A. The context inference engine 142 in the network server 140 can perform the required processing on the metadata vector 138 and then return it to the context inference engine 136 in the wireless device 100 for completion of the an inferred current context result. Alternately, the context inference engine 142 in the network server 140 can complete the required processing and then return the resultant inferred current context to the wireless device 100.

Figure 2 shows the architecture of a wireless device with support for context awareness. The context awareness is built on top of sensory information received from various types of sensors physically located in the handset shown in Figure 1. The sensors shown include POSITIONING SENSOR 122, TOUCH SENSOR 124, AUDIO SENSOR 125, COMPASS SENSOR 126, AMBIENT LIGHT SENSOR 128, AMBIENT TEMPERATURE SENSOR 132, and THREE-AXIS ACCELERATION SENSOR 134. The sensors can also be located in accessory-like phone covers or in a wireless accessory such as a Bluetooth enabled device. The sensors may also be located in the environment such as in the user's rooms or vehicles. Also the time duration of use of a phone and other available information can be used along with sensor data in context awareness services.

Figure 2 shows sensor data received from the sensors 122, 124, 125, 126, 128, 132, and 134 is processed by Context Inference Engine 136. The application programs A, B, X, or Y running in the wireless device 100, may optionally provide application data to the context inference engine 136, along with their request for current context. The context inference engine 136 can optionally process the sensor signals and the application data to

produce the current context. The context inference engine 136 then feeds the current context through various APIs 154, 156, 158, and 162 to application programs A, B, X, and Y. The application programs may register themselves at the Application Programming Interface 154 to receive current context or changes in the context. This enables context sensitivity in the application programs.

Figure 2 shows "native" application programs A and B which are executed in a first software system SS1 of the wireless device 100. The term "Software System" is used here for any environment with execution capability. This first software system may be proprietary or based on a commercially available real-time operating system, such as NOS, ISA, EPOC, JAVA, or WAP. Third party application programs X and are executed within an execution environment. This execution environment may limit the system capabilities available for the application programs, such as access to APIs (fixed, not dynamic behavior).

Figure 2 shows the mobile user's privacy control feature. The privacy control feature enables the user to designate which application programs are granted access to the context awareness APIs 154 to utilize the current context information produced by the context inference engine 136. All requests or registrations by application programs A, B, X, and Y to have access to the Context Inference Engine 136, must first go through the Privacy Control block 150. Privacy Control block 150 uses the user's security data check stored in the Privacy Profile 152 to grant access rights to the requesting application programs. The user controls the granting of access rights by means of the user's security data input by the user through the user interface. The user's security data includes permissions list 155, Public Key Infrastructure (PKI) certificates 157, PKI trusted authority trust list 159, and flags set by the user for those application programs that have been authenticated by the PKI procedures, data set 161. The user can update the user's security data with the UPDATE PRIVACY FEATURES menu displayed by the wireless device 100 shown in Figures 1A and 1B. Access might be granted to an application program based on its digital signature, which is a part of the system applications, or other means known in the art. It is also possible to provide a separate system-wide Privacy User Interface to the privacy control 150, which can be employed by the mobile user to set the privacy policies and to alert the mobile user that an application program is attempting to

register to receive the user's private context awareness information. The privacy control 150 and Privacy Profile 152 enable the mobile user to grant, deny, or revoke access, to grant access for a limited time, or to require an application program to always request registration before the user grants access.

In Figure 2, the Context Inference Engine 136 in the wireless device 100 makes inferences from all the sensor inputs based on where the wireless device is located by the mobile user. For instance the inferred current context of the device 100 may be "IN THE USER'S POCKET", when a certain set of sensors input a specific combination of signals having a specific value range. As an example, the resulting inference of the current context by the Context Interference Engine 136 could be expressed in XML language format as follows:

<Context Inference Engine in Device>

<device placement> pocket </ device placement>

<User Interface state> sleep mode </User Interface state>

< device location> in elevator 5 building 1 floor 2</ device location>

<API active actions> meeting starting on floor 3 room 322 </API active actions>

</Context Inference Engine in Device >

The Context Inference Engine 136 in the wireless device 100 can perform the context inference process with any of several methods. Different input information from the sensors can be weighted according to their relative value of importance appropriate for each environment condition or situation to be analyzed. Each sensor has it's own weight value. Alternatively, the weight values for each sensor for each environment condition can be learned from training sessions using, for example artificial neural networks (ANNs), self-organizing maps (SOMs), decision trees, fuzzy rule-based systems, or model-based systems such as Hidden Markov Modeling (HMM). Combinations of two or more of the alternate methods can be used, depending on the application.

The Context Inference Engine 136 can continuously adapt its weights through adaptive and continuous learning methods, where the user teaches the wireless device 100 new environment conditions and names them. Hidden Markov Modeling (HMM) can be

used, for example, to implement an adaptive and continuous learning method for the Context Inference Engine 136. Alternately, the wireless device 100 can be programmed to spontaneously recognize a changed scene by comparing it with known scenes. The user can teach the wireless device new environmental conditions and name them, using the adaptive and automatic learning capability of neural networks. Adaptive and continuous learning methods are computationally intensive and are appropriate candidates to place on the network server 140, which assists the wireless device 100, as discussed below.

The field of context inference has applied the principles of automated pattern recognition to processing diverse types sensor inputs. Speech recognition has been applied to processing speech signals and handwriting recognition has been applied to processing hand force and accelerometer signals. In the field of robotics, image recognition has been applied to processing digitized still and motion images, mechanical location recognition has been applied to processing laser and sonar range finder signals, and mechanical motion recognition to has been applied to processing inertial, acceleration, and heading signals. In the field of prosthetic devices, touch recognition has been applied to processing tactile sensor signals. In the field of medicine, automated diagnostic programs recognize various pathologies by processing bioelectric field signals, as well as the more traditional pulse, respiration rate, and body temperature signals. These diverse sensor signal recognition processes have the common feature that an initial training stage is conducted where sampled signals are equated with a statistical model for those signals.

The principles of automated pattern recognition for these diverse sensor inputs are exemplified by the techniques for recognizing speech patterns. A common technique used in speech recognition is Hidden Markov Modeling (HMM). The term "Hidden" refers to the probabilistic and not directly observable events which underlie a speech signal. HMM speech recognition systems typically use realizations of phonemes which are statistical models of phonetic segments having parameters that are estimated from a set of training examples. Models of words are made by chaining or linking appropriate statistical models of phonetic segments. The statistical models serve as standards which are to be matched with the unknown voice signals to be recognized.

Recognition of unknown voice signals requires sampling and digitizing the speaker's spoken phonemes. These digitized phonemes are then processed into metadata. The metadata is then compared with the standard statistical models of phonemes. The most likely matches are then the inferred speech recognition result.

Recognition consists of finding the most likely path through the set of word models for the input speech signal. HMM speech recognition decoding systems first need to be trained through an iterative process. The system must be exposed to training examples or words of a particular speaker's voice. A training word is analyzed to generate a framed sequence of acoustic parameters or statistical models. A valid or "good" recognition occurs when the most likely path through the set of word models for the training word results in recognizing the correct training word.

Some useful references discussing the principles of Hidden Markov Models are:

Rabiner, L. R., "A tutorial on hidden Markov models and selected applications in speech recognition", Proceedings of the IEEE, volume 77, number 2, 1989, pages 257-286.

Rabiner, L. R. and Juang, B. H., "An introduction to hidden Markov models", IEEE ASSP Magazine, January 1986, pages 4-15.

Fraser, Andrew M. and Dimitriadis, Alexis, "Forecasting Probability Densities by Using Hidden Markov Models with Mixed States", Time Series Prediction: Forecasting the Future and Understanding the Past, Addison-Wesley, editor Weigend, Andreas S. and Gershenfeld, Neil A., 1994.

Charniak, Eugene, Statistical Language Learning, MIT Press, Cambridge, Massachusetts, 1993.

To illustrate how Hidden Markov Modeling (HMM) can be extended beyond speech recognition, an example is given here for touch recognition. In the training stage for touch recognition, tactile sensor signals are input from touching a tactile transducer to a rough texture, such as for example sandpaper. The tactile sensor signals are transformed into a statistical model of the input signal. The statistical model is stored as a standard in a computer memory under the handle "rough_texture". To expand the range of sensor signals that are included in the model for "rough_texture", several training

sessions can be conducted, each with a different direction or pressure for touching the sandpaper, resulting in several different samples of the statistical model. The set of samples of the statistical model are stored as a standard under the handle "rough_texture". Other training sessions are conducted with a smooth texture, such as glass. The tactile sensor signals input from touching the tactile transducer to the smooth texture are transformed into a statistical model of the input signal and stored as a standard under the handle "smooth_texture". Later, in the recognition mode, an unknown object is touched by the tactile transducer resulting in a sample tactile sensor signal. Recognition of unknown touch signals requires sampling and digitizing the touch transducer's signals. These digitized sensor signals are then processed into metadata. The metadata is then compared with the standard statistical models of "rough_texture" and "smooth_texture". The most likely match is then the inferred touch recognition result.

Combinations of two or more types of sensors can have their signals combined into an input metadata vector that characterizes a composite sampling event. The composite sampling event can be recognized using the principles of Hidden Markov Modeling (HMM). An example composite sampling event can be the state of the health and fatigue of the user of a wireless device 100. For example, a wireless device 100 can be equipped with a tactile transducer which outputs tactile sensor signals in response to the hand force and pulse rate of the user who is gripping the wireless device 100. The wireless device 100 can be equipped with a temperature sensor which outputs body temperature signals in response to the user gripping the wireless device 100. Hidden Markov Modeling (HMM) can be used to recognize a force/temperature input metadata vector that characterizes the combination of the hand force and the temperature sensor signals resulting from a sampling event. A composite sampling event in this example can have an extended duration so that the force sensor can transduce the pulse rate of the user over a period of time.

In the training stage, the tactile sensor signals and the force sensor signals are output while the user is in a condition of good health and resting normally. The tactile sensor signals and the force sensor signals are combined into a force/temperature input metadata vector which is transformed into a statistical model of the input signals. The statistical model is stored as a standard in the computer memory of the wireless device

100 under the handle "good_health_ resting_normally". Other training sessions are conducted with the user in different states of health and fatigue. For example, the user may be training the wireless device 100 while working late at night at the office. The tactile sensor signals and the force sensor signals resulting from holding the wireless device 100, are combined into a force/temperature input metadata vector for the user in the condition of being in good health but fatigued. The force/temperature input metadata vector is transformed into a statistical model of the input signals and stored as a standard under the handle "good_health_ fatigued".

Later, in the recognition mode, as the user holds the wireless device 100, the tactile sensor signals and the force sensor signals are sampled. The Health/Fatigue_State recognition consists of sampling and digitizing the touch transducer's signals. These digitized sensor signals are then processed into a metadata vector. The metadata vector is then compared with the standard statistical models of handle "good_health_ resting_normally" and "good_health_ fatigued". The most likely match is then the inferred touch recognition result.

In accordance with the invention, this recognition result can be used by a health maintenance application program in the wireless device 100, to provide useful and appropriate information to the user. For example, a health maintenance program can process the recognition result, and in response, signal an alarm to the user and provide suggestions for medications to palliate the sensed fatigue. One problem with automatic recognition programs is that they are either relatively large or they call databases that are relatively large in comparison to the memory capacity of the wireless device 100.

Another aspect of the invention is the recognition result can be used by a supplementary application program in a remote server, to provide additional and more detailed useful and appropriate information to the user. For example, the server can access a large database of suggestions for medications to palliate the sensed fatigue of the user. The results of the search of the database can be returned to the wireless device 100. The server can also maintain a personal profile of the user's characteristics and preferences and it can use that profile in automatically formulate its query to the database. For example, the user's drug allergies can be stored in the server's database, to insure that

recommendations are not made that will result in an allergic reaction by the user to the suggested medication.

Figure 2A is a functional block diagram of the wireless device 100, the server 140, and the web server 160, and their interaction when exchanging the metadata vector 138 and the privacy control data 150'. These exchanges are bulk encrypted with a symmetric session key, such as a Data Encryption Standard (DES) key, to protect the privacy of the data. To insure the integrity of the metadata vector 138 and the privacy control data 150', a message authentication code (MAC) can be computed and appended to the data, as described in the above referenced book by Stephen Thomas entitled "SSL and TLS", published by John Wiley and Sons, 2000. To insure that the source of the metadata vector 138 and the privacy control data 150' cannot be repudiated, a digital signature can be appended to the data, as described in the above referenced book by Richard E. Smith entitled "Internet Cryptography", published by Addison Wesley, 1997.

Figure 2A shows the scope of the distributed context awareness implementation. The wireless device 100 has context sensitive applications A, B, X, and Y either downloaded or in firmware. The wireless device 100 may locally preprocess part of the context information in the metadata vector 138 before sending it to the context inference engine 142 in the network server 140 which is capable of processing the data and responding back with the resulting current context. The wireless device 100 may run application programs that require accessing the web service server 160 to provide context sensitive services to the mobile user.

Figure 2A shows how processing of sensor data from the sensors in the wireless device 100, can be distributed between the wireless device and the network server 140. The operation in Figure 2A is as follows:

1. The sensors continuously provide the sensor data to the Context Inference Engine 136 in the wireless device 100.

2. An application program that utilizes the context awareness APIs 154 may request the latest context information, or the application program may be registered to receive any changes to specific context information.

3. The Context Inference Engine 136 securely contacts the Context Inference Engine 142 of the network server 140 and sends the metadata vector 138 to the server 140. Depending on the sensors and the implementation details, Context Inference Engine 136 may preprocess part of the sensor data in the metadata vector 138 prior to sending it. Depending on the sensors and the interval for processing, there may be virtual connection open between Context Inference Engine 136 and Context Inference Engine 142 for frequent data exchanges. Context Inference Engine 142 at the network server 140, has the processing power and memory capacity to handle computationally intensive and/or memory intensive processing of the preprocessed sensor data in the metadata vector 138 to produce the current context result information.

4. Context Inference Engine 142 at the network server 140 may utilize local user information (history information, customer details) stored in the user database 146 for making a more accurate determination of the mobile user's current context.

5. Context Inference Engine 142 at the network server 140 then securely returns the current context awareness information to Context Inference Engine 136 in the wireless device 100.

6. Context Inference Engine 136 in the wireless device 100 then provides the current context awareness information through Context Awareness APIs 154 to the application programs registered for to receive that information.

Figure 2A shows how Web Services in Web Service Server 160 are enabled to receive current context results of the wireless device 100. Web Services Server 160 has a software system for server application program A and an execution environment for server application programs X and Y that are similar to the software system SS1 and execution environment (Exec. Env.) in the wireless device 100 shown in Figure 2. Server Application programs A, X, and Y in Web Service Server 160 may require access through the Context Awareness APIs to provide Web Services with the current context of the wireless device 100.

In Figure 2A, Web Service Server 160 uses the Context Inference Client 176 to contact the Context Inference Server 174 in the network server 140. Context Inference Client 176 may utilize customer database information in database 184 to enhance the context sensitivity capabilities of the web server 160. The contact to the network server

140 is done through a context awareness interface 186 to the Context Inference Server 174 in the network server 140.

Context Inference Server 174 registers the Web Services of the web server 160 through the privacy control 164 of the network server 140 to the Context Inference Engine 142. Privacy control 164 has a cached copy 144 of the Privacy Profile 152 of the wireless device 100. This enables processing of the privacy check in the network Server 140 for access requests from web server 160. The communication between web server 160 and network server 140 is secured using the Internet secure protocols such as HTTPS or SSL. The Context Inference Server 174 can publish its own service as a Web Service to other Web Services on the Internet, in which case the implementation of the interface 186 between web server 160 and network server 140 can be Extensible Markup Language (XML) messages carried in the Simple Object Access Protocol (SOAP) messaging protocol.

The Context inference Engine 142 in the network server 140 will receive processed sensor metadata vector 138 information and possibly some application API information originated from the Context Inference Engine 136 of the wireless device 100. The Context inference Engine 142 of the network server has user database 146 information of the behavior of the user and of the past usage of the wireless device. The Context inference Engine 142 of the network server may also have third party services available (such as instances offering content and/or services) to be offered to potential users. What is offered to the user can also depend on the user profile 144. The nature of the Context inference Engine 136 information of the wireless device 100 that is conveyed to the Context inference Engine 142 of the network can be controlled with the privacy control 150 that is managed by the user of the wireless device 100. The user may thus fully or partly disable the Context inference Engine 142 of the network to control the amount of his/her information that can be used by third party services. The privacy control 150 enables the user to control access by anyone to his/her private information.

The Context inference Engine 136 of the wireless device receives an input from the API interface 154 from the applications A, B, X, or Y located in the wireless device 100. An example would be from a calendar application program indicating that a meeting is starting in 25 minutes time. As another example the calendar application program

indicates that Lisa is having a birthday tomorrow into which you are participating. The Context inference Engine 136 of the wireless device can convey processed result information to the Context inference Engine 142 of the network server. Now in addition to the sensor information, information from the application programs A, B, X, or Y can also be used in the decision making of the Context inference Engine 136 of the wireless device. A combination of the sensor information and information coming from the application programs A, B, X, or Y can be processed by the Context inference Engine 136. The user's behavior or usage patterns can be detected from the sensor and recorded in a the user database, concerning the usage of the application programs. As previously discussed, the processing of this combined information from the sensors and from the application programs can be shared between the Context inference Engine 136 and the Context inference Engine 142. Either the application programs A, B, X, or Y running in the wireless device 100 or the server application programs A, X and Y running in the web server 160, may optionally provide application data to the context inference engine 142 in the network server 140. The context inference engine 142 can optionally process the metadata vector 138 and the application data to produce the current context.

The information transfer from the Context inference Engine 136 of the wireless device to the Context inference Engine 142 of the network server can be done in alternative ways. The system can be managed so that the current consumption and transfer capacity between the wireless device 100 and the network server 140 is taken into account. The context information does not always have to be collected so frequently that it would have to be periodically transferred to the network side 140 every few seconds. Depending on the application, the timing window applied to information transfer from the Context inference Engine 136 of the wireless device 100 to the Context inference Engine 142 of the server 140 can vary from seconds to minutes. If there were no event change or condition change in the environment of the wireless device 100, there would be no need to transfer information to the Context inference Engine 142 of the server 140. Additionally information can be temporarily stored in a buffer in the wireless device 100, which can then transferred less frequently to the network Context inference Engine 142. Packet based GPRS and UMTS can support the less frequent information transfer rates. Also, it is advantageous to send the network Context inference Engine 142 information

from the wireless device 100 as an attachment, immediately subsequent to other signaling made to in the network direction from the wireless device 100, thus saving the radio transmitter of the wireless device 100 from having to be switched on again for transferring the Context inference Engine 136 information separately to the network server 140.

Returning to Figure 1, the relationship is shown between the network server 140, the Universal Description, Discovery and Integration (UDDI) registry 170, and a plurality of web site servers 160. UDDI is a defacto standard for an Internet-based registry. The UDDI registry 170 enables the network server 140 to discover new web sites for services and businesses on the Internet. Once such services and businesses are identified by the UDDI registry 170 to the network server 140, then the server 140 must apply the mobile user's cached privacy profile 144 in Figure 2A, in order to prevent unauthorized access of the user's private data by application programs on the newly discovered web sites.

Figure 3 is a network process flow diagram of the interaction of the wireless device 100 I the first column, network server 140 in the middle column, and web server 160 in the right column, when they carry out the determination of the current context of the wireless device 100. The process begins with the wireless device 100 in step 302:

Step 302: PRIVACY CONTROL 150 IN WIRELESS DEVICE 100 SENDS UPDATED PRIVACY PROFILE TO NETWORK SERVER 140.

Then the network server 140 continues with step 304:

Step 304: NETWORK SERVER 140 UPDATES CACHED PRIVACY PROFILE 144.

The wireless device 100 continues with the following steps 306, 308, and 310:

Step 306: SENSORS CONTINUOUSLY PROVIDE SENSOR DATA TO CONTEXT INFERENCE ENGINE 136 IN WIRELESS DEVICE 100.

Step 308: APPLICATION PROGRAM THAT USES CONTEXT AWARENESS API 154 REQUESTS LATEST CONTEXT INFORMATION.

Step 310: CONTEXT INFERENCE ENGINE 136 CONTACTS CONTEXT INFERENCE ENGINE 142 OF THE NETWORK SERVER 140 AND SENDS THE METADATA VECTOR 138 TO SERVER 140.

Then the network server 140 continues with steps 312 and 314:

Step 312: CONTEXT INFERENCE ENGINE 142 AT NETWORK SERVER 140 USES LOCAL USER INFORMATION STORED IN USER DATABASE 146 TO MAKE A MORE ACCURATE DETERMINATION OF THE MOBILE USER'S CURRENT CONTEXT.

Step 314: NETWORK SERVER 140 REQUESTS DATA FROM WEB SERVER 160.
THE NETWORK SERVER'S ACCESS IS AUTHORIZED BY CACHED PRIVACY PROFILE 144 IN NETWORK SERVER.

Then the web server 160 continues with step 316:

Step 316: WEB SERVER PROVIDES USER INFORMATION STORED IN DATABASE 184 TO NETWORK SERVER 140.

Then the network server 140 continues with step 318:

Step 318: CONTEXT INFERENCE ENGINE 142 AT THE NETWORK SERVER 140 THEN SECURELY RETURNS THE CURRENT CONTEXT AWARENESS INFORMATION TO CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100.

Then the wireless device 100 finishes with step 320:

Step 318: CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100 THEN PROVIDES THE CURRENT CONTEXT AWARENESS INFORMATION THROUGH CONTEXT AWARENESS APIs 154 TO THE APPLICATION PROGRAMS REGISTERED TO RECEIVE THAT INFORMATION.

Figure 4 is a functional block diagram of the network server 140, showing the memory 402 storing the application services software programs needed to perform the operations of the invention. The memory is connected by the bus 404 to the cache 144, user database 146, TCP/IP network adapter 406, and central processor 410. The memory 402 stores programs which are sequences of executable instructions which, when executed by the processor 410, carry out the methods of the invention.

Figure 4 is a functional block diagram of the network server, showing the memory storing the application services software programs needed to perform the operations of an embodiment of the invention. Figure 4 discloses the functional components of an exemplary network server 140 arranged as an object model. The object model groups the

object oriented software programs into components that perform the major functions and applications in network server 140. The object model for memory 402 of network server 140 employs a three-tier architecture that includes presentation tier 415, infrastructure objects partition 422, and business logic tier 414. The object model further divides business logic tier 414 into two partitions, application objects partition 422 and data objects partition 426.

Presentation tier 415 retains the programs that manage the device interfaces to network server 140. In Figure 4, presentation tier 415 includes network interface 420. A suitable implementation of presentation tier 415 may use Java servlets to interact with WAP protocol gateway 120 via the hypertext transfer protocol ("HTTP"). The Java servlets ran within a request/response server that manages the exchange of messages between WAP protocol gateway 120 and network server 140. A Java servlet is a Java program that runs within a Web server environment. A Java servlet takes a request as input, parses the data, performs logic operations, and issues a response back to WAP protocol gateway 120. The Java runtime platform pools the Java servlets to simultaneously service many requests. Network interface 420 accepts request messages from WAP protocol gateway 120 and passes the information in the request to visit object 428 for further processing. Visit object 428 passes the result of that processing to network interface 420 for transmission back to the WAP protocol gateway 120. Network interface 420 may also use network adapter 406 to exchange data with another user device.

Infrastructure objects partition 422 retains the programs that perform administrative and system functions on behalf of business logic tier 414. Infrastructure objects partition 422 includes operating system 425, and an object oriented software program component for database server interface 430, and system administrator interface 432.

Business logic tier 414 in Figure 4 includes multiple instances of visit object 428, 428', 428". A separate instance of visit object 428 exists for each network interface 420 session. Each visit object 428 is a stateful session object that includes a persistent storage area from initiation through termination of the session, not just during a single interaction or method call. The persistent storage area retains information associated with the session.

When WAP protocol gateway 120 sends a metadata vector 138 message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in context inference engine 142 application 440 to perform a context inference on the metadata vector and return a current context result.

When WAP protocol gateway 120 sends a privacy control data 150' message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in privacy control 164 application 442 to update the cached privacy profile 144. The application 442, in turn make a method call to privacy profile update application 448 to store the updated data 150' in the cache 144.

When WAP protocol gateway 120 sends a user data update message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in user database application 446 to store the user data in the database 146.

A description of server programming applications developed with Enterprise Java Beans is provided in the book by Ed Roman entitled "Mastering Enterprise Java Beans", published by John Wiley and Sons, 1999. A description of the use of an object model in the design of server applications is provided in the book by Matthew Reynolds entitled "Beginning E-Commerce", Wrox Press Inc, 2000, (ISBN: 1861003986). Java servlets and the development of web site servers is described in the book by Duane K. Fields, et al. entitled "Web Development with Java Server Pages", published by Manning Publications Co., 2000.

The resulting context sensitive web services invention enables a mobile phone or wireless device 100 to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's

perceived environment. The mobile user is provided with the ability to control access by application programs anywhere in the network, to the user's private data.

Although a specific embodiment of the invention has been disclosed, it will be understood by those having skill in the art that changes can be made to the specific embodiment without departing from the spirit and the scope of the invention.

CLAIMS

What is claimed is:

1. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

2. The method of claim 1, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

3. The method of claim 1, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

4. The method of claim 3, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

5. The method of claim 3, wherein the wireless device offloads a portion of the processing of the sensor signals with a context inference engine to the server.

6. The method of claim 3, wherein a personal profile of the user is maintained by the server.

7. The method of claim 1, which further comprises:

providing user control of access by application programs to the user's private data.

8. The method of claim 3, which further comprises:

providing user control of access by application programs to the user's private data in the server.

9. The method of claim 1, which further comprises:

providing user control of access by application programs in a web server, to the user's private data.

10. The method of claim 1, which further comprises:

providing the current context result to an application program; and

receiving the useful information for the user from the application program.

11. The method of claim 1, which further comprises:

providing user control of access by an application program to the current context result;

providing the current context result to the application program in response to the user control; and

receiving the useful information from the application program.

12. The method of claim 11, which further comprises:

granting access permission to the application program to access the current context result, based on the user's data stored in a privacy profile.

13. The method of claim 11, wherein providing user control of access is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

14. The method of claim 13, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

15. The method of claim 13, wherein the wireless device offloads a portion of the processing of providing user control of access, to the server.

16. The method of claim 13, wherein a personal profile of the user is maintained by the server.

17. The method of claim 16, which further comprises:

providing user control of access by application programs to the user's personal profile.

18. The method of claim 13, which further comprises:

providing user control of access by application programs to the user's personal profile in the server.

19. The method of claim 11, which further comprises:

providing user control of access by application programs in a web server, to the user's private data.

20. The method of claim 19, which further comprises:

enabling context sensitive applications and services within the wireless device while providing to the user control over the privacy user's current context result.

21. The method of claim 19, which further comprises:

enabling context sensitive applications and services within the network server while providing to the user control over the privacy user's current context result.

22. An apparatus to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a processor;

a memory coupled to the processor, programmed to perform the steps of:

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

23. The apparatus of claim 22, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

24. The apparatus of claim 22, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

25. The apparatus of claim 24, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

26. A wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a sensor for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine coupled to the sensor, for processing the sensor signals;

said context inference engine providing a current context result from the processing; and

an output device coupled to the context inference engine, for providing useful information to the user in response to the current context result.

27. A wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a privacy control for providing the user control of access by an application program to the user's private data;

a sensor for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine coupled to the sensor, for processing the sensor signals;

said context inference engine coupled to the privacy control, for providing a current context result from the processing to the application program; and

an output device coupled to the privacy control, for providing useful information to the user in response to the application program.

28. A system to provide useful information to the user of a wireless device that is appropriate to the device's current environment, comprising:

a privacy control in a server for receiving a user privacy profile from the wireless device and providing the user control of access by an application program to the user's private data;

a sensor in the wireless device for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine in the server coupled to the wireless device, for processing sensor information derived from the sensor signals;

said context inference engine coupled to the privacy control, for providing a current context result from the processing to the application program; and

an output device in the server, coupled to the privacy control, for transmitting useful information to the wireless device in response to the application program.

29. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

running a program that provides application data to the wireless device;

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals and the application data with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

30. The method of claim 29, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

31. The method of claim 30, wherein the step of running a program occurs in the wireless device.

32. The method of claim 29, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

33. The method of claim 32, wherein the step of running a program occurs in a web server coupled to the network server.

34. A system to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a processor;

a memory coupled to the processor, programmed to perform the steps of:

running a program that provides application data to the wireless device;

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals and the application data with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

35. The system of claim 34, wherein the processing of the sensor signals and the application data with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

36. The system of claim 35, wherein the step of running a program occurs in the wireless device.

37. The system of claim 34, wherein the processing of the sensor signals and the application data with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

38. The system of claim 37, wherein the step of running a program occurs in a web server coupled to the network server.

39. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

partially processing the sensor signals with a first context inference engine within the user's wireless device;

sending the partially processed sensor signals to a second context inference engine within a separate network server;

completing the processing the sensor signals with the second context inference engine;

sending a current context result from the second context inference engine to the wireless device; and

providing useful information to the user in response to the current context result.

40. A system to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a wireless device for receiving sensor signals characterizing a current environment of the wireless device;

a first context inference engine within the user's wireless device for partially processing the sensor signals;

a second context inference engine within a separate network server for receiving the partially processed sensor signals sent from the wireless device and completing the processing the sensor signals;

said second context inference engine sending a current context result from the second context inference engine to the wireless device; and

said wireless device providing useful information to the user in response to the current context result.

41. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

partially processing the sensor signals with a first context inference engine within the user's wireless device;

sending the partially processed sensor signals to a second context inference engine within a separate network server;

completing the processing the sensor signals with the second context inference engine;

forwarding a current context result from the network server to a second server; and

sending useful information from the second server to the user's wireless device in response to the current context result.

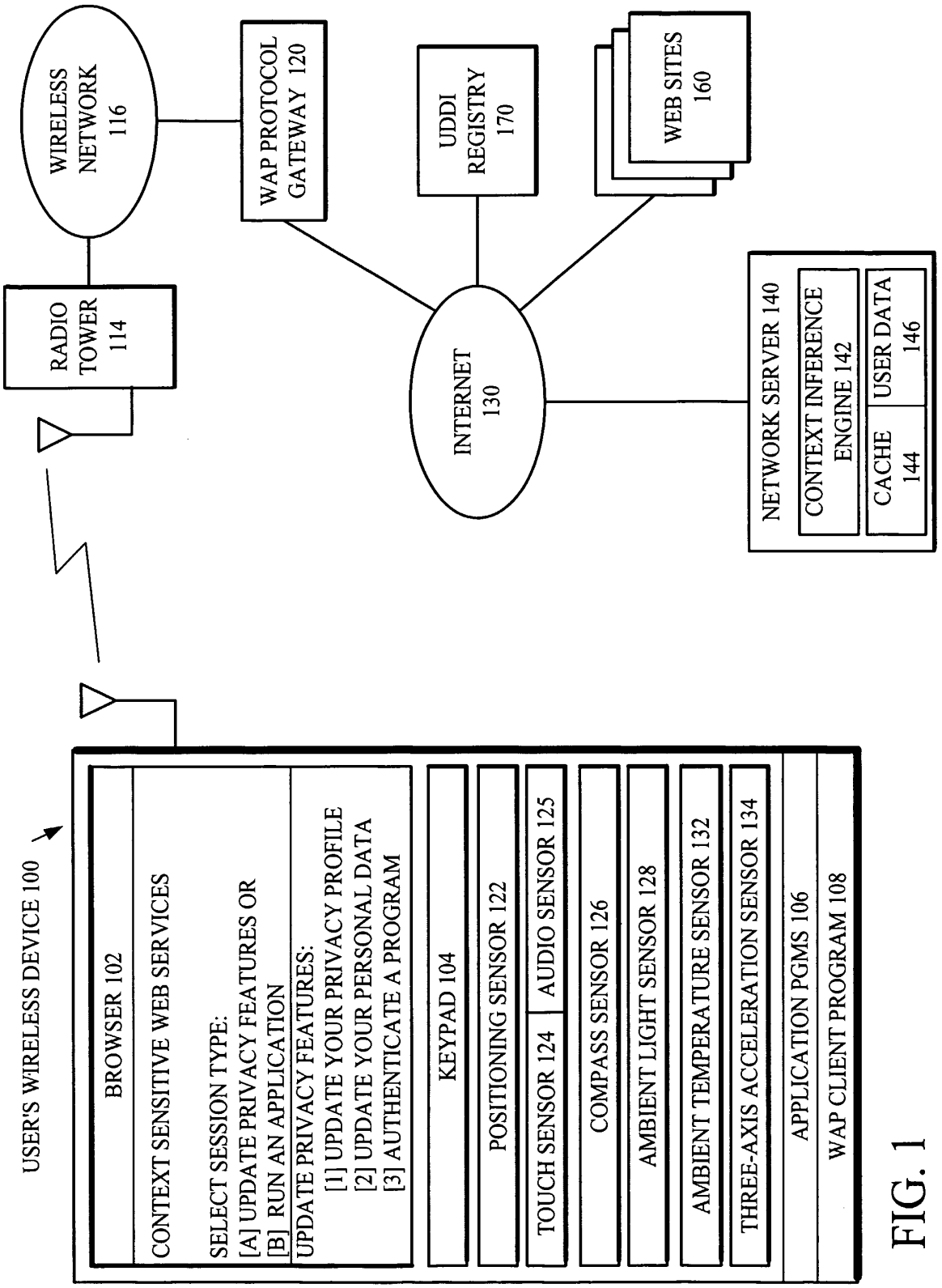

USER'S WIRELESS DEVICE 100
BROWSER 102
CONTEXT SENSITIVE WEB SERVICES
SELECT SESSION TYPE:
[A] UPDATE PRIVACY FEATURES OR
[B] RUN AN APPLICATION
UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[2] UPDATE YOUR PERSONAL DATA
[3] AUTHENTICATE A PROGRAM
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
AUDIO SENSOR 125
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134
APPLICATION PGMS 106
WAP CLIENT PROGRAM 108
RADIO TOWER 114
WIRELESS NETWORK 116
WAP PROTOCOL GATEWAY 120
INTERNET 130
UDDI REGISTRY 170
WEB SITES 160
NETWORK SERVER 140
CONTEXT INFERENCE ENGINE 142
CACHE 144
USER DATA 146

FIG. 1

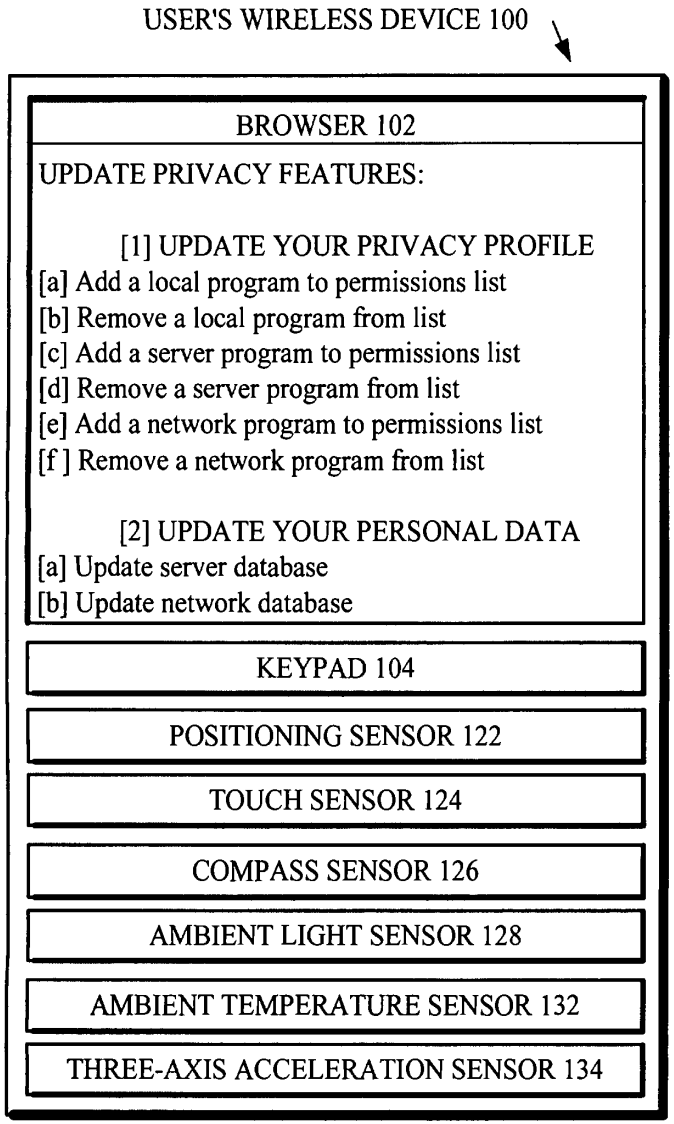

USER'S WIRELESS DEVICE 100
BROWSER 102
UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[a] Add a local program to permissions list
[b] Remove a local program from list
[c] Add a server program to permissions list
[d] Remove a server program from list
[e] Add a network program to permissions list
[f] Remove a network program from list
[2] UPDATE YOUR PERSONAL DATA
[a] Update server database
[b] Update network database
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1A

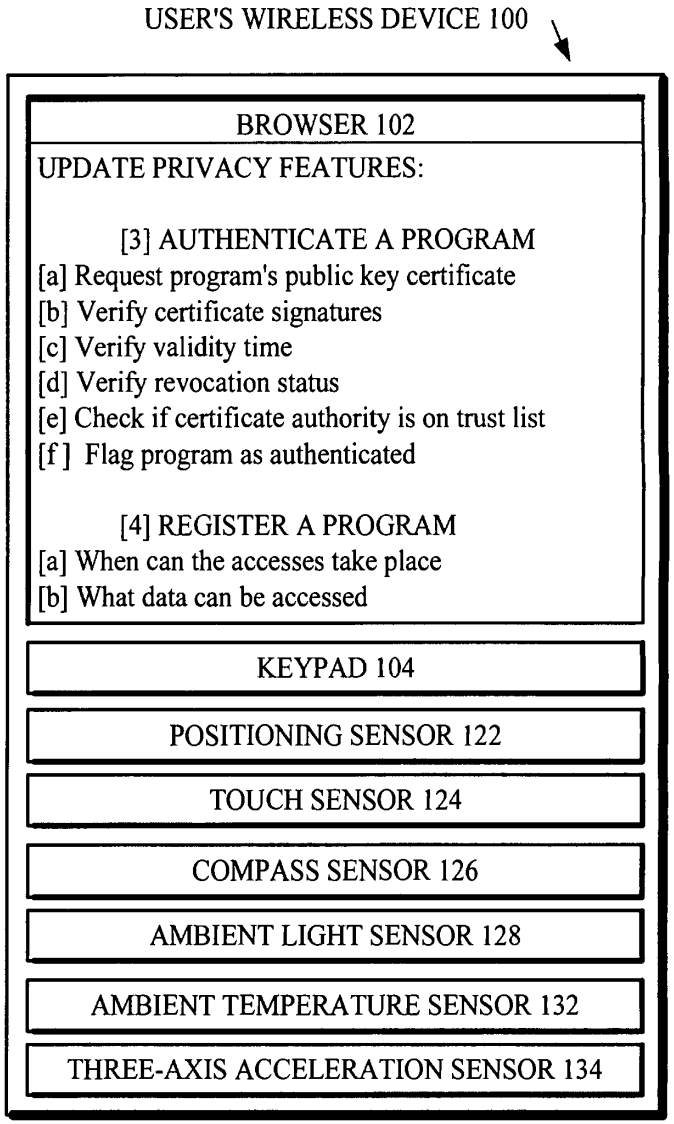

USER'S WIRELESS DEVICE 100
BROWSER 102
UPDATE PRIVACY FEATURES:
[3] AUTHENTICATE A PROGRAM
[a] Request program's public key certificate
[b] Verify certificate signatures
[c] Verify validity time
[d] Verify revocation status
[e] Check if certificate authority is on trust list
[f] Flag program as authenticated
[4] REGISTER A PROGRAM
[a] When can the accesses take place
[b] What data can be accessed
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1B

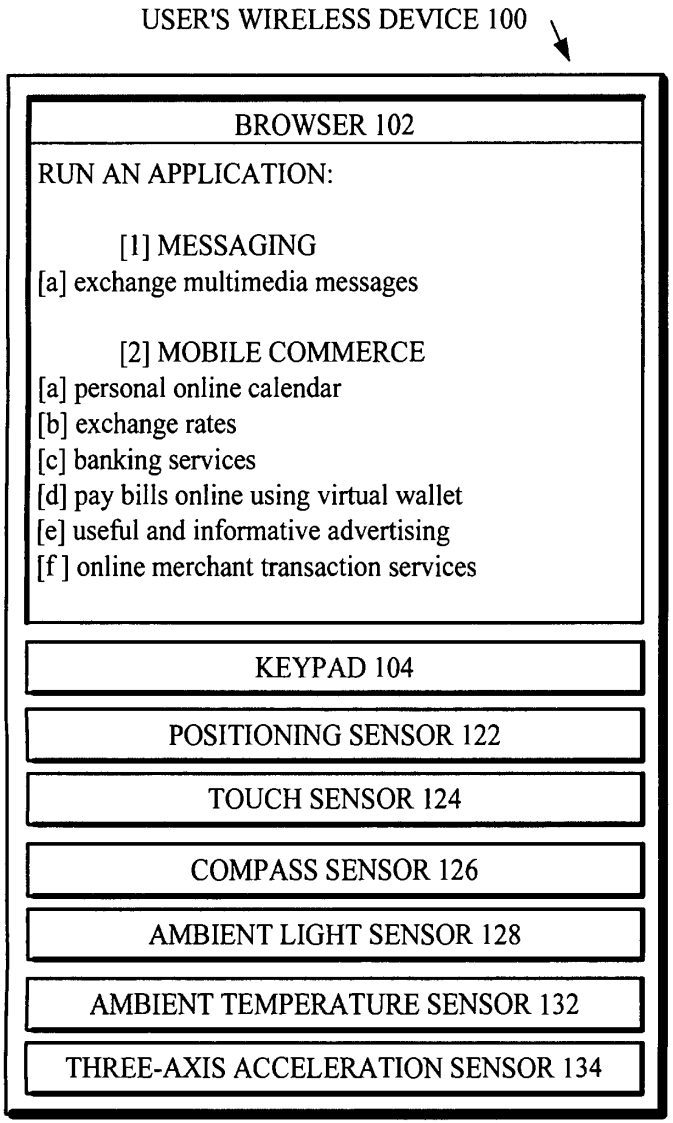

USER'S WIRELESS DEVICE 100
BROWSER 102
RUN AN APPLICATION:
[1] MESSAGING
[a] exchange multimedia messages
[2] MOBILE COMMERCE
[a] personal online calendar
[b] exchange rates
[c] banking services
[d] pay bills online using virtual wallet
[e] useful and informative advertising
[f] online merchant transaction services
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1C

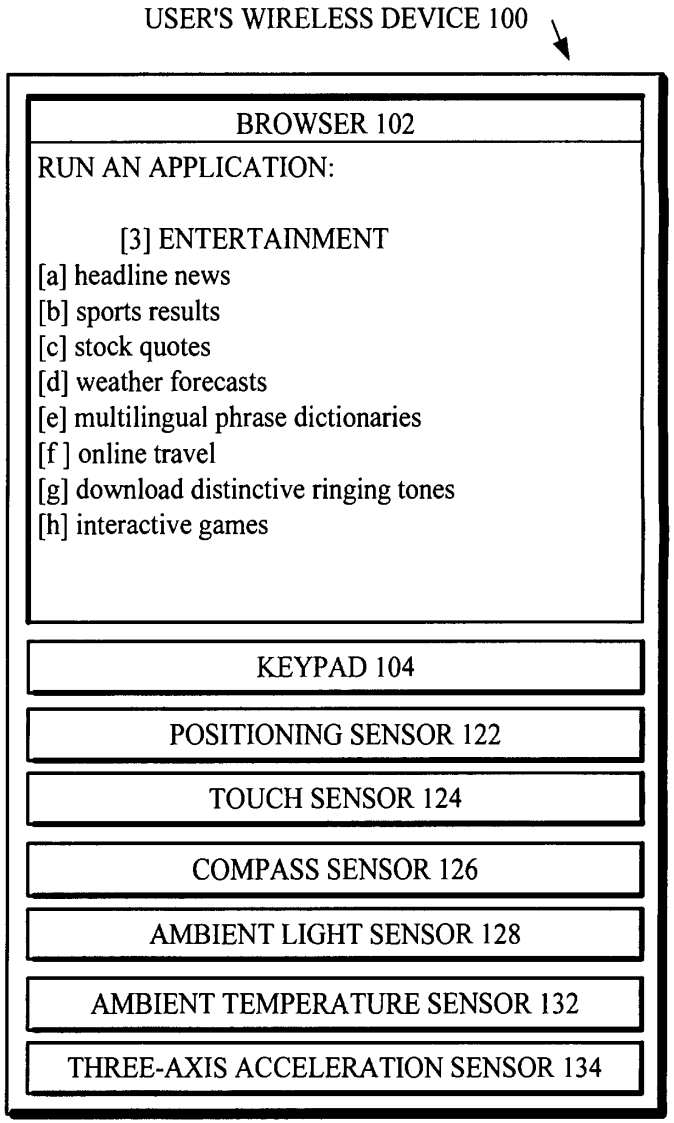

USER'S WIRELESS DEVICE 100
BROWSER 102
RUN AN APPLICATION:
[3] ENTERTAINMENT
[a] headline news
[b] sports results
[c] stock quotes
[d] weather forecasts
[e] multilingual phrase dictionaries
[f] online travel
[g] download distinctive ringing tones
[h] interactive games
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1D

FIG. 2

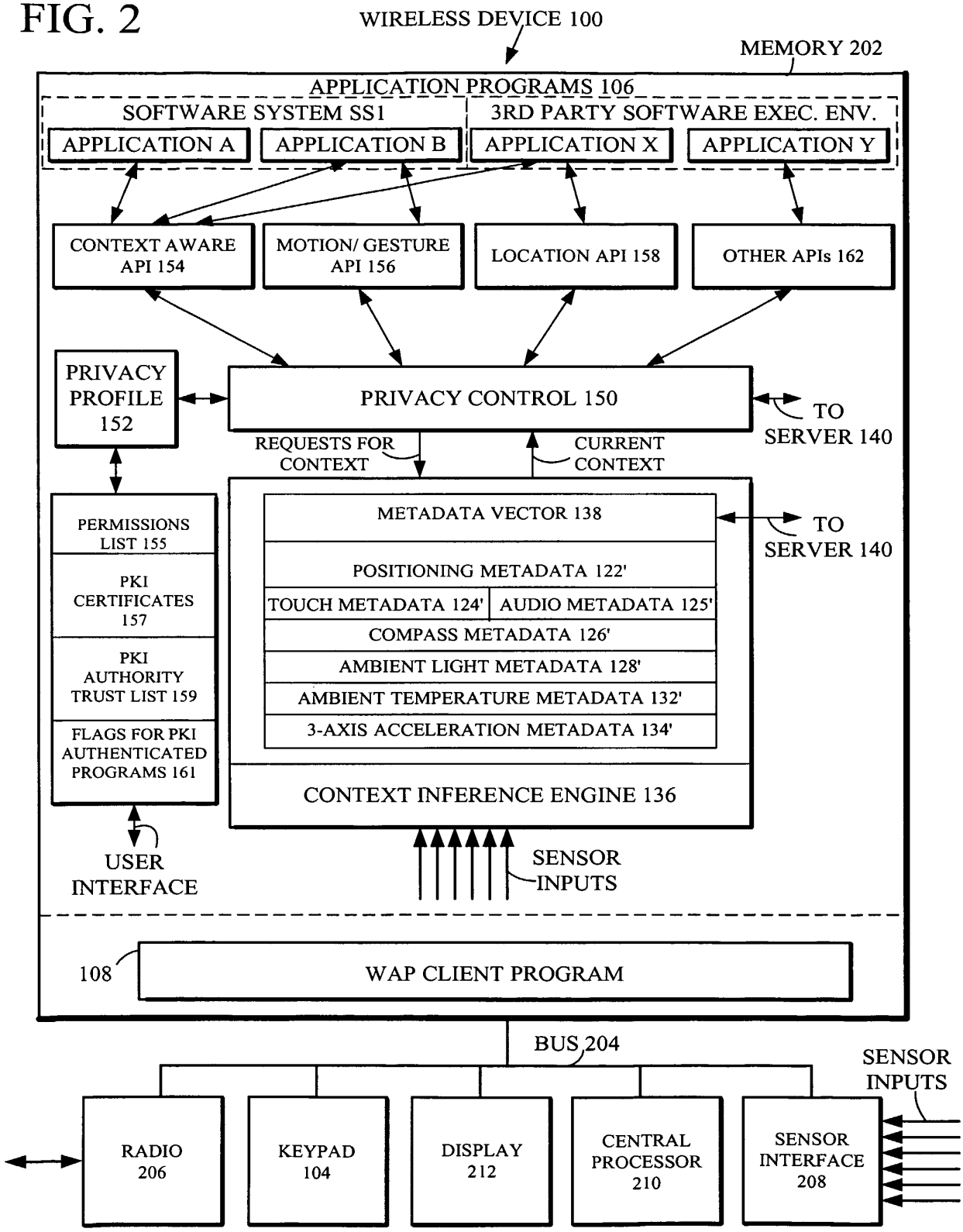

WIRELESS DEVICE 100
MEMORY 202
APPLICATION PROGRAMS 106
SOFTWARE SYSTEM SS1
3RD PARTY SOFTWARE EXEC. ENV.
APPLICATION A
APPLICATION B
APPLICATION X
APPLICATION Y
CONTEXT AWARE API 154
MOTION/ GESTURE API 156
LOCATION API 158
OTHER APIs 162
PRIVACY PROFILE 152
PRIVACY CONTROL 150
TO SERVER 140
REQUESTS FOR CONTEXT
CURRENT CONTEXT
PERMISSIONS LIST 155
PKI CERTIFICATES 157
PKI AUTHORITY TRUST LIST 159
FLAGS FOR PKI AUTHENTICATED PROGRAMS 161
METADATA VECTOR 138
TO SERVER 140
POSITIONING METADATA 122'
TOUCH METADATA 124'
AUDIO METADATA 125'
COMPASS METADATA 126'
AMBIENT LIGHT METADATA 128'
AMBIENT TEMPERATURE METADATA 132'
3-AXIS ACCELERATION METADATA 134'
CONTEXT INFERENCE ENGINE 136
USER INTERFACE
SENSOR INPUTS
108
WAP CLIENT PROGRAM
BUS 204
SENSOR INPUTS
RADIO 206
KEYPAD 104
DISPLAY 212
CENTRAL PROCESSOR 210
SENSOR INTERFACE 208

FIG. 2A

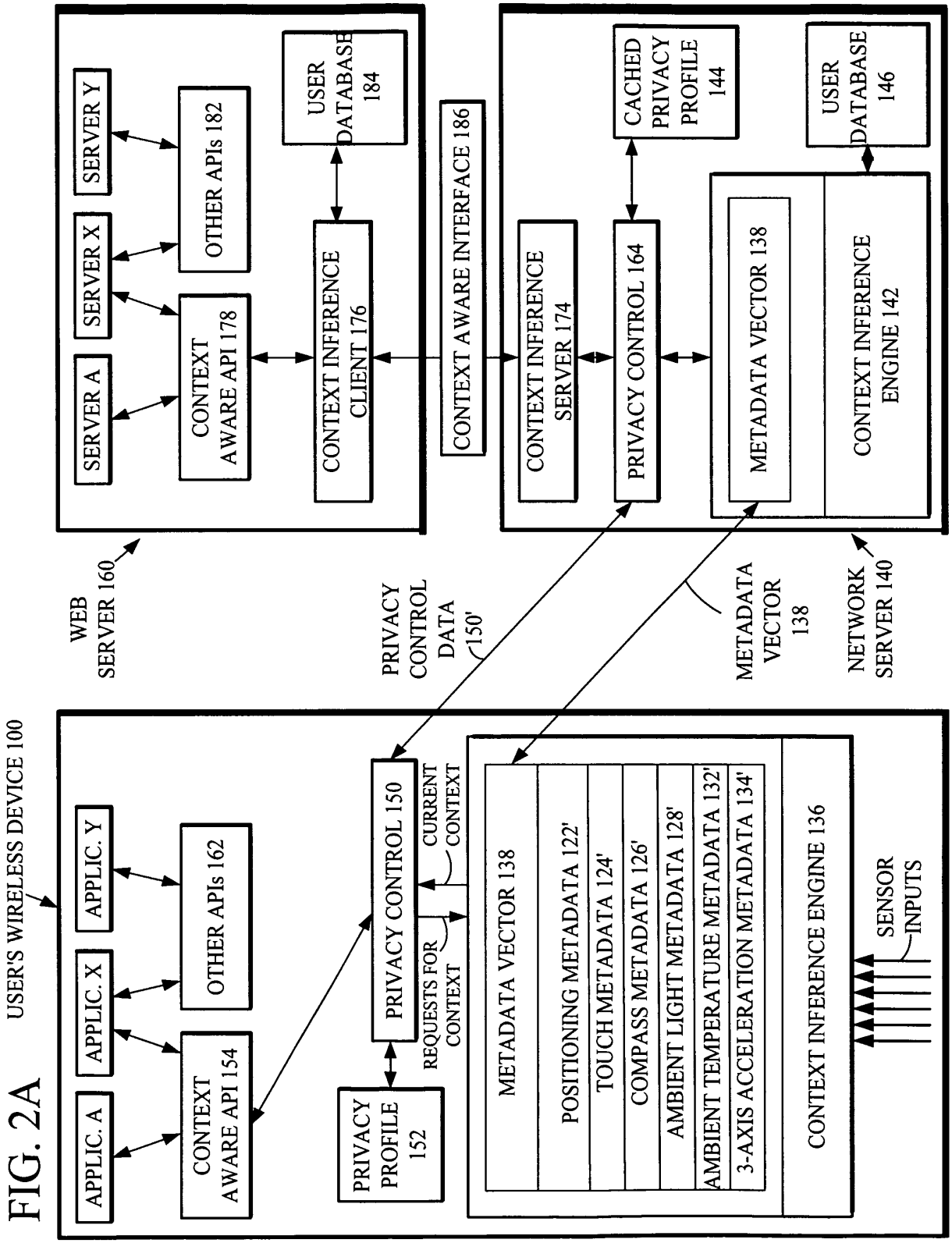

USER'S WIRELESS DEVICE 100
APPLIC. A
APPLIC. X
APPLIC. Y
CONTEXT AWARE API 154
OTHER APIs 162
PRIVACY PROFILE 152
PRIVACY CONTROL 150
REQUESTS FOR CONTEXT
CURRENT CONTEXT
METADATA VECTOR 138
POSITIONING METADATA 122'
TOUCH METADATA 124'
COMPASS METADATA 126'
AMBIENT LIGHT METADATA 128'
AMBIENT TEMPERATURE METADATA 132'
3-AXIS ACCELERATION METADATA 134'
CONTEXT INFERENCE ENGINE 136
SENSOR INPUTS
WEB SERVER 160
SERVER A
SERVER X
SERVER Y
CONTEXT AWARE API 178
OTHER APIs 182
CONTEXT INFERENCE CLIENT 176
USER DATABASE 184
CONTEXT AWARE INTERFACE 186
PRIVACY CONTROL DATA 150'
CONTEXT INFERENCE SERVER 174
PRIVACY CONTROL 164
CACHED PRIVACY PROFILE 144
METADATA VECTOR 138
METADATA VECTOR 138
CONTEXT INFERENCE ENGINE 142
USER DATABASE 146
NETWORK SERVER 140

FIG. 3

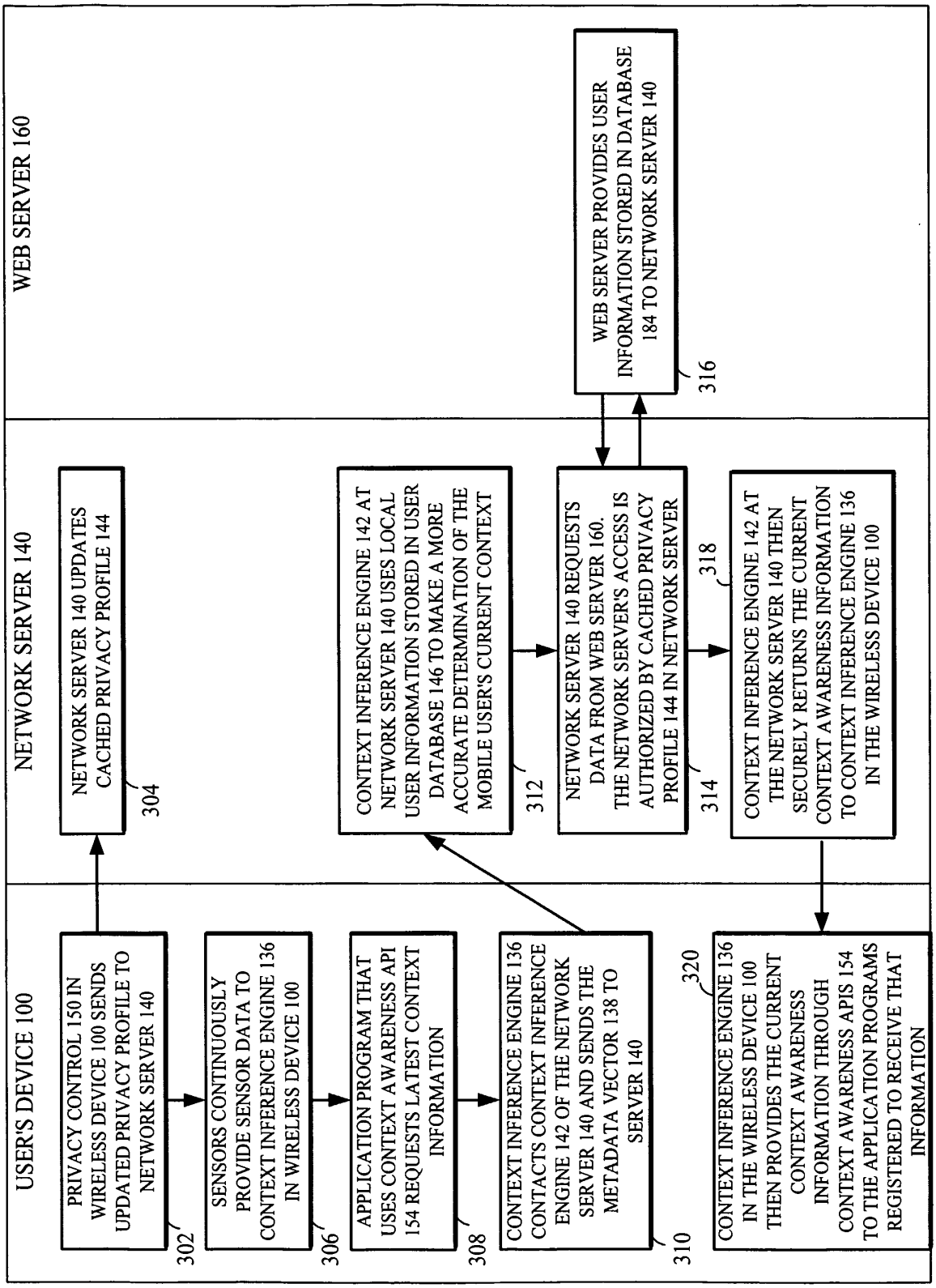
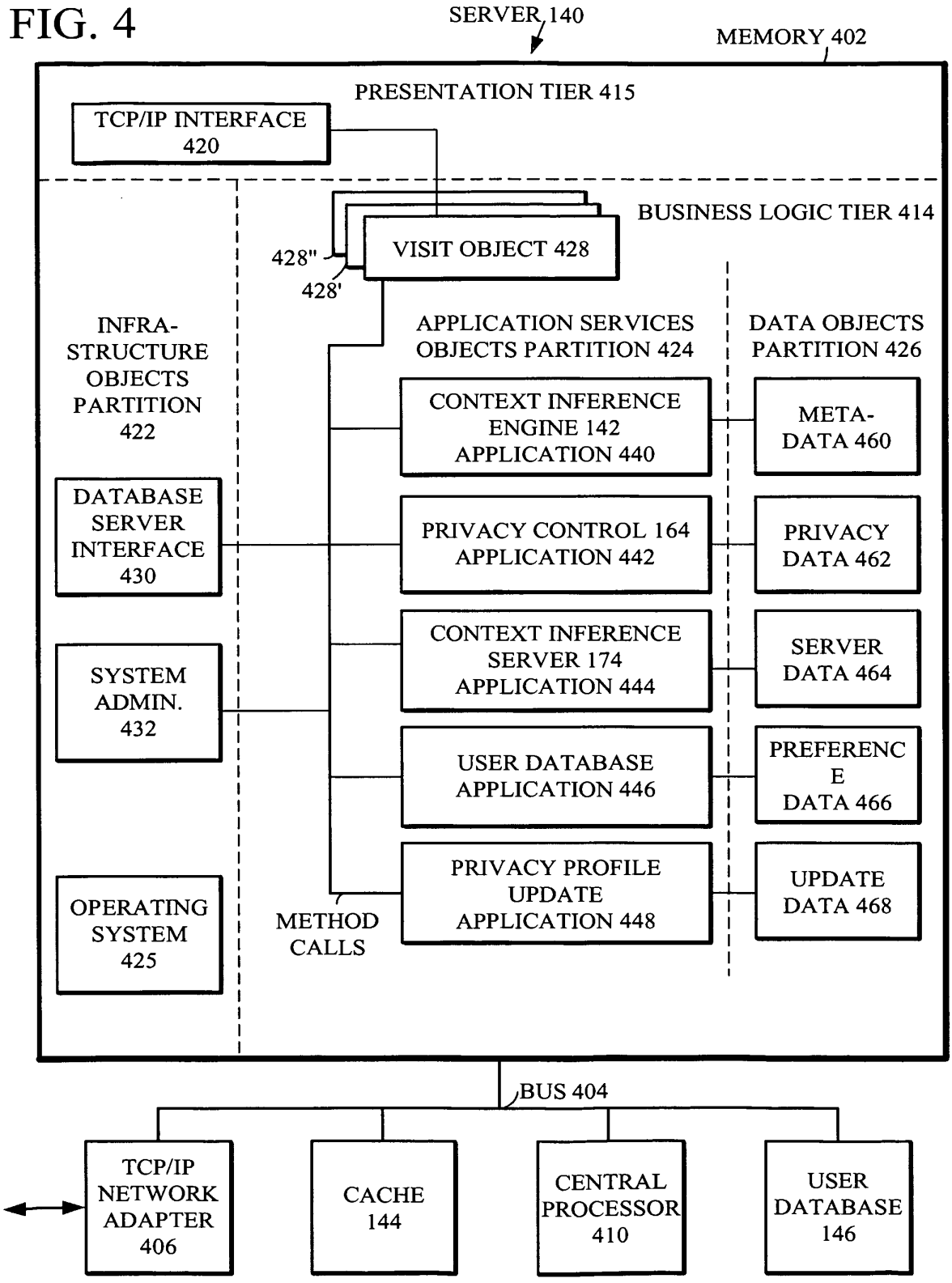

USER'S DEVICE 100
NETWORK SERVER 140
WEB SERVER 160
PRIVACY CONTROL 150 IN WIRELESS DEVICE 100 SENDS UPDATED PRIVACY PROFILE TO NETWORK SERVER 140
302
NETWORK SERVER 140 UPDATES CACHED PRIVACY PROFILE 144
304
SENSORS CONTINUOUSLY PROVIDE SENSOR DATA TO CONTEXT INFERENCE ENGINE 136 IN WIRELESS DEVICE 100
306
APPLICATION PROGRAM THAT USES CONTEXT AWARENESS API 154 REQUESTS LATEST CONTEXT INFORMATION
308
CONTEXT INFERENCE ENGINE 136 CONTACTS CONTEXT INFERENCE ENGINE 142 OF THE NETWORK SERVER 140 AND SENDS THE METADATA VECTOR 138 TO SERVER 140
310
CONTEXT INFERENCE ENGINE 142 AT NETWORK SERVER 140 USES LOCAL USER INFORMATION STORED IN USER DATABASE 146 TO MAKE A MORE ACCURATE DETERMINATION OF THE MOBILE USER'S CURRENT CONTEXT
312
NETWORK SERVER 140 REQUESTS DATA FROM WEB SERVER 160. THE NETWORK SERVER'S ACCESS IS AUTHORIZED BY CACHED PRIVACY PROFILE 144 IN NETWORK SERVER
314
WEB SERVER PROVIDES USER INFORMATION STORED IN DATABASE 184 TO NETWORK SERVER 140
316
CONTEXT INFERENCE ENGINE 142 AT THE NETWORK SERVER 140 THEN SECURELY RETURNS THE CURRENT CONTEXT AWARENESS INFORMATION TO CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100
318
CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100 THEN PROVIDES THE CURRENT CONTEXT AWARENESS INFORMATION THROUGH CONTEXT AWARENESS APIS 154 TO THE APPLICATION PROGRAMS REGISTERED TO RECEIVE THAT INFORMATION
320

FIG. 4


SERVER 140
MEMORY 402
PRESENTATION TIER 415
TCP/IP INTERFACE 420
BUSINESS LOGIC TIER 414
VISIT OBJECT 428
428"
428'
INFRA-STRUCTURE OBJECTS PARTITION 422
APPLICATION SERVICES OBJECTS PARTITION 424
DATA OBJECTS PARTITION 426
CONTEXT INFERENCE ENGINE 142 APPLICATION 440
META-DATA 460
DATABASE SERVER INTERFACE 430
PRIVACY CONTROL 164 APPLICATION 442
PRIVACY DATA 462
CONTEXT INFERENCE SERVER 174 APPLICATION 444
SERVER DATA 464
SYSTEM ADMIN. 432
USER DATABASE APPLICATION 446
PREFERENCE DATA 466
PRIVACY PROFILE UPDATE APPLICATION 448
UPDATE DATA 468
OPERATING SYSTEM 425
METHOD CALLS
BUS 404
TCP/IP NETWORK ADAPTER 406
CACHE 144
CENTRAL PROCESSOR 410
USER DATABASE 146

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB02/01550

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04M 1/00, 3/00, 3/42, 11/10; H04B 1/38
US CL : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,115,611 A (KIMOTO et al) 05 September 2000, figs. 1, 7-8, 10, 12, 19, 27, 31, 42.	1-38 --- 39-41
Y	US 6,073,075 A (KONDOU et al) 06 June 2000, fig. 3, column 4 lines 26-42.	39-41

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 2002 (19.07.2002)	27 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer William Trost Telephone No. 703 306-0377

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 January 2006 (12.01.2006)

PCT

(10) International Publication Number
WO 2006/004784 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00

(21) International Application Number: PCT/US2005/022982

(22) International Filing Date: 27 June 2005 (27.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/583,765	28 June 2004 (28.06.2004)	US
60/598,364	3 August 2004 (03.08.2004)	US
60/652,121	11 February 2005 (11.02.2005)	US
60/653,411	16 February 2005 (16.02.2005)	US

(71) Applicant *(for all designated States except US)*: **JAPAN COMMUNICATIONS, INC.** [JP/JP]; 6-25-3 Minami-ohi, Shinagawa-ku, Tokyo, Tokyo 140-0013 (JP).

(72) Inventors; and

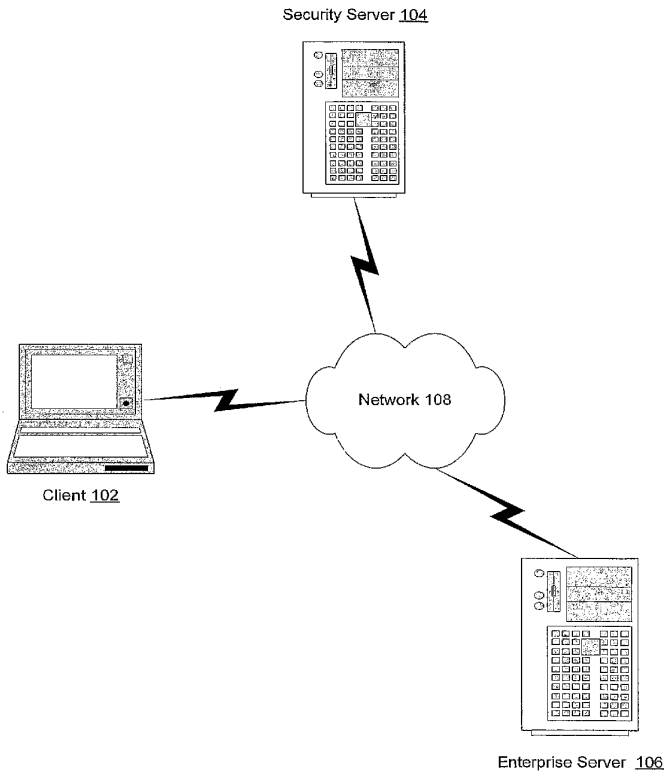
(75) Inventors/Applicants *(for US only)*: **SANDA, Frank, S.** [JP/US]; 29 Plandome Court, Manhasset, New York 11030 (US). **FUKUDA, Naohisa** [JP/JP]; #405, 6-1-8 Kita-Shinagawa, Shinagawa-ku, Tokyo, Tokyo 141-0001 (JP). **LAVES, Edward, W.** [US/US]; 1012 Sleepy Hollow Road, Golden, Colorado 80401 (US). **GURGONE, Raymond, T.** [US/US]; 807 N. Concord Drive, Woodstock, Illinois 60098 (US). **JOHNSTON, Robert, L.** [US/US]; 30 Midland Road, Colorado Springs, Colorado 80906 (US). **ROBINS, David, S.** [US/US]; 6 Wakefield Court, Buffalo Grove, Illinois 60089 (US). **TIDWELL, Justin, Owen** [US/US]; 19058 East Hampden Drive, Aurora, Colorado 80013 (US). **ZEITZ, Karlton, Mark** [US/US]; 6014 S. Zeno Court, Centennial, Colorado 80016 (US). **WORTHINGTON, Laura, J.** [US/US]; 6295 E. Jamison Circle North, Centennial, Colorado 80112 (US).

(74) Agent: **ALEMANNI, John, C.**; Kilpatrick Stockton LLP, 1001 West Fourth Street, Winston-Salem, North Carolina 27101, (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR ENHANCED NETWORK ACCESS



(57) Abstract: Systems and methods for enhanced network access are described. One aspect of one described embodiment includes receiving a request to connect to a network, the request associated with a user, determining a policy associated with the user, identifying at least one available network connection, determining at least one property of the at least one available network connection, evaluating the property based at least in part on the policy, and selecting the at least one available network connection based on the evaluation. In another embodiment, a computer-readable medium (such as, for example random access memory or a computer disk) includes code for carrying out such a method.

WO 2006/004784 A1

GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEMS AND METHODS FOR ENHANCED NETWORK ACCESS

RELATED APPLICATIONS

This application claims priority to Application Serial No. 60/583,765, filed on June 28, 2004, titled "Controlling Use of a Mobile Work Station Based on Network Environment," Application Serial No. 60/598,364, filed on August 3, 2004, titled "Systems and Methods for Enhancing and Optimizing a User's Experience on an Electronic Device," Application Serial No. 60/652,121, filed on February 11, 2005, titled "Remote Access Services," and Application Serial No. 60/653,411, filed on February 16, 2005, titled "Creating an Environment for Secure Mobile Access Anywhere," the entirety of all of which are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to computer networking and, more particularly to systems and methods for enhanced network access.

BACKGROUND

As the workforce becomes more mobile, enterprises often must provide a means for their users to connect to the enterprise network remotely. Enterprises and their users have much greater flexibility in selecting methods of connecting to the enterprise network as well as other resources, such as the Internet. With this added flexibility comes a concomitant increase in complexity and risk. Thus, although remote access may be necessary, enterprises may resist providing their users with remote access.

Each remote method for connecting to an enterprise network opens a potential security hole that might be exploited. For instance, listeners on a network, such as rogue access points, may be able to determine a user's username/password combination for accessing the network.

Also, each connection type may be purchased from a different network provider. The enterprise must reconcile charges from each of the providers for each of the users accessing the network remotely.

Further, every conventional connection product connecting to the enterprise network provides a unique interface. And although each interface may be relatively straightforward, complexity arises from the enterprise and its users having to deal with multiple interfaces for each of the various network connections the user wishes to make.

SUMMARY

Embodiments of the present invention provide systems and methods for enhanced network access. One aspect of one embodiment of the present invention comprises receiving a request to connect to a network, the request associated with a user, determining a policy associated with the user, identifying at least one available network connection, determining at least one property of the at least one available network connection, evaluating the property based at least in part on the policy, and selecting the at least one available network connection based on the evaluation. In another embodiment, a computer-readable medium (such as, for example random access memory or a computer disk) comprises code for carrying out such a method.

This illustrative embodiment is mentioned not to limit or define the invention, but to provide one example to aid understanding thereof. Illustrative embodiments are discussed in the Detailed Description, and further description of the invention is provided there. Advantages offered by the various embodiments of the present invention may be further understood by examining this specification.

FIGURES

These and other features, aspects, and advantages of the present invention are better understood when the following Detailed Description is read with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram showing an illustrative environment for implementation of one embodiment of the present invention;

Figure 2 is a block diagram illustrating the modules present on a client device 102 in one embodiment of the present invention;

Figure 3 is a block diagram illustrating the modules present on a security server 104 in one embodiment of the present invention;

Figure 4 is a block diagram illustrating the modules present on an enterprise server 106 in one embodiment of the present invention;

Figure 5 is a flowchart illustrating a process for creating a policy for a group in one embodiment of the present invention;

Figure 6 is a flowchart illustrating a process for updating policy information on a client in one embodiment of the present invention; and

Figure 7 is a flowchart illustrating a method for changing a network connection while downloading data in one embodiment of the present invention.

DETAILED DESCRIPTION

Embodiments of the present invention provide systems and methods for enhanced network access. There are multiple embodiments of the present invention. By way of introduction and example, one illustrative embodiment of the present invention provides a method for a client device to seamlessly switch from a first network connection to a second.

As a mobile client device moves from a first location to a second location, the device is provided with an indication that the second network connection is available. The device determines a set of properties regarding the second connection, such as speed, reliability, and cost for the connection. The client device then evaluates these properties based on a set of policies, which are specified by the enterprise with which the user is associated, so that at any one time, the user is connected to the "best" network from the point of view of the enterprise. A rules engine automatically determines which of the two connections is most suitable based on the policies and the properties of the connection.

For instance, the second connection may be faster and cheaper than the first. However, the first connection is more reliable. The enterprise policies weigh speed and cost more highly than reliability. Thus, the client device automatically switches from the first connection to the second connection without any user intervention.

This introduction is given to introduce the reader to the general subject matter of the application. By no means is the invention limited to such subject matter. Illustrative embodiments are described below.

System Architecture

Various systems in accordance with the present invention may be constructed. Referring now to the drawings in which like numerals indicate like elements throughout the several figures, Figure 1 is a block diagram showing an illustrative environment for implementation of one embodiment of the present invention. The system shown in Figure 1 includes a client 102. The client is in communication with a security server 104.

Communication with the security server 104 occurs via a network 108. The network 108 may comprise a public or private network and may include the Internet. The network may also comprise a plurality of networks, including, for example, dedicated phone lines between the various components. In one embodiment, the client 102 communicates with the security server 104 via a virtual private network ("VPN") established over the Internet.

The security server 104 is also in communication with an enterprise server 106 via a network. The network 108 may comprise various elements, both wired and wireless. In one

embodiment, the communication between the security server 104 and enterprise server 106 occurs over a static VPN established over dedicated communication lines.

In one embodiment, a user connects a client device 102 to the network 108 using a network access user interface. The network access user interface is always on and only allows the user to connect to the network 108 via the interface. The network access user interface automatically causes the client 102 to connect to the security server 104 through the network 108. The security server 104 provides value added services to the client 102 and to one or more enterprises. Access to other services, such as the Internet, may be provided via the security server 104.

Although Figure 1 includes only a single client 102, security server 104, and enterprise server 106, an embodiment of the present invention will typically include a plurality of clients 102 and may include a plurality of security servers 104 and enterprise servers 106.

Figures 2 through 4 are block diagrams illustrating components on the client 102, security server 104, and enterprise server 106. Each of the components shown may be a third-party application, a custom application, or a combination of both. Each of the components may also be implemented in hardware, software, or a combination of hardware and software.

Client Devices

Figure 2 is a block diagram illustrating the modules present on a client device 102 in one embodiment of the present invention. Examples of client device 102 are personal computers, digital assistants, personal digital assistants, cellular phones, mobile phones, smart phones, pagers, digital tablets, laptop computers, Internet appliances, and other processor-based devices. In general, a client device 102 may be any suitable type of processor-based platform that is connected to the network 108, and that interacts with one or more application programs. The client device 102 can contain a processor coupled to a computer-readable medium, such as RAM. Client device 102 may operate on any operating system, such as Microsoft® Windows® or Linux. The client device 102 is, for example, a laptop computer executing a network access user interface.

The modules shown in Figure 2 represent functionality of the client 102. The modules may be implemented as one or more computer programs that include one or more modules. For instance, in one embodiment, all the modules shown in Figure 2 are contained within a single network access application. Also, the functionality shown on the client 102 may be implemented on a server in other embodiments of the present invention. Likewise,

functionality shown in Figures 3 and 4 as being on a server may be implemented on the client 102 in some embodiments of the present invention.

The client 102 shown in Figure 2 comprises a VPN client 202. The VPN client 202 allows the client 102 to connect to the enterprise server 106. In one embodiment of the present invention, the VPN client 202 is used to determine whether or not the VPN client 202 is active and whether or not the VPN client 202 is connected to a VPN server. For instance, an embodiment of the present invention may determine whether or not to connect to a particular service based on whether or not the VPN client 202 is enabled.

In another embodiment of the present invention, the VPN client 202 is used for four purposes: (1) to manage policy files, which include information, such as a gateway Internet Protocol (IP) address, secrecy and authentication level, and hash; (2) automatically connecting a VPN; (3) automatically disconnecting the VPN; and (4) monitoring the status of the VPN. Each of these four purposes may be affected by other modules, including, for example, the connection manager 210.

The client 102 also comprises a secure vault 204. The secure vault 204 protects content on the client 102. In one embodiment, the secure vault 204 is responsible for storing encrypted content on the client 102 and allowing access to the encrypted content based on a set of permissions or policies. In such an embodiment, a content creator can provide access via a viewer to secured content and allow a recipient of the content read-only access or allow the recipient to perform other tasks, such as modifying the content and forwarding it to other users. In another embodiment, the secure vault 204 allows the user to create and distribute secure content to other clients 102, the content creator can decide to send a document to several users and allow two of the users full access and one of the users read-only access.

The client 102 shown in Figure 2 also comprises a firewall 206. The firewall 206 allows port blocking via predefined policies. For instance, in one embodiment, an information technology ("IT") manager specifies port blocking based on two zones, a safe zone and a dangerous zone. The IT manager specifies one of these two zones for each of the network interface devices installed on the client 102. The IT manager is then able to set port-blocking rules by zone on the firewall 206.

For example, the IT manager may classify a Wireless Fidelity ("Wi-Fi") network interface as dangerous since it has traditionally been considered fairly unsafe. And the IT manager may apply more restrictive port-blocking rules to the dangerous zone than to the safe zone and network interface devices, such as those used to connect to a wired Local Area Network ("LAN") or a Personal Handyphone System ("PHS") cellular connection. The PHS

standard is a TDD-TDMA based microcellular wireless communications technology and has been traditionally considered relatively safer than Wi-Fi connections. The PHS cellular connection may also be referred to as a wireless wide area network ("WWAN") as opposed to a dial-up connection providing access to a wide area network ("WAN").

In various other embodiments, the port-blocking rules of the firewall 206 may be based on time of day, client IP address, terminating IP address, terminating and originating port, protocol, and other variables. In one embodiment, the port-blocking rules are based on policy data associated with individual users logged into the client 102.

In one embodiment, the port-blocking rules of the firewall 206 include a blacklist. The blacklist allows an IT manager to prevent an application from executing on the client 102. For instance, an IT manager may blacklist a DVD player so that a user is unable to view DVD's on the client 102. The firewall 206 may provide a message to the user informing the user that an application is unavailable.

In another embodiment, the firewall 206 implements a white list. The white list is somewhat more restrictive than the blacklist described above. The white list allows only specified applications to execute. For example, an IT manager may allow only MS Word, Excel, PowerPoint, and Outlook to execute. No other applications will be permitted to execute. The firewall 206 may be a custom firewall or a third-party firewall integrated into an embodiment of the present invention.

The embodiment shown in Figure 2 also includes an antivirus module 208. The antivirus module 208 shown determines whether policy files, virus dictionary, or other virus-related resources are out of date and provides the client 102 with a mechanism for updating the files or data. The antivirus module 208 may restrict access to various connections, applications, and other functionality when the policy files are out of date. For instance, the antivirus module 208 may restrict the client 102 to connecting to a single gateway through which the policy files are available. In one embodiment, the antivirus module 208 comprises a third-party antivirus product that is integrated with the other modules on the client 102.

The client 102 also comprises a connection manager 210, which includes a rules processor. In one embodiment, the connection manager 210 assigns a priority number to every connection, e.g., one to one hundred, and selects the connection with the highest number to connect to.

The connection manager 210 may provide a connection to a variety of networks, including, for example, dial-up, LAN, digital subscriber line ("DSL"), cable modem, Wi-Fi, wireless local area network ("WLAN"), PHS, and satellite.

In one embodiment, the connection manager 210 differentiates between public and private connections. A public connection is a connection provided by a service provider who has a relationship with the administrator of the security server 104, which allows the security server 104 to authenticate the connection. For instance, the security server 104 administrator may have a business arrangement with a hotspot provider. In order to connect, the client 102 connects to a local access point and the authentication of the user occurs automatically at the security server 104. In contrast, a private connection requires that all aspects of the authentication mechanism for a connection are managed in the absence of the security server 104, although the connection manager may provide certain facilities to allow for automated authentication where possible.

In one embodiment, the connection manager 210 makes connections available or unavailable to the client 102 based on policies present on the client 102. The connection manager 210 may also download changes to policy data and transmit quality of service ("QoS") and other data to the security server 104 or the enterprise server 106.

In one embodiment, the connection manager 210 determines the type of connections that are available based on signals provided by hardware associated with the client 102. For example, when the client 102 passes near a hotspot, a Wi-Fi card in the client 102 senses the hotspot and sends a signal to the connection manager 210. For instance, the Wi-Fi card may sense a broadcast service set identifier ("SSID"). Once the signal exceeds a threshold, the connection manager 210 provides a signal to a user of the client 102 that the network is available or may automatically connect to the hotspot. Alternatively, the Wi-Fi card may poll for a non-broadcast SSID. The connection manager 210 may provide a single connection to the client 102 at one time or may provide multiple connections to the client 102.

The client 102 shown in Figure 2 also comprises a QoS collector 212. The QoS collector 212 collects data values, including, for example, the number of bytes sent and received, the average transfer rate, the average signal strength at connection, termination cause, failed connections, and a network identifier. In another embodiment, the QoS collector 212 collects data during the session to determine when a connection provides inconsistent performance.

In one embodiment, the QoS collector 212 collects data regarding a connection during a session but does not send the data for a session until the next session. Thus, if a session is terminated abnormally, the QoS data will still be collected and transferred successfully. In another embodiment, the QoS collector 212 transfers data only when a particular type of connection is detected, such as a high-speed or low cost connection.

The client 102 also comprises a session statistics module 214. The session statistics module stores data representing user characteristics. For instance, the session statistic module 214 may store a list of the applications a user generally accesses, how often the user is connected, the typical CPU and memory utilization measure, keyboard sequences, and other characteristics of a user. If a particular user deviates from the expected characteristics by greater than a threshold, such as N standard deviations, and the significance of the statistic is more than a specified amount, the session statistics module 214 can identify the current user as a potential unauthorized user.

The session statistics module 214 may perform other tasks as well. For instance, in one embodiment, the session statistics module 214 pre-loads applications based on a user's general usage patterns.

The client 102 shown in Figure 2 also comprises a policy reader 216. In one embodiment, a company's policies are housed on the enterprise server 106. For instance, individual groups and users within an enterprise are identified and associated with policies, such as what types of connections they are able to access and what a user's VPN profile is. The user may also be able to specify a VPN policy on the client 102. In such an embodiment, the policy reader 216 downloads the policy rules from the enterprise server 106 and accesses local user policies and reconciles any conflicts between the two.

For example, an IT manager may establish a VPN profile to be used by a user when connecting to a Wi-Fi network. However, the user may wish to create a secondary VPN profile to be used if the first VPN becomes unavailable. The policy reader 216 loads both local and enterprise VPN profiles, resolving any conflict between the two VPN profiles.

In one embodiment, the policy reader 216 accesses data at an enterprise, department, and user level. In such an embodiment, some of the policy rules may be stored in a lightweight directory access protocol ("LDAP") server on the client 102, security server 104, or enterprise server 106. In another embodiment, the policy reader 216 receives only changes to policy data and does not typically download all of the policy data at once. Policies downloaded by the policy reader 216 may be provided to the rules processor of the connection manager 210.

The client 102 may also comprises a client security module 216. In one embodiment, the client security module 216 implements a client asset protection process. When the client security module 216 receives a signal indicating that the client asset protection process is to be executed, the client security module 216 may, for example, disable devices and interfaces

on the client device 102 and may, in some embodiments, encrypt the hard drive of the client device 102 so that the files stored on the drive are not easily accessible.

The client 102 may also comprise a user interface 220. The user interface 220 may control the underlying operating environment or the user's view of the underlying environment. For example, in one embodiment, the user interface 220 supplants the Microsoft® Windows operating system interface from the user's perspective. In other words, the user is unable to access many of the standard Windows features. Such a user interface may be implemented to limit the applications and configuration setting a user is able to access. In some embodiments, such as a personal digital assistant ("PDA"), no user interface is provided by an embodiment of the present invention; the standard PDA user interface is utilized.

The user interface 220 provides the user with an easy-to-use mechanism for accessing network connections. In one embodiment, when the user interface 220 is visible, it provides a very easy-to-use format that displays network connection types and provides other functionality to the user. For example, during complex operations, such as connecting to a new network type, the user can simply select a single button within the user interface 220 and the client 102 will properly disconnect from the previous network, acquire the new network, perform all authentication and policy-based requirements, and then allow the user to continue using an application on the new network. This simple, easy-to-use user interface 220, the complexity of which may be hidden and completely automatic, allows a less-technical user to successfully operate the client 102. All network connection, authentication, secure sign on, VPN parameters, and other aspects of the connection are managed by the user interface 220.

The client 102 shown in Figure 2 also comprises a security agent 222. In some embodiments, the security agent 222 is also referred to as a "bomb." In one embodiment, an IT manager indicates that the security agent 222 should be activated when the client 102 next connects to the enterprise server 106. The IT manager may do so because the client 102 has been reported stolen. Subsequently, the client 102 connects to the enterprise server 106, either directly or indirectly and receives the message to initiate the security agent 222.

In one embodiment, when the security agent 222 activates, it stops all applications from being able to run and encrypts the data on the hard drive of the client 102. For instance, the security agent 222 may implement a white list as described above and then implement a secure vault for all data on the client 102. The connection manager 210 may also be configured so that no connections are possible.

In one such embodiment, since the data is merely encrypted by security agent 222, rather than erased, the data may be recovered if the client 102 is subsequently recovered. For instance, the enterprise may retain the key needed for decrypting the local drive. The client 102 is returned to the enterprise, which then decrypts the drive. In another embodiment, the data on the local drive of the client is rendered inaccessible by, for example, writing over the data multiple times.

The client 102 shown in Figure 2 also comprises an out-of-band communication receiver 224. The out-of-band communication receiver 224 allows the client to receive communications other than through a network-based connection. The connection manager 210 may manage the out-of-band communication. For instance, the command to activate the security agent 222 may be transferred via a short messaging service ("SMS") communication received by the out-of-band communication receiver 224.

Security Server

Figure 3 is a block diagram illustrating the modules present on a security server 104 in one embodiment of the present invention. The security server 104 shown in Figure 3 comprises a remote authentication dial-in user service ("RADIUS") server 302, which may also be referred to as an AAA (authentication, authorization, and accounting) server. RADIUS is the standard by which applications and devices communicate with an AAA server.

The RADIUS server 302 provides authentication services on the security server 104. In some embodiments of the present invention, the RADIUS server 302 proxies to a RADIUS server on the enterprise server 106. In one embodiment, the RADIUS server 302 provides mutual authentication for the client 102 using Extensible Authentication Protocol Transport Layer Security ("EAP-TLS"). Although EAP-TLS itself is strictly an 802.1x authentication protocol, designed primarily for WiFi connections, the underlying TLS authentication protocol may be deployed in both wired and wireless networks. EAP-TLS performs mutual secured sockets layer ("SSL") authentication. This requires both the client device 102 and the RADIUS server 302 to have a certificate. In mutual authentication, each side may prove its identity to the other using its certificate and its private key.

The security server shown in Figure 3 also comprises an LDAP server 304. The LDAP server 304 uses the LDAP protocol, which provides a mechanism for locating users, organizations, and other resources on the network. In one embodiment of the present invention, the LDAP server 304 provides access control at the network layer to various components that an enterprise customer may or may not purchase. For example, a customer

may choose to implement a secure vault as described in relation to Figure 1. In such a case, the customer or users or groups associated with the customer are also associated with the firewall module. The LDAP entry is then used to determine that the firewall is to be enabled on a client.

In some embodiments, the LDAP server 304 is implemented as a list of user identifiers not using the LDAP protocol. In another embodiment, data in the LDAP server 304 is propagated from data present in the enterprise server 106.

The security server 104 shown in Figure 3 also comprises a session manager 306. The session manager 306 controls sessions, including sessions between the client 102 and enterprise server 106. In some embodiments, the session manager 306 also determines how to route data requests. For instance, the session manager 306 may determine that a particular data request should be routed to the Internet rather than to the enterprise server 106. This may be referred to as "splitting the pipe" and provides a mechanism to replace "split tunneling" (a traditional configuration option with most standard VPN clients) at the client device by the more secure split of traffic not intended for the enterprise at the security server, allowing monitoring of all traffic without the enterprise incurring the expense of the extra bandwidth required.

In some embodiments, the client 102 and enterprise server 106 establish a VPN for communication. In such an embodiment, the session manager 306 may be unable to route requests to any location other than the enterprise – the packets are encrypted and thus, cannot be separately evaluated.

In one embodiment, the session manager 306 performs automated authentication of a client device 102 or user. For example, if the session manager 306 determines that a client 102 is approaching a Wi-Fi hotspot, the session manager 306 is able to pre-populate the hotspot with the certificate that the hotspot requires to authenticate the user. In this manner, the authentication appears very fast to the user. The session manager 306 may also control the manner in which data is queued for download to the client device 102.

In one such embodiment, the session manager 306 provides two modes for data queuing. In a first mode, the session manager 306 determines that the network down time will be brief, e.g., the user is moving through a tunnel, which interferes with network access. In such a case, the session manager queues a minimal amount of data. In a second mode, the session manager 306 determines that the network down time will be of a longer duration, e.g., the user is boarding a plane from New York to Tokyo. In such a case, the session manager 306 may queue a larger amount of data. In one such embodiment, the session manager 306

determines the mode by querying the user for the downtime interval. When the user reconnects to the security server 104, the session manager 306 determines the best manner of downloading the queued data and begins the download.

In one embodiment, the session manager 306 comprises a packet shaper (not shown). The packet shaper provides various functional capabilities to the session manager 306. For example, in one embodiment, the packet shaper provides a mechanism for prioritizing packets sent between the enterprise server 106 and the client 102. In one embodiment, the packet shaper utilizes Multiprotocol Label Switching ("MPLS"). MPLS allows a specific path to be specified for a given sequence of packets. MPLS allows most packets to be forwarded at the switching (layer 2) level rather than at the (routing) layer 3 level. MPLS provides a means for providing QoS for data transmissions, particularly as networks begin to carry more varied traffic.

The session manager 306 may also provide session persistence capabilities. For instance, in one embodiment, when a user drops a connection or moves from one provider network coverage area to another, the connection manager 306 persists a virtual connection as the first connection is terminated and the second is initiated.

The session manager 306 may include a server-side rules engine. The server-side rules engine may use historical information, such as the session statistics described above, for statistical attack determination. For instance, session manager 306 may access a stored statistic regarding a client device 102 and based on monitoring of the current statistics for the client device 102 determine that an unauthorized user is using the client device 102.

The security server 104 shown in Figure 3 also comprises a real-time monitor 308. The real-time monitor 308 monitors the status of communications, such as which clients and users are logged on, the amount of data being transferred, ongoing QoS measures, ports in use, and other information.

When the real-time monitor 308 detects a problem, it may issue an alert to network support. In one embodiment, data from the real-time monitor 308 is provided to users via a portal available on the security server 308. In another embodiment, the real-time portal 308 transfers information to the enterprise server 106, from which users access the data.

The embodiment shown in Figure 3 also comprises a historical monitor 310. The historical monitor 310 provides information similar to the real-time monitor 310. However, the underlying data is historical in nature. For instance, in one embodiment, the historical monitor 310 provides audit information for making intelligent business decisions and for dealing with regulatory compliance issues.

The information available via the historical monitor 310 may include, for example, historical QoS data, registration compliance data, and metrics consistency data. The historical data monitor 310 may be used to determine that certain clients are not performing optimally by comparing metrics of various clients over time. For instance, by evaluating information available via the historical data monitor 310, a support person may be able to determine that a radio tuner on a specific client device 102 is failing. If the user of one client device 102 is complaining about the availability of service, but other users are able to successfully access service, then the client device's radio may be the problem.

The historical data monitor 310 may also be used to reconcile information captured on the security server 104 regarding connections and data provided by telecommunication carriers. The data may be used to determine when certain resources need to be increased and when a certain carrier is not performing adequately.

The security server also comprises a database 312. In embodiments of the present invention, the database 312 may be any type of database, including, for example, MySQL, Oracle, or Microsoft SQL Server relational databases. Also, although the database 312 is shown as a single database in Figure 2, the database 312 may actually comprise multiple databases, multiple schemas within one or more databases, and multiples tables within one or more schemas. The database 312 may also be present on one or more other machines, e.g., database servers.

In one embodiment of the present invention, the database 312 stores customer information regarding enterprises served by the security server 104, such as a list of valid users, a list of valid cellular cards, the relationships between the individual users and groups within the enterprise, and other customer information.

For example, in one embodiment, the database 312 stores an association between users and cellular data cards. The enterprise may allocate a single user to a specific data card. Alternatively, the enterprise may associate a group of users with a group of cellular data cards. Other types of data may also be stored in the database 312, such as billing data.

The security server 104 shown in Figure 3 also comprises a QoS server 314. The QoS server 314 uploads information from the QoS collector 212 on the client device 102 and stores the QoS data. The QoS server 314 can collect data from multiple clients and store it in the database 312.

The security server also comprises a QoS tools engine 316. The QoS tools engine 316 displays data made available by the QoS server 314 and other processes, such as the real-time monitor 308.

In one embodiment, the QoS tools engine 316 provides an aggregation of QoS data in a spreadsheet. In another embodiment, the QoS tools engine 316 provides data using map views, pie charts, and graphs. The QoS tools engine 316 may also provide the capability for setting QoS-based alarms and may provide data to users via a portal.

In the embodiment shown in Figure 3, the security server 104 also comprises a portal server 318. The portal server 318 may be, for example, a web server. Any standard web server application may be utilized, including Microsoft® Internet Information Server ("IIS") or Apache.

Although the security server 104 shown in Figures 1 and 3 is illustrated as a single server, it may comprise multiple servers. For example, in one embodiment of the present invention, the security server 104 comprises multiple regional servers.

Also, the description above suggests that data is provided to and queried from the security server 104 by the client 102, i.e., the client pulls the data. However, in some embodiments, the client 102 also comprises a listener (not shown) so that the security server 104 can push data to the client 102.

Enterprise Server

Figure 4 is a block diagram illustrating the modules present on an enterprise server 106 in one embodiment of the present invention. The enterprise server 106 may also be referred to herein as a customer server and may comprise one or more servers for one or more enterprises linked to one or more security servers 104.

The enterprise server 106 shown in Figure 4 comprises a policy server 402. The policy server 402 provides a means for managing the policy rules, including, for example, available VPN profiles, available transports (e.g. WiFi, LAN, PHS, Dialup), firewall rules, such as blacklists and white lists, connection rules, and antivirus rules. The policy server 402 may include other rules as well, such as the level of data throttling to perform for each client or group of clients. Data throttling limits the data transfer rate to a particular client 102 so that connection resources can be optimized.

The policies may be managed at one or more levels. For example, an IT manager may wish to create a VPN profile for the enterprise as a whole, but a different VPN profile for an engineering group since the engineering group needs access to various unique applications.

The policy server 402 may also provide a mechanism for configuring the location of various servers that the client 102 will utilize. For instance, the policy server 402 may allow an IT manager to specify the IP address of an acceleration server 404 or a vault server 406

In one embodiment, the policy server also allows the IT manager to specify which users receive updates for various components on the client 102. The policy server 402 may also allow the IT manager to perform connection configuration. For instance, the IT manager may use the policy server to specify phone numbers for PHS connections, Wi-Fi SSID's for private connections, and other connection configuration information.

The enterprise server 106 shown in Figure 4 also comprises an acceleration server 404. The acceleration server 404 performs processes to improve the performance of data transfer. For instance, the acceleration server 404 may automatically compress images that are to be transferred to a client 102.

In one embodiment, the acceleration server 404 communicates with the policy server 402. An IT manager sets acceleration rules using the policy server 402, and the acceleration server 404 uses these rules to determine what level of acceleration to use for a particular communication. In one embodiment, the IT manager sets a default level of acceleration for all communication and a specific level of acceleration for one group of users. The specific level of acceleration may be referred to as an override.

The enterprise server 106 also comprises a vault server 406. The vault server comprises two components, an automatic component and an administration component. In one embodiment, the automatic component integrates with an enterprise's mail server (not shown) and performs operations on emails to and from the mail server. For instance, the vault server 406 may quarantine an email, automatically encrypt the email before it is sent, add a legal disclaimer to an email, or perform other functions on the email.

In one embodiment, the automatic component of the vault server 406 searches an email based on words or based on the domain or specific address to which the email is addressed or from which the email originated. Using this information, the user can perform functions on the email, such as those described above.

The administration component of the vault server 406 allows a user to terminate access to secure content, either by a specific user or by all users. It also logs activity. Using one embodiment of the vault server 406, a user can indicate that a set of users whose employment has been terminated will no longer have access to any secure content. In an alternative embodiment of the vault server 406, a user can indicate that a given element of secure content, say a price list, is now out of date, and so that piece of secure content will no longer be viewable by any user. When each user accesses the secure content, the vault server 406 logs the event. So for each secure content element, the vault server 406 creates a log of all activity on the secure content.

In one embodiment, the vault server 406 also compresses data. For instance, one embodiment utilizes standard PKZIP compression to compress all content. In another embodiment, an IT manager may identify three types of images and specify a different level of compression for each type of image based on the level of resolution necessary for each type of image.

The enterprise server 108 also comprises a RADIUS server 408 and LDAP server 410, which are similar to those described above in relation to the security server 104. The RADIUS server 302 on the security server 104 may proxy to the RADIUS server 408 on the enterprise server 106. Similarly, data in the LDAP server 410 may be propagated to the LDAP server 204 on the security server 104.

The enterprise server 106 also comprises a one-time password ("OTP") server 412. The OTP server 412 provides a mechanism for authentication. For instance, in one embodiment of the present invention, the enterprise server 106 uses the OTP server 412 to perform a mutual authentication process.

The enterprise server 106 also comprises a concentrator 414. The concentrator 414 provides remote access capability to the client 102. For instance, the concentrator 414 may serve as a means for terminating a VPN between the client 102 and enterprise server 106.

The enterprise server 104 shown in Figure 4 also comprises a portal server 416. The portal server 416 may comprise a standard web server, such as IIS or Apache. The portal server 416 may provide one or more portals. For example, in one embodiment, the portal server 416 provides two portals, portal one and portal two.

Portal one provides a configuration interface for managing the various elements shown in Figures 2 and 3, including, for example, the policy server 402 and LDAP server 410. Portal two provides an interface for accessing data, such as QoS data and session data.

For instance, a user may use historical QoS data on portal two to determine how a particular provider is performing in terms of throughput, user connections, and other QoS metrics. Portal two may also provide real-time information, such as how many users are currently connected.

For instance, in one embodiment, an IT manager determines that twenty users have been rejected by a carrier in the last three minutes due to authentication failure and five users with the same user identifier are currently logged on to five different devices. The IT manager uses this information to detect a potential security problem. Portal two may also be used to set alerts as described above.

It should be noted that the present invention may comprise systems having a different architecture than that which is shown in Figures 1 through 4. For example, in some systems according to the present invention, the security server 104 and enterprise server 106 may comprise a plurality of security and enterprise servers. The system 100 shown in Figures 1 through 4 is merely illustrative, and is used to help explain the illustrative systems and processes discussed below.

Illustrative Methods of Enhanced Network Access

The following illustrative embodiments utilize a central policy server 402 on an enterprise server 106. The client device 102 downloads policies from the policy server 402 and the connection manager 210 utilizes the policies to make connections. In other embodiments, policy files are created and distributed to the client device 102 in other ways. For example, an email attachment or disk may be distributed to each client device 102. Each time an update is necessary, a new disk or email is distributed.

In embodiments of the present invention, policies are created and distributed to client devices 102. The client devices 102 utilize the policies for making connections. Figure 5 is a flowchart illustrating a process for creating a policy for a group in one embodiment of the present invention.

In the embodiment shown in Figure 5, policy administrator first determines a policy 502. The policy may be based on a variety of factors, such as, for example, regulatory issues, the type of data and/or applications to be used, the level of control desired by the enterprise, the physical environment in which a client device or group of client devices will operate, the experience and technical knowledge of the user group associated with the policy, and the job to be performed by the group or groups associated with the policy. The policy may include various elements, including, for example a list of allowed connections or applications and a list of disallowed connections or applications, acceleration preferences, and a VPN profile. The policy may also include connection preferences of the enterprise or of the users. For instance, an enterprise may decide not to use certain WiFi hotspots. The policy may vary by time of day.

The policies may be based on a number of factors, including, for example, an enterprise's need to minimize overall transport cost when billed on a usage basis, an enterprise's wish to minimize perceived security exposure based on assumed insecurity on some transports and specific connections, and an enterprise's wish to ensure the highest speed and most reliable usage experience for their users. The policies may be based on third party

parameters as well. For instance, the policy may be based on the enterprise's security provider's desire to minimize its transport costs overall.

The policy administrator next selects a group to be associated with the policy 504. The administrator may manually enter group names and user identifiers. Alternatively, the administrator may select groups from a central directory, such as the LDAP 410 or a Microsoft Active Directory Server. Each policy may be associated with, for example, an enterprise, a group within the enterprise or across enterprises, or with an individual.

Once the administrator has created a policy and associated the policy with a group, the administrator saves the policy-group association 506. The policy-group association may be stored in a database (not shown) in communication with the policy server 402. Alternatively, the policy-group association may be stored in a file, for example, in an XML format in a file.

The administrator then causes the policy and policy-group association to be distributed to client devices 508. For instance, the policy and policy-group association may reside in the database, which is in communication with the policy server 402, so that when a client device attempts to download a policy, the policy-group association is used to determine which policy or policies to download. The policy and policy-group association may be distributed via a network, such as network 108, or by media, such as CD-ROM. In one embodiment, only changes to the policies are downloaded. In other embodiments, all policies are downloaded each time a download occurs.

In some embodiments, once the policies are downloaded to the client device, the user may make changes to them. For instance, the user may set up an alternative VPN profile on the client if the VPN associated with the VPN profile downloaded from the policy server 402 is temporarily unusable.

Figure 6 is a flowchart illustrating a process for updating policy information on a client in one embodiment of the present invention. In the embodiment shown, the policy reader 216 on the client device 102 loads policies 602. For instance, the policies may exist in an XML file, which the policy reader 216 opens and reads.

The connection manager 210 then determines what the most recently used connection was and whether the most recently used connection is available 604. For example, a user may shut down a client device 102 while the client device 102 is connected to a WiFi hotspot. When the user starts the client device 102, the client device will attempt to connect to the WiFi hotspot.

If the client device 102 is not able to connect to the most recently used connection, the client device 102 attempts to identify a new connection 606. For example, the client device 102 may have moved out of range of the WiFi hotspot to which the client was connected. The client device 102 identifies all currently-available connections. The client device 102 also identifies one or more policies associated with the user. The client device 102 then identifies properties of the network connection or connections and compares the network properties to the policy (rule). A network property may be, for example, quality of service measures, such as security, reliability, and speed may be utilized. The client device 102 may also use cost or a combination of cost and a plurality of other properties in making the determination. In one embodiment, the client device 102 applies a normalization algorithm to the plurality of properties to come up with a single number for each network connection. The client device 102 then compares the single numbers to determine to which network to connect.

Using either the most recently used connection or the newly-identified connection, the client device connects to the policy server (402) 608. For instance, the client device 102 may connect to the most recently used WiFi hotspot and then establish a connection with the policy server 402 and the QoS server 310 over the Internet.

Once the client device 102 has established a connection with the network, the client device uploads QoS data to the QoS server (310) 610. In one embodiment, QoS data from the previous session is uploaded at the start of the current session so that interruptions in service, such as a lost connection, can be accurately tracked.

The client device next downloads the latest policy data from the policy server (402) 612. The policy data may comprise only changes since the last connection. For example, the client device 102 may store a last download date and only download policies from the policy server 402 that have been created or changed since the last update date. The client device may download other information as well. For instance, the administrator may determine that a particular client device 102 has been stolen and set an indicator to cause the client device to encrypt data on its hard drive. When the client device 102 connects, it downloads the indicator.

The process may be transparent to the user. In one embodiment, the download process runs as a service. Each time the client device 102 starts up, the process executes. The process may also include having the client device 102 connect to a VPN automatically so that the user can access enterprise applications.

Figure 7 is a flowchart illustrating a method for changing a network connection while downloading data in one embodiment of the present invention. In the embodiment shown, the connection manager 210 receives an indication to change network connections 702. The indication may be due to an identification of a newly available network, a manual selection by a user, or some other indication. For instance, a hardware device, such as a cellular data card, may indicate that a new connection is available. The user receives the indication and decides to change to the new network and clicks a button on a user interface, indicating the desire to change.

In one embodiment, the connection manager 210 identifies a new network. The connection manager then compares a first property of the currently connected (existing) network to a first property of the second new network. The properties may signify the same or similar information about the two networks, e.g., the type of network. Based on policies, the connection manager 210 determines to which network to connect.

In one embodiment, the connection manger 210 rules engine makes connection decisions based on six core pieces of data for connection that is physically available (the correct device is installed and operating, and a signal is available):

(1) Is the connection allowed for this user;

(2) How secure is the connection deemed to be;

(3) How reliable is the connection deemed to be;

(4) How fast is the connection deemed to be;

(5) How expensive is the connection relative to others for the enterprise; and

(6) How expensive is the connection relative to others for a service provider, such as a network security service provider?

Item (1) in this list is specified based on whether or not the connection is available to the enterprise in general and whether the enterprise has made the connection available to the user (or, more precisely in some implementations, not barred the user from the connection). Item (2) is based on enterprise preference indication. It could also be based on attack detection algorithms automatically applied, e.g., if relatively more attacks on a specific type of connection or specific location are detected, then relatively more attacks are occurring.

Item (3) is based on connection statistics. In one such embodiment, the enterprise has the option to indicate perceived relative reliability measures. Item (4) is also based on connection statistics. Item (5) is based on the pricing plan that the enterprise has entered into with the provider. And item (6) is based on carrier pricing arrangements and usage assumptions for various connections.

One embodiment of the present invention takes each of these six items and uses a normalization algorithm to work these elements (with their relative strengths) into a "weighting" within a range. Then, the rules engine on the client device 102 simply selects the connection with the highest weighting.

In some cases, despite the rules based analysis, an enterprise may not wish for a user to use a specific connection for a given, short period of time. In one embodiment, the system allows the enterprise to specifically exclude a connection for a short time.

Before disconnecting, the connection manager 210 sends a signal to the session persistence server 316 to suspend any currently active data transfer 704. By suspending data transfer, the connection manager 210 helps to eliminate the potential for losing data.

The connection manager 210 then disconnects the client device 102 from the network (108) 706. The process for disconnecting may differ between various networks. During the period when the client device 102 is disconnected, the session persistence server 316 caches data. After a period of time, which may be very brief, the connection 210 manager attempts to reconnect to a network 708. The network 108 may be the most recently used network or may be a newly identified network. The connection may be dropped for a period of time. In one embodiment, a user may specify the duration that the user expects to be disconnected when the disconnect occurs. The persistence server 316 uses this information to determine how much data to cache during the period of disconnection.

The connection manager 210 or persistence server 316 then determines whether the download that was occurring before the disconnect should continue 710. For instance, the connection manager 210 may determine that the new connection is too slow to support the data download. The connection manager 210 may also look to the policies to determine what rules apply to the connection.

If the download, should continue, the connection manager 210 resumes the data transfer 712. The data transfer may then complete or may be subject to subsequent disconnects. If the new network is not suitable to support the download, or if the download is complete, the process ends 714.

For example, in one embodiment, a salesperson needs to download a large document containing a price list. The salesperson's computer is currently connected via a wide area network connection, which is relatively slow. The salesperson enters a coffee shop that the salesperson knows has a high speed WiFi connection.

When the client device 102 indicates that the WiFi connection is available, the user indicates that the client device 102 should change networks. The client device seamlessly

connects to the WiFi network and, based on rules established in the policies, begins downloading the document. If the user must leave the coffee shop before the download is complete, the connection manager 210 can signal the session persistence server 316 to pause the download until the user reenters the coffee shop or connects to another high-speed network.

In one embodiment, session persistence operates on the following process: when a disconnection event occurs, the connection manager 216 buffers application data coming to the client device 102, making applications "believe" that they are still connected. At the same time, session persistence server 216 buffers information on the server side, making the server 104 "believe" that it is still connected. Once a network connection has been reconnected, the connection manager 210 and session persistence server 316 empty the buffers that have built up on both sides.

One such embodiment implements a kernel mode driver at the NDIS layer in the Microsoft Protocol stack (roughly equivalent to layer 3 in the OSI model). This kernel mode driver is implemented as an "Intermediate Driver" on the Microsoft W2K/WXP operating systems. The driver acts as a single "virtual device" through which all network communications goes. This single device routes this traffic to the appropriate physical device (directed through a virtual device associated with a third-party VPN when appropriate), depending on the current physical connection.

In order to make application layer components believe that a network is still up and running, no "disconnect" signal is transmitted to the application layer components when a network interruption occurs. In this way, application layer components treat the connection as if it is simply slow.

The primary interface component between the client 102 and server 104 in such an embodiment is an indication that a client will be disconnecting for a long period of time, but wishes to persist the session over this extended time. In this case, the client 102 provides the user a means to enter the time that the system will be un-connected (say for the duration of a domestic flight), and the client notifies the server of the expected length of the disconnection event.

On the server 104, the session persistence server 316 functions as a proxy for connections from clients to network resources. Be those resources at the enterprise data center or public resources. The server implementation includes a similar intermediate driver architecture to that on the client, combined with application layer components to manage caching locations and recording for billing purposes. There may be cases where enterprises

wish caching to occur at the enterprise. In this case, the system allows for the cache to be on the other side of a static tunnel to the enterprise.

General

The foregoing description of the embodiments of the invention has been presented only for the purpose of illustration and description and is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Numerous modifications and adaptations thereof will be apparent to those skilled in the art without departing from the spirit and scope of the present invention.

That which is claimed:

1. A method comprising:

receiving a request to connect to a network, the request associated with a user;

determining a policy associated with the user;

identifying at least one available network connection;

determining at least one property of the at least one available network connection;

evaluating the property based at least in part on the policy; and

selecting the at least one available network connection based on the evaluation.

2. The method of claim 1, wherein the policy comprises a list of allowed connections.

3. The method of claim 1, wherein the policy comprises a list of disallowed connections.

4. The method of claim 1, wherein the property comprises a property selected from the group consisting of security, reliability, speed, and cost.

5. The method of claim 1, wherein the at least one property comprises a plurality of properties and further comprising applying a normalization algorithm to the plurality of properties.

6. The method of claim 1, wherein determining the policy comprises retrieving the policy from a central policy repository.

7. The method of claim 1, wherein the at least one available network connection comprises a public connection.

8. The method of claim 1, wherein the at least one available network connection comprises a private connection.

9. The method of claim 1, further comprising receiving a quality of service datum associated with the at least one available network connection.

10. The method of claim 1, wherein the at least one available network connection comprises a plurality of available network connections.

11. A method comprising:

receiving an indication that a new network connection is available for a client device associated with a user;

determining at least one first property associated with the new network connection;

determining at least one second property associated with an existing network connection;

determining a policy associated with the user;

evaluating the at least one first property based at least in part on the policy;

evaluating the at least one second property based at least in part on the policy;

disconnecting from the existing network connection; and

connecting to the new network connection.

12. The method of claim 11, further comprising signaling that the new network connection is available.

13. The method of claim 11, further comprising before disconnecting from the existing network connection, opening a data cache for buffering data during a disconnection.

14. The method of claim 13, further comprising after connecting to the new network connection:

receiving data from the data cache; and

closing the data cache.

15. The method of claim 13, further comprising receiving a measure for determining the size of the data cache.

16. The method of claim 15, wherein the measure comprises an estimated disconnection duration.

17. The method of claim 11, wherein the indication that a new network connection is available comprises a signal from a hardware device.

18. The method of claim 17, wherein the hardware device comprises an adapter selected from the group consisting of a WiFi adapter, a LAN adapter, a cellular adapter (WWAN), and a dial-up (WAN) adapter.

19. A computer-readable medium on which is encoded program code, the program code comprising:

program code for receiving a request to connect to a network, the request associated with a user;

program code for determining a policy associated with the user;

program code for identifying at least one available network connection;

a policy reader operable to determine a policy associated with a user;

a connection manager operable to:

receive a request to connect to a network, the request associated with a user;

identify at least one available network connection;

determine at least one property of the at least one available network connection;

evaluate the property based at least in part on the policy; and

select the at least one available network connection based on the evaluation.

27. The system of claim 26, further comprising a quality of service collector operable to receive a quality of service datum associated with the at least one available network connection.

28. A system comprising:

a policy reader operable to determine a policy associated with a user;

a connection manager operable to:

receive an indication that a new network connection is available;

determine at least one first property associated with the new network connection;

determine at least one second property associated with an existing network connection;

evaluate the at least one first property based at least in part on the policy;

evaluate the at least one second property based at least in part on the policy;

disconnect from the existing network connection; and

connect to the new network connection.

program code for determining at least one property of the at least one available network connection;

program code for evaluating the property based at least in part on the policy; and

program code for selecting the at least one available network connection based on the evaluation.

20. The computer-readable medium of claim 19, further comprising program code for receiving a quality of service datum associated with the at least one available network connection.

21. A computer-readable medium on which is encoded program code, the program code comprising:

program code for receiving an indication that a new network connection is available;

determining at least one first property associated with the new network connection;

determining at least one second property associated with an existing network connection;

determining a policy associated with a user;

evaluating the at least one first property based at least in part on the policy;

evaluating the at least one second property based at least in part on the policy;

disconnecting from the existing network connection; and

connecting to the new network connection.

22. The computer-readable medium of claim 21, further comprising signaling that the new network connection is available.

23. The computer-readable medium of claim 21, further comprising before disconnecting from the existing network connection, opening a data cache for buffering data during a disconnection.

24. The computer-readable medium of claim 23, further comprising after connecting to the new network connection:

receiving data from the data cache; and

closing the data cache.

25. The computer-readable medium of claim 23, further comprising receiving a measure for determining the size of the data cache.

26. A system comprising:

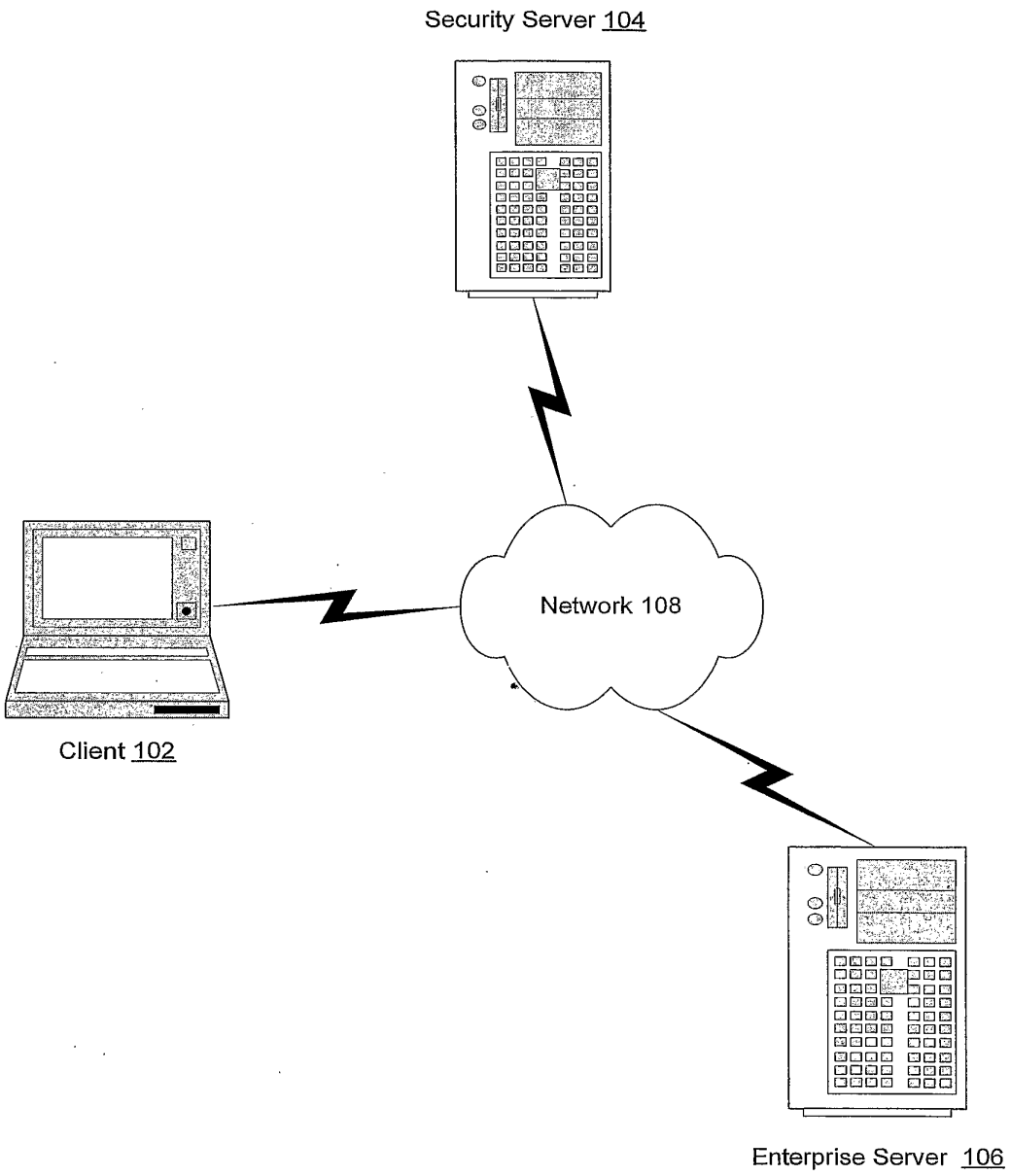

Security Server 104
Network 108
Client 102
Enterprise Server 106

Figure 1

Client 102

202 Client VPN
204 Secure Vault
206 Firewall
208 Antivirus
210 Connection Manager (Rules Processor)
212 QoS Collector
214 Session Statistics
216 Policy Reader
218 Client Security
220 User Interface
222 Security Agent
224 Out-of-Band Communication Receiver

Figure 2

3/7

Security Server 104

302 RADIUS Server (AAA)
304 LDAP
306 Session Manager
308 Real-time Monitor
310 Historical Monitor
312 Database
314 QoS Server
316 QoS Tools Engine
318 Portal Server

Figure 3

Enterprise Server 106

402 Policy Server
404 Acceleration Server
406 Vault Server
408 RADIUS Server
410 LDAP
412 OTP Server
414 Concentrator
416 Portal Server

Figure 4

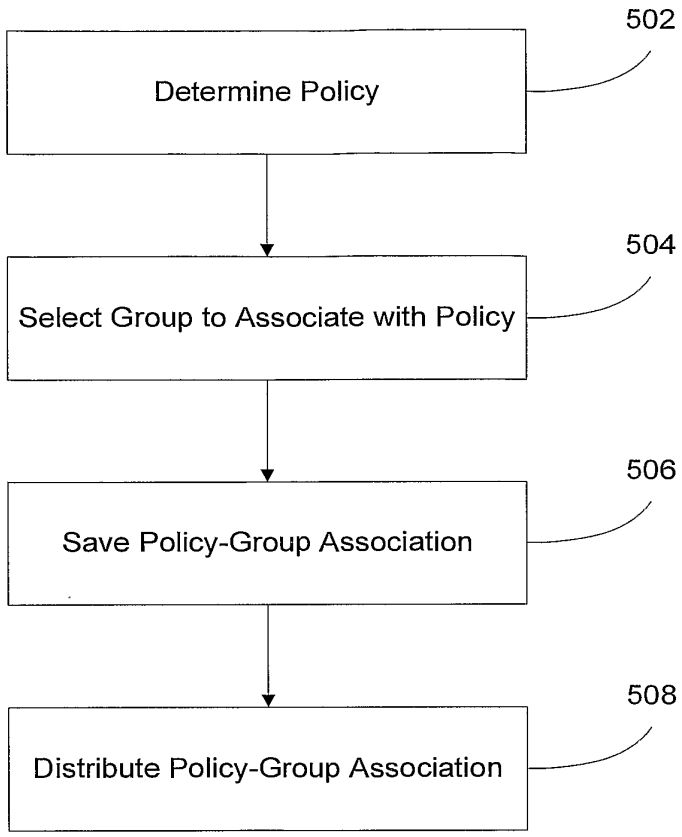

502
Determine Policy
504
Select Group to Associate with Policy
506
Save Policy-Group Association
508
Distribute Policy-Group Association

Figure 5

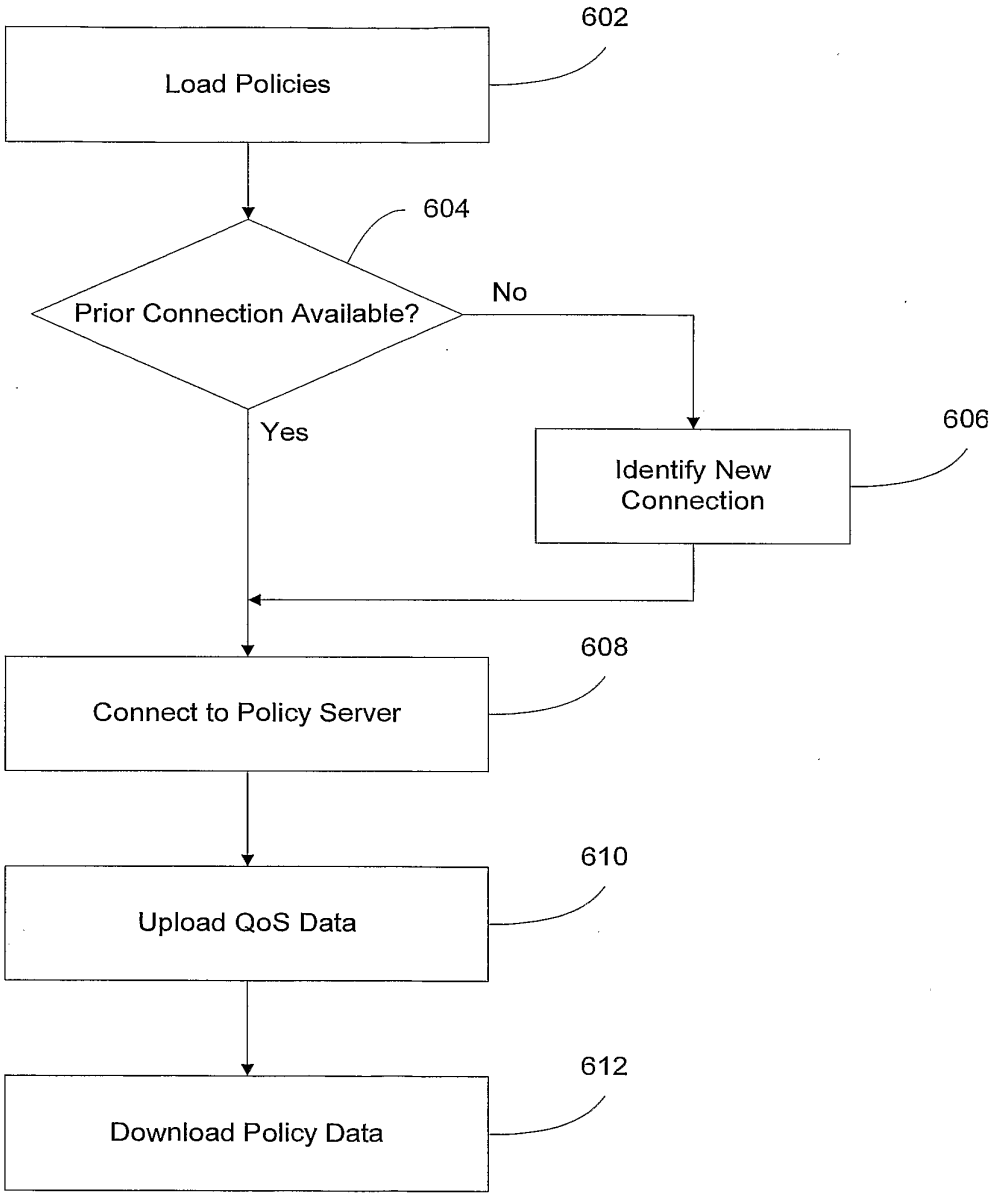

602
Load Policies
604
Prior Connection Available?
No
Yes
606
Identify New Connection
608
Connect to Policy Server
610
Upload QoS Data
612
Download Policy Data

Figure 6

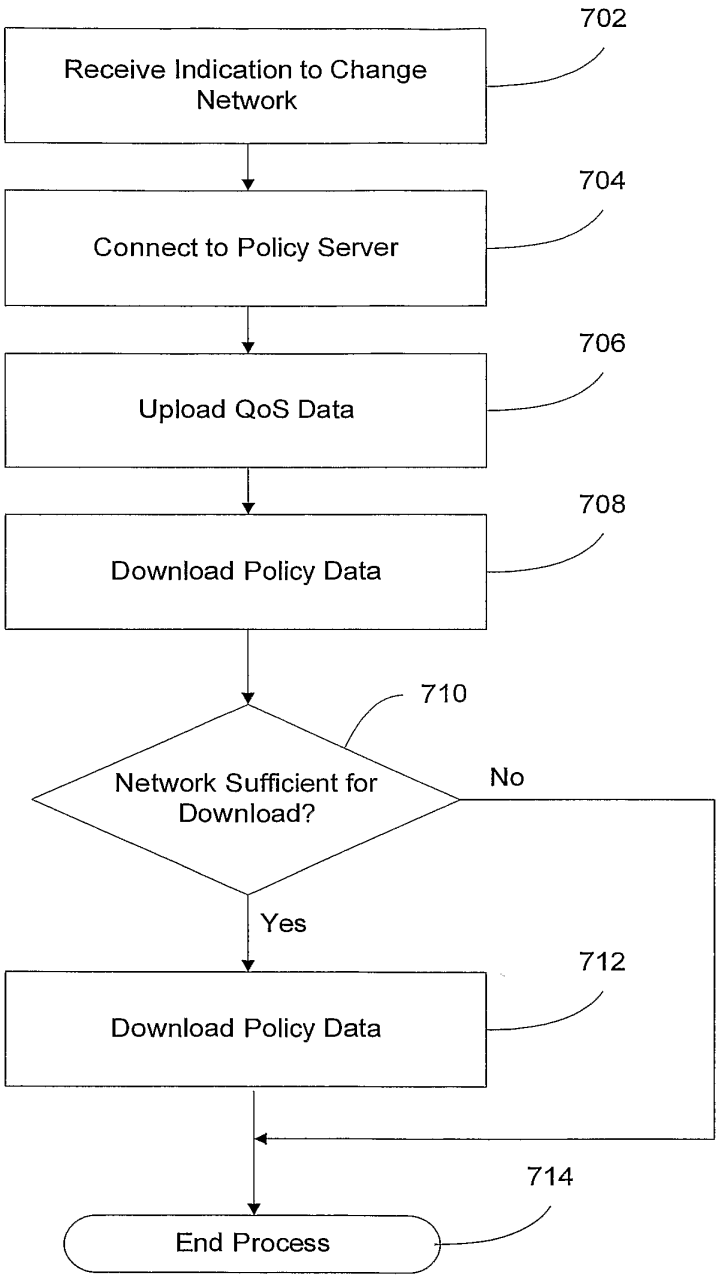

Receive Indication to Change Network
702
Connect to Policy Server
704
Upload QoS Data
706
Download Policy Data
708
Network Sufficient for Download?
710
No
Yes
Download Policy Data
712
End Process
714

Figure 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022982

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/073782 A (NOKIA CORPORATION; JOERESSEN, OLAF) 4 September 2003 (2003-09-04) abstract page 1, line 7 - page 2, line 31 page 3, line 6 - page 4, line 27 page 5, line 27 - page 8, line 24 -/--	1-28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October 2005	27/10/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kopp, K

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022982

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/23362 A (NETMOTION WIRELESS, INC; HANSON, AARON, D; STURNIOLO, EMIL, A; MENN, A) 21 March 2002 (2002-03-21) abstract page 1, line 5 - line 12 page 4, line 11 - line 22 page 5, line 10 - line 23 page 6, line 6 - line 21 page 7, line 21 - page 8, line 3 page 11, line 15 - page 14, line 17 page 15, line 18 - page 16, line 2 page 17, line 9 - line 10 page 18, line 23 - page 21, line 18 page 22, line 5 - line 15 page 23, line 12 - line 27 figure 1	1-28
X	US 2004/123150 A1 (WRIGHT MICHAEL ET AL) 24 June 2004 (2004-06-24) abstract figure 6a paragraph '0005! paragraph '0007! - paragraph '0009! paragraph '0012! paragraph '0028! paragraph '0040! - paragraph '0042! paragraph '0044! paragraph '0046! paragraph '0085! - paragraph '0086!	1-28
A	WO 02/077816 A (BOT, INC; USZOK, ANDRZEJ; KUNSTMAN, PAWEL) 3 October 2002 (2002-10-03) page 25, line 3 - line 12	2,3
A	US 5 748 084 A (ISIKOFF ET AL) 5 May 1998 (1998-05-05) abstract figures 3,4 column 1, line 4 - line 7 column 1, line 48 - column 3, line 4 column 3, line 46 - line 53 column 4, line 3 - line 33 column 4, line 62 - column 5, line 33 column 5, line 59 - column 6, line 15 column 6, line 31 - line 54 column 9, line 53 - column 10, line 31	1-28

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2005/022982

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03073782 A	04-09-2003	AU 2002233595 A1	09-09-2003
		EP 1479257 A1	24-11-2004
		US 2005148359 A1	07-07-2005
WO 0223362 A	21-03-2002	CA 2421609 A1	21-03-2002
		EP 1364296 A1	26-11-2003
		JP 2004509539 T	25-03-2004
US 2004123150 A1	24-06-2004	US 2004123153 A1	24-06-2004
WO 02077816 A	03-10-2002	NONE	
US 5748084 A	05-05-1998	NONE	

Form PCT/ISA/210 (patent family annex) (January 2004)

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JP2005339247

【課題】

[Problem] without entering a user ID and password automatically authenticates the user, and provides a two-way one-time ID authentication system that does not perform the authentication in the content server. Define the initial authentication code in accordance with the registration of the user ID that is defined in A URL of the content server and the content server, authentication key for the URL of the content server, user ID, and a two-way one-time ID authenticates the initial authentication code managed in association with the authentication server, and mobile terminal to perform to install the authentication key from the authentication server authentication server and the two-way one-time ID authentication, and a gateway server to the mobile terminal to access, the mobile terminal, gateway carries out bidirectional one-time ID authentication using the authentication key with the authentication server via the server, a bidirectional one-time ID authentication system requests a content to the content server via a gateway server when authentication is successful is there. .FIELD 6

Two-way one-time ID authentication system and authentication method

[0001]

[0001] The present invention relates to a bidirectional one-time authentication system and an authentication method for performing a bidirectional one-time ID authentication between the mobile terminal and the server

[0002]

[0002] The content server that provides e-commerce and financial transactions of the service is widely known via the Internet. As shown in FIG. 24, the user communicates over the Internet with the content server using the mobile device or computer or the like, actually the user ID and password, etc. in advance determined when using the service on the input to have authenticated, it may be utilized. In other words, the content server by using the user ID and password, and the like that has been input, take the integrity of the user information, to identify a user who comes to access, and to allow the request if the legitimate user. Patent 2003-1 62507

[0003]

[0003] However, the user ID and password, and the like guess by a third party, there is a fear that leakage, or are prying eyes, if there is such a thing, would also be available easily content server is a third party, there is a fear that is the illegal commerce and financial transactions. Further, the user information managed by the content server, in addition to such as a user ID and a password, for example, the user's address and phone number, E-mail address, date of birth, bank account number or credit used for settlement since even personal information number or the like are managed, the user ID and password, etc. to a third party would be known, there is a possibility that, also known these information at the same time. Therefore, the user has a problem that can not be utilized with confidence services such as e-commerce and financial transaction provided by the content server.

[0004]

[0004] paying attention to these problems, the present invention is, and automates the authentication of users without having to enter a user ID and password, and, two-way one-time ID authentication system and is not carried out by the content server the authentication and to provide an authentication method.

[0005]

[0005] According to a first aspect of the present invention defines an initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, user ID, and an initial and the authentication server for managing the authentication code in association with the authentication key to perform a two-way one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said portable terminal, said carries out bidirectional one-time ID authentication by using the authentication key between the authentication server via the gateway server, if the authentication is successful a bidirectional one-time ID authentication system, wherein the request content to the content server via the gateway server to.

[0006]

[0006] The invention described in claim 2 of the present invention, a bidirectional one-time ID authentication system according to claim 1 , wherein the authentication server, one-time ID authentication of the mobile terminal is successful in the authentication server the generates a session ID associated with the authentication key sent to the mobile terminal via the gateway server in the case, the session ID sent via the gateway server together with the content request from said portable terminal when confirming reads the URL and the user ID of the content server sends the gateway server, the gateway server sends the content request to the URL and the user ID and synthesized and the content server of the content server, the content sending of content of a server to the portable terminal via the gateway server, it said mobile devices, characterized by acquiring and displaying the content.

[0007]

[0007] The invention described in claim 3 of the present invention, a bidirectional one-time ID authentication system according to claim 1 or 2, to perform the bidirectional one-time ID authentication by using the authentication key, the authentication via the gateway server if the server one-time ID has been successfully authenticated by requesting the content to the content server, to acquire the content, that you previously installed a browser-type application program to perform the series of processes the features.

[0008]

[0008] The invention described in claim 4 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 3, wherein the application program and the authentication key is installed said portable terminal and activating the application program, carries out bidirectional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the via the gateway server when authentication is successful acquired by requesting the content to the content server, and performing automatically the operation of displaying on said portable terminal.

[0009]

[0009] The invention described in claim 5 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 4, wherein the session ID has a session time, the authentication server the session and features that you disable the session ID when the time has passed.

[001 0]

[001 0] The invention described in claim 6 of the present invention, a bidirectional one-time ID authentication system according to claim 5, when the session time is the session ID was disabled too, automatically and performing re-authentication by the bi-directional one-time ID authentication.

[001 1]

[001 1] The invention described in claim 7 of the present invention defines an initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, user ID, and an initial and the authentication server for managing the authentication code in association with the authentication key to perform a two-way one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said

portable terminal performs bi-directional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the authentication server, authentication generates the session ID and the token associated with the authentication key on success sends the token to the mobile terminal via the gateway server, differs from the mobile terminal to the token from the mobile terminal type in the terminal, the authentication server,Reads the URL and the user ID of the content server when confirming that the session time of the session ID associated with the token which is sent along with the content request via the gateway server from said different terminal is not passed said along with the session ID is sent to the gateway server, the gateway server sends to the content server and combined with the URL and the user ID of the content server the content request, the content of the content server via the gateway server on sent to different terminals and the mobile terminal together with the session ID, the registered in the Cookie the session ID as well as retrieve and display the content in the different terminals and the mobile terminal, since it was registered in the Cookie a bidirectional one-time ID authentication system characterized in that requesting content using the session ID.

[001 2]

[001 2] The invention described in claim 8 of the present invention, a bidirectional one-time ID authentication system according to claim 7, to perform the bidirectional one-time ID authentication by using the authentication key, bidirectional one-time to acquire the token when the ID authentication is successful, characterized in that to have been installed on the token-type application program to perform the series of processes.

[001 3]

[001 3] The invention described in claim 9 of the present invention, a bidirectional one-time ID authentication system according to claim 7 or 8, wherein the session ID has a session time, the authentication server only said session time disable the session ID when the said case of the session ID in the authentication server is disabled, characterized in that said from the portable terminal activates the application program acquires the token.

[001 4]

The invention according to claim 1 0 of the [001 4] present invention, a bidirectional one-time ID

authentication system according to any one of claims 1 to 9, wherein the authentication key, to activate the application program, said portable terminal the case where the initial authentication code and the required received in by inputting the download destination address of the authentication key, characterized in that it is installed.

[001 5]

[001 5] The invention described in Claim 1 1 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 9, wherein the authentication key, the download destination of the authentication key have been described characterized in that it is installed by clicking on the download destination e-mail to receive the mobile terminal.

[001 6]

[001 6] The invention described in Claim 1 2 of the present invention, characterized by a bidirectional one-time ID authentication system according to any one of claims 1 to 1 1 , for use as a model that can identify the user in the authentication server to.

[001 7]

[001 7] The invention described in Claim 1 3 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 1 1 , for use as a model that can guarantee the anonymity of the user at the authentication server it features a.

[001 8]

[001 8] The invention described in Claim 1 4 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 1 3, can disable the authentication key if you lose the portable terminal characterized in that it comprises a device separate.

[001 9]

[001 9] The invention described in Claim 1 5 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 1 4, wherein the content server and the gateway server is connected via the Internet If you are, and performing a bidirectional one-time ID authentication between the two servers.

[0020]

[0020] The invention described in Claim 1 6 of the present invention is to define a user ID, the user's address, phone number, and E-mail address, date of birth, bank account number or credit card number used for payment or the like both the content server for managing personal information, and defines the initial authentication code according to the registration of the user ID defined in the URL and the content server of the content servers, URL of the content server, user ID, and the initial authentication code and the authentication server to manage in association with the authentication key for the direction one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said portable terminal performs bi-directional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the gateway server when authentication is successful a content providing system characterized in that requests the content to the content server via.

[0021]

[0021] The invention described in Claim 1 7 of the present invention is to define a user ID, the user's address, phone number, and E-mail address, date of birth, bank account number or credit card number used for payment or the like both the content server for managing personal information, and defines the initial authentication code according to the registration of the user ID defined in the URL and the content server of the content servers, URL of the content server, user ID, and the initial authentication code and the authentication server to manage in association with the authentication key for the direction one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said portable terminal performs bi-directional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the authentication server, authentication was successful the generates a session ID and a token associated with the authentication key sends the token to the mobile terminal via the gateway

server in the case, the token from the mobile terminal type in different terminals and the mobile terminal ,The authentication server reads the URL and the user ID of the content server when confirming that the session time of the session ID associated with the token which is sent along with the content request via the gateway server is not only the feed along with the session ID to the gateway server, the gateway server sends to the content server and combined with the URL and the user ID of the content server the content request, the content of the content server via the gateway server said along with the session ID sent to a different terminal and the mobile terminal, the registered in the Cookie the session ID as well as retrieve and display the content in the different terminals and the mobile terminal, since it was registered in the Cookie session a content providing system characterized in that to request the content using the ID.

[0022]

[0022] The invention described in Claim 1 8 of the present invention, in the authentication server, and defines the initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, the user ID, and a step of initial management of the authentication code in association with the authentication key to perform a two-way one-time ID authentication, a step of the mobile terminal to install the authentication key from the authentication server, the portable terminal is the gateway server when the step of performing bidirectional one-time ID authentication, where the one-time ID authentication of the authentication server in the mobile terminal is successful by using the authentication key between the authentication server via said portable terminal the gateway a bidirectional one-time ID authentication method characterized by a step of requesting the content to the content server via the server.

[0023]

[0023] The invention described in Claim 1 9 of the present invention, the authentication if a bidirectional one-time ID authentication method according to claim 1 8, in the authentication server, the one-time ID authentication of the mobile terminal is successful generating a session ID associated with the key, the step of sending to said mobile terminal to the session ID via said gateway server, sent through the gateway server together with the content request from said portable terminal a step of reading the URL and the user ID of the content server when confirming the session ID, a step of sending to the content server the content request at the gateway server synthesizes the URL and the user ID of the content server, a step of sending to said mobile terminal a content of the content server via the gateway server, said portable terminal; and a step of acquiring and displaying the content.

[0024]

[0024] The invention described in Claim 20 of the present invention, in the authentication server, and defines the initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, the user ID, and a step of initial management of the authentication code in association with the authentication key to perform a two-way one-time ID authentication, a step of the mobile terminal to install the authentication key from the authentication server, the portable terminal is the gateway server associated with the authentication key if the the step of performing a bidirectional one-time ID authentication using the authentication key, the one-time ID authentication of the mobile terminal in the authentication server is successful between the authentication server via having the steps of generating a session ID and token, the step of sending the token to the mobile terminal via the gateway server, and a step of inputting said token in said mobile terminal different from the terminal and the mobile terminal was two-way one-time ID authentication method according to claim.

[0025]

[0025] The invention described in Claim 21 of the present invention, a bidirectional one-time ID authentication method according to claim 20, via the gateway server from a different terminal from said mobile terminal said token is input a step together with the content request and sends the token, the reading of the URL and the user ID of the content server when confirming that the session time of the session ID associated with the sent come token is not passed session through a step of sending to the gateway server along with ID, a step of sending to the content server the gateway server synthesizes the URL and the user ID of the content server of the content request, the gateway server for the content on the content server and a step to send to different terminals and the mobile terminal together with the session ID on, said the mobile terminal and the step of registering to Cookie the session ID as well as retrieve and display the content in a different terminal, after that, the characterized by a step of requesting the content using the session ID registered in the cookie.

[0026]

According to [0026] the present invention, it is possible to automatically perform authentication

without entering a user ID and password, not the user ID and password, and the like are known to a third party, the user content server There can be used with confidence to e-commerce and service of financial transactions, etc. to provide.

[0027]

[0027] Further, according to the present invention, authentication and access to the content server when starting the application program downloaded to the portable terminal is automatically performed.

[0028]

[0028] Further, according to the present invention, since no authentication by the content server, the content server need only provide information, it is possible to save time and cost of the authentication system construction.

[0029]

[0029] Hereinafter will be described the best mode for carrying out the present invention, but the present invention is not limited to the scope of the following examples, as long as without departing from the scope thereof, appropriately changed and those that can be implemented. First, the one-time ID and a two-way one-time ID authentication, as well as the application program and the authentication key will be explained.

[0030]

[0030] The one-time ID and a two-way one-time ID authentication will be described. One-time ID is identification information that can be used only once in the authentication, is generated based on the common key and the authentication data between devices or between applications. Authentication by an one-time ID, is to ensure the effect of anonymity that a third party while to become able to identify the sender, recipient, can grasp the one-time ID as identification information if a legitimate sender, recipient together with the resulting, for the one-time ID is changed each time the communication between sender and receiver is carried out, the effect is

obtained that a third party can not be predicted for the next one-time ID. The bidirectional one-time ID authentication, in order to authenticate with each other using the one-time ID, it is possible to prevent the spoofing each other.

[0031]

[0031] In the P-SIGMA is the key exchange and authentication method using the one-time ID for example, the key exchange and authentication in the procedure as shown in FIG. 1 have been made. First of all, the client is, proposal of SA (Security Association), to send a random number Rc, DH (Diffie-Hellman) public value gx, OID (the one-time ID) to the server. Note that the proposal of the SA, contains proposals on parameters used encryption algorithm and authentication method, the key exchange.

[0032]

[0032] Next, the server, to identify the client from the received OID, in the case that can not be identified, deny the communication. If it can be identified, send acceptance was SA, random number Rs, DH public value gy, HASHs, IDs that were encrypted with the session key e (the server ID) to the client. It should be noted that the session key e is a pre-shared key, a random number Rs, the function value of a keyed hash function to the random number Rc and DH common key gxy the argument, HASHs is, pre-shared key, a random number Rs, random number Rc, DH public value gx, which is a function value of the pseudo-random number function which takes a gy and IDs.

[0033]

[0033] Next, the client, to verify the HASHs received, to confirm the validity of the server on the basis of this HASHs. If it is correct HASHs, HASHc, send IDc encrypted with the session key e the (client ID) to the server. Here, HASHc is a pre-shared key, a random number Rs, random number Rc, DH public value gx, function value of the pseudo-random number function which takes a gy and IDc. Subsequently, the server to verify the HASHc received, to confirm the validity of the client on the basis of this HASHc. If it is correct HASHc, it terminates the protocol.

[0034]

[0034] In the P-SIGMA, OID (onetime ID) is defined as follows.

[0035]

[0035] OID1 = prf (K, 1) OID2 = prf (K, 2) ... OIDn = prf (K, n)

[0036]

[0036] In this defining expression, OIDn the one-time ID to be used when the n-th SA establishment, prf pseudo random function, K is a pre-shared key or a value generated from the pre-shared key.

[0037]

[0037] Therefore, according to the P-SIGMA, by introducing an OID, while the third party can not be identified the sender-recipient identifying OID if legitimate sender-recipient together effect is obtained such can be grasped as the information, every time the communication between the client and the server is performed (i.e., generation or each update of the SA) for OID to be changed, by a third party to predict the next OID effect can be obtained, such as can not.

[0038]

[0038] some of which was used as the variable shared key arguments that vary from session to this other or variable shared key and the one-time ID the function value of the hash function to a communication order as the argument, (SIGNAL) (Fig. 2, see Fig. 3). Thus, for example, it is variable shared key leaks to a third party, since the variable shared key is to be changed for each session, leaking variable shared key one-time non onetime ID generated using not be able to predict the ID. In other words, wiretapping is possible to generate a superior one-time ID to the difficult and safety. Further, by using the one-time ID (SIGNAL), since to carry out the authentication between the client and the server, while the third party can not be identified the sender-recipient, legitimate senders, recipients it is possible to grasp the one-time ID as

identification information, if any. Therefore, DoS attacks and spoofing resistance can be enhanced with respect to such, even under open network environment, aims to protect the ID information, it is possible to improve the security of communication. Further, it allows remote access, it is also possible to enhance the convenience.

[0039]

[0039] followed by the application program will be described. Bidirectional one-time ID authentication system of the present invention can be utilized by installing the application program to the mobile terminal. Then, by activating an application program installed, automatically carries out bidirectional one-time ID authentication with the authentication server, information can be obtained from the content server. This section describes how to install the application program, a description of the specific operation will be described later.

[0040]

To install the [0040] application program, there is the following method. However, not the method of installation is not limited to this. (1) you will receive an e-mail the download destination has been described of the mobile terminal to the authentication application software, by clicking on the download destination, to download and install the application program from the download site. (2) is notified of the download site of the application program in the mail or the like, the user has to enter the download site, download and install the application program from the download site. (3) software application program is sent by mail, etc., to install using it.

[0041]

[0041] The authentication key is a shared key used in performing the bidirectional one-time ID authentication generates a one-time ID. When performing bidirectional one-time ID authentication can be utilized by installing the pre-authentication key. How to install the authentication key will be explained. The user's address in the content server, phone number, E-mail address, date of birth, and the user information such as user ID is registered, by the operation or the like of an operator in the authentication server, defined in the URL of the content server and the content server It has been registered user ID, and this in accordance to register to define the initial authentication code associated with the authentication key in the corresponding table. When the download site or software application programs by mail or the

like is sent, the initial authentication code is also enclosed. It should be noted that, if necessary, have also been enclosed download destination site address of the authentication key. When to start the installed application program, if the initial authentication code and the necessary will be prompted to request the input of the download destination site address of the authentication key, and the client to enter the site address of the initial authentication code and download destination , the initial authentication code to request the download of the authentication key is sent to the authentication server through a gateway server. On the other hand, if the e-mail download destination application program is sent, the download location and the initial authentication code of the authentication key is described. User by entering the download destination and the initial authentication code of the authentication key, the initial authentication code to request the download of the authentication key is sent to the authentication server through a gateway server. It is to be noted that, by the download destination of the authentication key is to click on it, the initial authentication code also may have been to be sent together, the user by entering or click on the download destination of the authentication key, automatically initial authentication code may request a download of the authentication key is sent to the authentication server via the gateway server.

[0042]

[0042] Then, the authentication application program was started entering the download destination site address of the initial authentication code and authentication key, or by clicking the authentication key download destination, authentication server, which has received the initial authentication code, corresponding to the initial authentication code the authentication key is attached read from the correspondence table, and sends the authentication key to the user of the portable terminal that had download request via the gateway server. Authentication key on a mobile device is installed. Although there is no intended for authentication key is variable, in the present system can also be used with any authentication key.

[0043]

[0043] The above authentication application program and the authentication key by be installed in the portable terminal, when activating an application program on the mobile terminal, automatically an authentication key with the authentication server via the gateway server using carries out bidirectional one-time ID authentication can be acquired by requesting the content to the content server via a gateway server when authentication is successful.

[0044]

[0044] The following describes the first embodiment of the present invention with reference to the drawings. In this embodiment, described browser type bidirectional one-time ID authentication system. As shown in FIGS. 4 to 7, browser type bidirectional one-time ID authentication system includes a portable terminal, comprising an authentication server and a gateway server, mobile device, among via the gateway server and the authentication server carries out bidirectional one-time ID authentication using the authentication key to obtain the session ID if the authentication is successful, is a system for requesting the content to the content server via the gateway server.

[0045]

[0045] Here, the session ID will be explained. Session ID, assigned a unique value in the authentication server, an identifier associated with the authentication key. If the bidirectional one-time ID authentication in the authentication server is successful, thereafter, it adds the session ID when the access request from the mobile terminal to the content server, to authenticate the access to the content server to the authentication server by the session ID We have to get so. The user need not be aware of the addition of session ID, the application is programmed to automatically adds the session ID.

[0046]

[0046] That is, in the present system, performing the gateway server and an authentication server for authenticating the user, are separated and a content server that provides the service content, the portable terminal and the content server to communicate directly and authentication not.

[0047]

[0047] Each of the components will be described below. As described above, the mobile terminal be installed an authentication key and the application program. Here, it is assumed that installing a browser type application program. The mobile terminal is a terminal to access only to the gateway server. In the mobile terminal, it is a mobile phone or PDA (Personal Digital (Data)

Assistants) and the like. Authentication server, the operation or the like of the operator, and registers the URL and the user ID defined by the content server of the content server and the server to be registered in the correspondence table in association with this in accordance defines the initial authentication code authentication key . Also, generating an authentication server performs the two-way one-time ID authentication using the authentication key between the mobile terminal via the gateway server, the session ID if the one-time ID authentication of the mobile terminal is successful in the authentication server to.

[0048]

[0048] Session ID generated in the authentication server is managed by the correspondence table in association with the authentication key. That is, the session ID is therefore associated with the authentication key can be associated also with the content server URL and the user ID associated with the authentication key. Also, the session ID generated is sent together with the one-time ID to the mobile terminal via the gateway server. The authentication server may When confirming the session ID sent via the gateway server from the mobile terminal, reading the content server URL and the user ID associated with the session ID. Gateway server, the communication between the mobile terminal and the authentication server, which controls the communication between the content server and the mobile terminal, in the present system, a mobile terminal, the authentication server, and content server, always via a gateway server to communicate on. Content server is a server that provides services such as e-commerce and financial transactions. The content server, the user ID of the user to use the server is defined, address and phone number, E-mail address, date of birth, personal information such as bank account number or credit card number to be used in the settlement is registered It is managed. This system, by activating a browser-type application program on the mobile device, automatically authentication is performed, it is possible to acquire the contents on the content server.

[0049]

[0049] Hereinafter, with reference to FIGS. 1 0 to 1 3, the operation of the program when starting the installed browser application program of the mobile terminal. When you start the application program on the mobile terminal, it is determined whether or not the beginning to have obtained the authentication key. If the authentication key is not, because you must install the authentication key, authentication key download operation moved to the (preparatory stage), if necessary and the initial authentication code as described above is input the download destination address of the authentication key or click the authentication key download

destination, be installed on the mobile terminal (see Figure 1 0). If the authentication key is acquired proceeds to operation of generating the one-time ID using the authentication key (step 1).

[0050]

[0050] Hereinafter, the operation of step 1 will be described with reference to FIG. When you generate a one-time ID using the authentication key, the mobile terminal sends a one-time ID for mobile terminal authentication to the gateway server, gateway server sends the one-time ID to the authentication server. An authentication server using the authentication key is managed by the correspondence table, authenticates the one-time ID sent from the mobile terminal, generates a session ID if the authentication is successful. Then, the session ID generated is managed by the correspondence table in association with the authentication key in the authentication server. On the other hand, when the mobile terminal authentication is performed by the authentication server, one-time ID for another authentication server authentication with the one-time ID is generated by the authentication server. The authentication server sends the generated one-time ID to the gateway server along with the session ID. In addition, the session ID has a session time, the authentication server and measure the that time and at the same time to generate a session ID. Then, when the session time has passed, it is programmed to disable the session ID. When the gateway server receives the one-time ID and session ID from the authentication server, send them to the mobile terminal. The mobile terminal performs authentication of the authentication server in the one-time ID sent from the authentication server via the gateway server, to acquire the session ID if the authentication is successful. When you get the session ID on a mobile terminal moves to the operation for requesting the content to the content server (step 2).

[0051]

[0051] Hereinafter, the operation in step 2 will be described with reference to FIG. And to get the session ID on a mobile terminal on a mobile terminal to generate an HTTP packet to request the content. The mobile terminal is sent to the gateway server with the session ID of the HTTP packet, the gateway server while sending a session ID to the authentication server, once to hold the HTTP packet. Get the session ID sent from the gateway server in the authentication server, to determine whether the session ID is managed by the correspondence table, the correspondence to the session ID if there is a session ID in the correspondence table is reading the content server URL and user ID are. That is, if it is possible to read the session ID in the session time, it is possible to read the content server URL and the user ID, to be able to read the session ID in the session time, there is no session ID corresponding to the correspondence table so, it is impossible

to read the content server URL and the user ID. If the session ID corresponding to the correspondence table is not present, the authentication server notifies the effect that it is impossible to obtain the content (NG) to the gateway server, the gateway server also notifies the mobile terminal. A mobile terminal which is notified to that effect, as shown in FIG. 1 3, and proceeds to automatically re-operation of generating the one-time ID using the authentication key (step 1). On the other hand, if there is a session ID corresponding to the correspondence table, the authentication server reads the content server URL and the user ID, and sends them to the gateway server. In addition, at that time, to reset the session had been measured in the authentication server time, measure the re-session time. Thus, when transmitted again through the gateway server with the same session ID from the portable terminal, if it is possible to read the session ID in the session time, it is possible to read the content server URL and the user ID.

[0052]

[0052] Gateway server that has received the contents server URL and the user ID is combined with HTTP packet requesting content that is temporarily held, and sends it to the content server. Content server acquires the user ID, performs authentication of a user from among a plurality of users that are managed by the content server by using this, the content subjected to electronic transactions such as electronic commerce and financial transaction based on the HTTP packet it can be obtained. The content server sends the acquired content to the gateway server, the gateway server sends it to the portable terminal. Content acquired by the mobile terminal can be displayed using the browser on your mobile device.

[0053]

[0053] in the browser type bidirectional one-time ID authentication system of the present embodiment, only to start the installed application program on the mobile device, without having to enter a user ID and password, and the like automatically users it is possible to perform authentication. Accordingly, since no personal information of the user ID and password, etc. to a third party it is known, the user can use it at ease services such as e-commerce and financial transaction provided by the content server.

[0054]

[0054] In addition, to have a session time in the session ID to receive when the two-way one-time

ID authentication has been, during the session time of the session ID is valid, again, may not be a two-way one-time ID authentication so, it is possible to reduce the communication time and the packet between the mobile terminal and the server.

[0055]

[0055] Hereinafter, a description will be given of a second embodiment of the present invention with reference to the drawings. In this embodiment, described token type bidirectional one-time ID authentication system. As shown in FIGS. 8 and 9, the token type bidirectional one-time ID authentication system includes a portable terminal, a personal computer, an authentication server, a gateway server, a mobile terminal, the authentication server via a gateway server It carries out bidirectional one-time ID authentication using the authentication key between, certified is associated with the session ID on success token, the token manual input, infrared communication, serial cable, the IC card , a memory card, using Bluetooth, and a means such as a USB cable type to the personal computer, is a system for requesting the content to the content server via the gateway server from the personal computer by using the token.

[0056]

[0056] Here, the token will be explained. Token is generated when the bidirectional one-time ID authentication is successful, it assigns a unique value in the authentication server, an identifier associated with the authentication key and the session ID. Tokens in the case of a content request from a terminal other than the portable terminal, an identifier necessary for associating the session ID generated in the authentication server. It should be noted that, if you want to manually enter the token to the terminal other than the mobile terminal uses a string that can be recognized by the user.

[0057]

[0057] That is, in this system, obtains the token by performing bidirectional one-time ID authentication between the portable terminal and the authentication server via the gateway server, a terminal, such as a different PC from the the token portable terminal Fill in a system that requires the content to the content server from the terminal such as a personal computer via a gateway server. Incidentally, the gateway server and an authentication server which authenticates a user in the system, which separates the content server that provides the service

content, the portable terminal or terminal such as a personal computer and the content server to communicate directly and authentication do not go.

[0058]

[0058] Each of the components will be described below. As described above, the mobile terminal be installed an authentication key and the application program. Here, it is assumed that installing the token type application program. The mobile terminal is a terminal to access only to the gateway server. In the mobile terminal, it is a mobile phone or PDA (Personal Digital (Data) Assistants) and the like. Authentication server, the operation or the like of the operator, and registers the URL and the user ID defined by the content server of the content server and the server to be registered in the correspondence table in association with this in accordance defines the initial authentication code authentication key . The authentication server performs the two-way one-time ID authentication using the authentication key between the mobile terminal via the gateway server, the session ID and token when the one-time ID authentication of the mobile terminal is successful in the authentication server to generate. Session ID and token generated in the authentication server is managed by the correspondence table in association with the authentication key. That is, the session ID and token are therefore associated with the authentication key can be associated also with the content server URL and the user ID associated with the authentication key. The generated token is sent with the authentication onetime ID of the authentication server to the mobile terminal via the gateway server. The token is inputted from the portable terminal to a terminal such as a personal computer, the authentication server, the session ID when confirming the token transmitted from the terminal such as a personal computer via a gateway server, associated with the token, the content it can be read server URL and the user ID. The gateway server, the communication between the mobile terminal and the authentication server, which controls the communication between the content server and the portable terminal, in this system, a portable device or computer, the authentication server, and content server, always gateway server communicate over. Content server is a server that provides services such as e-commerce and financial transactions. The content server, the user ID of the user to use the server is defined, address and phone number, E-mail address, date of birth, personal information such as bank account number or credit card number to be used in the settlement is registered It is managed. This system, by activating a token type application program on the mobile terminal, by obtains the token, and inputs the token to the computer, automatically authentication is performed, to obtain the contents on the content server can.

[0059]

[0059] In the following, with reference to FIGS. 1 4 to 1 7, for explaining the operation of the program when you start the installation token type application program of the mobile terminal. First, as shown in FIG. 1 4, when the access from the personal computer to the gateway server, the gateway server input token is requested to the personal computer. If the token be entered in the computer I do not know, to start the installed token type application program of the mobile terminal, move the operation to get the token (step 1). On the other hand, if the token to enter know, the process proceeds to an operation to request the content by entering the token on a personal computer to the content server (step 2).

[0060]

[0060] When you start the application program on the mobile terminal, it is determined whether or not the beginning to have obtained the authentication key. If the authentication key is not, because you must install the authentication key, authentication key download operation moved to the (preparatory stage), the initial authentication code and if necessary input or authentication key download download destination address of the authentication key click on the above, it is installed on the mobile terminal (see Figure 1 0). If the authentication key is acquired proceeds to operation of generating the one-time ID using the authentication key (see Figure 1 4).

[0061]

[0061] Hereinafter, the operation of step 1 will be described with reference to FIG 1 4. When you generate a one-time ID using the authentication key, the mobile terminal sends a one-time ID to the gateway server, gateway server sends the one-time ID to the authentication server. An authentication server using the authentication key is managed by the correspondence table, it authenticates the one-time ID sent from the mobile terminal, generates a session ID and token when the authentication is successful. Then, the session ID and token generated is managed by the correspondence table in association with the authentication key in the authentication server. On the other hand, when the mobile terminal authentication is performed by the authentication server, one-time ID for another authentication server authentication with the one-time ID is generated by the authentication server. The authentication server sends the generated one-time ID together with the gateway server token. In addition, the session ID has a session time, the authentication server and measure the that time and at the same time to generate a session ID. Then, when the session time has passed, it is programmed to disable the session ID. When the gateway server receives the one-time ID and the token from the authentication server, send them

to the mobile terminal. The mobile terminal performs authentication of the authentication server in the one-time ID sent from the authentication server via the gateway server obtains the token when the authentication is successful. By acquiring the token on a mobile terminal, and then proceeds to an operation that requires the content to the content server by entering the token on a personal computer (step 2)

[0062]

[0062] Hereinafter, the operation in step 2 will be described with reference to FIG. Enter the token on a PC, it is and is sent to the gateway server, the gateway server HTTP packet to request the content is sent as well. Gateway server while sending a token to the authentication server, once to hold the HTTP packet. Get the token authentication server sent from the gateway server, a session ID associated with the token, it is determined whether or not managed by the correspondence table, if there is a session ID in the correspondence table is read the content server URL and user ID is associated with the session ID. That is, if it is possible to read the session ID associated with the session time, it is possible to read the content server URL and the user ID, to be able to read the session ID in the session time, corresponding to the correspondence table because the session ID does not exist, it is impossible to read the content server URL and the user ID. If the session ID corresponding to the correspondence table is not present, the authentication server notifies the effect that it is impossible to obtain the content (NG) to the gateway server, the gateway server also notifies the PC. User who has been notified to that effect, as shown in FIG. 1 7, again manually, in order to obtain a token, to activate the token type application program on the portable terminal to acquire the token. On the other hand, if there is a session ID corresponding to the correspondence table, the authentication server reads the session ID, the content server URL and the user ID, and sends them to the gateway server. In addition, at that time, to reset the session had been measured in the authentication server time, measure the re-session time.

[0063]

[0063] Gateway server that has received the contents server URL and the user ID is combined with HTTP packet requesting content that is temporarily held, and sends it to the content server. Content server acquires the user ID, performs authentication of a user from among a plurality of users that are managed by the content server by using this, the content subjected to electronic transactions such as electronic commerce and financial transaction based on the HTTP packet it can be obtained. Content server sends the acquired content to the gateway server, gateway server and sends it to the personal computer. It displayed using a browser on your computer the

content that you have acquired a personal computer.

[0064]

[0064] In addition, the gateway server sends a session ID obtained by reading by using the token in the authentication server to the PC, the PC is registering the Cookie of the session ID on a personal computer. Thus, as shown in FIG. 1 6, and requests the content from the PC using the session ID registered in the Cookie from the next time. Then, the PC sends the session ID to the authentication server via the gateway server, the authentication server if it is possible to read the session ID, can be read out content server URL and the user ID, it is possible to acquire the content.

[0065]

[0065] In the bidirectional one-time ID authentication system token type of the present embodiment performs the two-way one-time ID authentication with the portable terminal as in the above description, by entering the token, has a Web browser whatever the terminal if the terminal can access the content server. That is, a dedicated application program to use the content server even if it is not installed.

[0066]

[0066] Incidentally, in the case where the above-described first and second embodiments the gateway server and the content server are connected over the Internet, because the user ID is prevented from flowing out, again gateway server and the content server by performing bidirectional one-time ID authentication between, it is possible to further ensure the anonymity of the user on the route. Although described as being separate the server that provides the server and the content to authenticate the user, it may be constructed content providing system together. In addition, in the present system, to provide a device to disable the authentication key that is managed by the authentication server in case you lose your mobile device. This is to prevent the event, being unauthorized use by a third party in case you happen to lose your phone.

[0067]

[0067] The system may be utilized with a model identifying the user in the content server to ensure the anonymity of the user on the path, the two models to ensure the anonymity of the user in the route and on the content server it can.

[0068]

[0068] Model for identifying the user in the content server to ensure the anonymity of the user on the route has been guaranteed anonymity is on the path, configured as a model by the authentication server can identify the user ID of the content server It is. The content server, because you have registered personal information necessary, it is possible to extract the personal information required from the user ID. The user need not transmit personal information. Examples of personal information, name, address, date of birth, bank account number that can be used in the settlement, such as credit card number, and the like. As the model, (see FIG. 19) Internet banking model (see FIG. 18) or virtual shop model, (see FIG. 20) racing Internet voting model, internet ticketing model (see FIG. 21), and the like.

[0069]

[0069] Internet banking model may utilize the services Internet banking system provides without entering a user ID, a password, such as account numbers from the mobile. In addition, virtual store model, it is possible to use a user ID, password, bank account number, the online shopping service that virtual store offers without having to input such as from a mobile credit card number. In addition, in the horse race of the Internet vote, to buy betting tickets and settled in the user's bank account at the direction of the user, automatically dividend after the end of the race will be credited to the bank account of the user. In the Internet ticketing When you purchase a ticket by the bank account number or credit card number, use point is added to the user. It is also possible to replace the usage point accumulated in the prize.

[0070]

[0070] On the other hand, a model that guarantees the anonymity of the user is in the path and on the content server, the content server, the personal information is not registered any, including the user ID. And, configured as a model that can be accessed while guaranteeing

anonymity to the content server. As the model, (see FIG. 22) electronic voting model, and the like electron questionnaire model (see Figure 23). Electronic voting model, the electronic voting server records only result found in the database, can not be known which users have voted. Once the user who vote will be set in the authentication server so that it can not be re-vote. Voting management agencies, voters to allow access to the electronic voting system while maintaining the anonymity, to distribute the application and the authentication key for the mobile terminal to the voters in a secure manner. In addition, the electronic questionnaire model, records filled out the questionnaire only to the database, who is filled out is not be known. Once the user who fill in the questionnaire will be set in the authentication server so that it can not be filled again. Questionnaire executing agency, survey respondents to allow access to the electronic questionnaire server while maintaining the anonymity, to distribute the application and the authentication key for the mobile terminal to the questionnaire respondents in a secure manner.

[0071] initial stage of the first and second embodiment example of a sequence diagram present invention for explaining a sequence diagram bidirectional one-time ID authentication for explaining a sequence diagram bidirectional one-time ID authentication to be described bidirectional one-time ID authentication for the in Fig present invention showing the process of obtaining the session ID in the first embodiment of FIG present invention showing the process of obtaining an authentication key in the first and second embodiments of FIGS present invention showing the 1 of obtaining content in the second embodiment of FIG present invention showing the process of obtaining a token in the second embodiment of FIG present invention showing a process of obtaining content in example process the first embodiment of FIG present invention showing the sequence of obtaining the session ID in the first embodiment of FIG present invention showing the sequence of obtaining the authentication key in the first embodiment of FIG present invention showing the It shows a sequence of obtaining a token in the second embodiment of automatically drawing the invention showing a sequence of performing re-authentication in the first embodiment of FIG present invention showing the sequence of obtaining content in It shows the session ID and the sequence of obtaining content by using the Cookie registration session ID in the second embodiment of FIG present invention showing the sequence of obtaining the contents of the second embodiment of FIG invention

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-339247
(P2005-339247A)
(43)公開日　平成17年12月8日(2005.12.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330B	5B085
H04L 9/32	G06F	15/00	330E	5J104
	H04L	9/00	673D	

審査請求 未請求　請求項の数 21　ＯＬ　（全 25 頁）

(21)出願番号　特願2004-157752 (P2004-157752)
(22)出願日　平成16年5月27日 (2004.5.27)

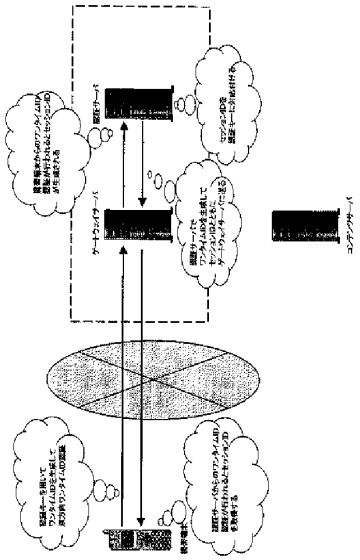
（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ
２．ＵＳＢ

(71)出願人　500196087
株式会社セキュアード・コミュニケーションズ
神奈川県川崎市中原区新丸子町９１５－１５
(74)代理人　100081514
弁理士　酒井　一
(74)代理人　100082692
弁理士　蔵合　正博
(72)発明者　大河　克好
東京都町田市三輪緑山１－３－２　緑山ヒルズ２１２

Ｆターム(参考)　5B085 AE02 AE09 AE23 AE29 BA06 BG07
5J104 AA07 KA01 KA04 KA21 NA05 NA38 PA07

(54)【発明の名称】双方向ワンタイムＩＤ認証システム及び認証方法

(57)【要約】
【課題】　ユーザＩＤやパスワードを入力しなくても自動的にユーザの認証を行い、かつ、その認証をコンテンツサーバで行わない双方向ワンタイムＩＤ認証システムを提供する。
【解決手段】　コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、認証サーバから認証キーをインストールして認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、携帯端末がアクセスするゲートウェイサーバとを備え、携帯端末は、ゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にゲートウェイサーバを介してコンテンツサーバへコンテンツを要求する双方向ワンタイムＩＤ認証システムである。
【選択図】　図６



【特許請求の範囲】
【請求項1】
コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、
前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システム。
【請求項2】
前記認証サーバは、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成して前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末では前記コンテンツを取得して表示することを特徴とする請求項１に記載の双方向ワンタイムＩＤ認証システム。
【請求項3】
前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、前記認証サーバのワンタイムＩＤ認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求させ、前記コンテンツを取得させる、一連の処理を行わせるブラウザ型のアプリケーションプログラムを前もってインストールしておくことを特徴とする請求項１または２に記載の双方向ワンタイムＩＤ認証システム。
【請求項4】
前記アプリケーションプログラム及び前記認証キーがインストールされた前記携帯端末は、前記アプリケーションプログラムを起動させると、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求して取得し、前記携帯端末上に表示する動作を自動で行うことを特徴とする請求項１乃至３の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項5】
前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にすることを特徴とする請求項１乃至４の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項6】
前記セッション時間が過ぎて前記セッションＩＤが無効になっていた場合、自動的に双方向ワンタイムＩＤ認証による再認証を行うことを特徴とする請求項５に記載の双方向ワンタイムＩＤ認証システム。
【請求項7】
コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、

前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、

前記携帯端末がアクセスするゲートウェイサーバとを備え、

前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークン

を送り、前記携帯端末から前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは、前記異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システム。

【請求項8】

前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、双方向ワンタイムＩＤ認証が成功した場合に前記トークンを取得させる、一連の処理を行わせるトークン型のアプリケーションプログラムを前もってインストールしておくことを特徴とする請求項７に記載の双方向ワンタイムＩＤ認証システム。

【請求項9】

前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にし、前記認証サーバにおいて前記セッションＩＤが無効になった場合、前記携帯端末から前記アプリケーションプログラムを起動させて前記トークンを取得することを特徴とする請求項７または８に記載の双方向ワンタイムＩＤ認証システム。

【請求項10】

前記認証キーは、前記アプリケーションプログラムを起動させ、前記携帯端末で受け取られる前記初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力することにより、インストールされることを特徴とする請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システム。

【請求項11】

前記認証キーは、当該認証キーのダウンロード先が記載された電子メールを前記携帯端末が受信して前記ダウンロード先をクリックすることによりインストールされることを特徴とする請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システム。

【請求項12】

前記認証サーバでユーザを特定できるモデルとして使用することを特徴とする請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システム。

【請求項13】

前記認証サーバでユーザの匿名性を保障できるモデルとして使用することを特徴とする請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システム。

【請求項14】

前記携帯端末を紛失した場合に前記認証キーを無効にできる装置を別に備えることを特徴とする請求項1乃至１３の何れかに記載の双方向ワンタイムＩＤ認証システム。

【請求項15】

前記ゲートウェイサーバと前記コンテンツサーバがインターネットを介して接続されている場合、両サーバ間で双方向ワンタイムＩＤ認証を行うことを特徴とする請求項1乃至

１４の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項16】
ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、
前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、
前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とするコンテンツ提供システム。
【請求項17】
ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、
前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、
前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送り、前記携帯端末は前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられたセッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とするコンテンツ提供システム。
【請求項18】
認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記携帯端末において前記認証サーバのワンタイムＩＤ認証が成功した場合に、前記携帯端末は前記ゲートウェイサーバを介してコンテンツサーバへコンテンツを要求する工程とを有することを特徴とする双方向ワン

タイムＩＤ認証方法。
【請求項19】
前記認証サーバにおいて、前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成する工程と、前記セッションＩＤを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出す工程と、前記ゲートウェイサーバにおいて前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末が前記コンテンツを取得して表示する工程とを有することを特徴とする請求項１８に記載の双方向ワンタイムＩＤ認証方法。
【請求項20】
認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成する工程と、前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送る工程と、前記携帯端末において前記トークンを当該携帯端末とは異なる端末に入力する工程とを有することを特徴とする双方向ワンタイムＩＤ認証方法。
【請求項21】
前記トークンが入力された前記携帯端末とは異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに前記トークンを送る工程と、前記送られてくるトークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送る工程と、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送る工程と、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録する工程と、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求する工程とを有することを特徴とする請求項２０に記載の双方向ワンタイムＩＤ認証方法。
【発明の詳細な説明】
【技術分野】
【0001】
本発明は、携帯端末とサーバとの間で双方向ワンタイムＩＤ認証を行う双方向ワンタイム認証システム及び認証方法に関する
【背景技術】
【0002】
インターネット経由で電子商取引や金銭取引等のサービスを提供するコンテンツサーバが広く知られている。図２４に示すように、ユーザは携帯端末やパソコン等を用いてコンテンツサーバとの間でインターネットを介して通信を行い、実際にそのサービスを利用する際には予め決定したユーザＩＤやパスワード等を入力して認証を行った上で、利用することができる。すなわち、コンテンツサーバは入力されたユーザＩＤやパスワード等を用いて、ユーザ情報との整合を取り、アクセスしてくるユーザを特定し、正当なユーザであれば要求を許可するようにしている。
【特許文献1】特開２００３－１６２５０７

【発明の開示】
【発明が解決しようとする課題】
【0003】
しかしながら、ユーザＩＤやパスワード等は第三者により推測、漏えい、あるいは盗み見られてしまうおそれがあり、そのようなことがあると、第三者でも簡単にコンテンツサーバが利用できてしまい、不正な商取引や金銭取引がされてしまうおそれがある。また、コンテンツサーバで管理されているユーザ情報には、ユーザＩＤやパスワード等の他に、例えば、ユーザの住所や電話番号、Ｅ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報等も管理されているので、第三者にユーザＩＤやパスワード等が知られてしまうと、同時にこれらの情報も知られてしまうおそれがある。そのため、ユーザはコンテンツサーバが提供する電子商取引や金銭取引等のサービスを安心して利用することができないという問題がある。
【0004】
こうした問題に着目し、本発明は、ユーザＩＤやパスワードを入力しなくても自動的にユーザの認証を行い、かつ、その認証をコンテンツサーバで行わない双方向ワンタイムＩＤ認証システム及び認証方法を提供することを目的とする。
【課題を解決するための手段】
【0005】
本発明の請求項１に記載の発明は、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システムである。
【0006】
本発明の請求項２に記載の発明は、請求項１に記載の双方向ワンタイムＩＤ認証システムについて、前記認証サーバは、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成して前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末では前記コンテンツを取得して表示することを特徴とする。
【0007】
本発明の請求項３に記載の発明は、請求項１または２に記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、前記認証サーバのワンタイムＩＤ認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求させ、前記コンテンツを取得させる、一連の処理を行わせるブラウザ型のアプリケーションプログラムを前もってインストールしておくことを特徴とする。
【0008】
本発明の請求項４に記載の発明は、請求項１乃至３の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記アプリケーションプログラム及び前記認証キーがインストールされた前記携帯端末は、前記アプリケーションプログラムを起動させると、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイ

ムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求して取得し、前記携帯端末上に表示する動作を自動で行うことを特徴とする。

【0009】

本発明の請求項５に記載の発明は、請求項１乃至４の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にすることを特徴とする。

【0010】

本発明の請求項６に記載の発明は、請求項５に記載の双方向ワンタイムＩＤ認証システムについて、前記セッション時間が過ぎて前記セッションＩＤが無効になっていた場合、自動的に双方向ワンタイムＩＤ認証による再認証を行うことを特徴とする。

【0011】

本発明の請求項７に記載の発明は、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送り、前記携帯端末から前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは、前記異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システムである。

【0012】

本発明の請求項８に記載の発明は、請求項７に記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、双方向ワンタイムＩＤ認証が成功した場合に前記トークンを取得させる、一連の処理を行わせるトークン型のアプリケーションプログラムを前もってインストールしておくことを特徴とする。

【0013】

本発明の請求項９に記載の発明は、請求項７または８に記載の双方向ワンタイムＩＤ認証システムについて、前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にし、前記認証サーバにおいて前記セッションＩＤが無効になった場合、前記携帯端末から前記アプリケーションプログラムを起動させて前記トークンを取得することを特徴とする。

【0014】

本発明の請求項１０に記載の発明は、請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーは、前記アプリケーションプログラムを起動させ、前記携帯端末で受け取られる前記初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力することにより、インストールされることを特徴とする。

【0015】

本発明の請求項１１に記載の発明は、請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーは、当該認証キーのダウンロード先が記載された電子メールを前記携帯端末が受信して前記ダウンロード先をクリックすることによりインストールされることを特徴とする。

【0016】

本発明の請求項１２に記載の発明は、請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証サーバでユーザを特定できるモデルとして使用することを特徴とする。

【0017】

本発明の請求項１３に記載の発明は、請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証サーバでユーザの匿名性を保障できるモデルとして使用することを特徴とする。

【0018】

本発明の請求項１４に記載の発明は、請求項1乃至１３の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記携帯端末を紛失した場合に前記認証キーを無効にできる装置を別に備えることを特徴とする。

【0019】

本発明の請求項１５に記載の発明は、請求項1乃至１４の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記ゲートウェイサーバと前記コンテンツサーバがインターネットを介して接続されている場合、両サーバ間で双方向ワンタイムＩＤ認証を行うことを特徴とする。

【0020】

本発明の請求項１６に記載の発明は、ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とするコンテンツ提供システムである。

【0021】

本発明の請求項１７に記載の発明は、ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送り、前記携帯端末から前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられたセッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテ

ンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とするコンテンツ提供システムである。

【0022】

本発明の請求項１８に記載の発明は、認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記携帯端末において前記認証サーバのワンタイムＩＤ認証が成功した場合に、前記携帯端末は前記ゲートウェイサーバを介してコンテンツサーバへコンテンツを要求する工程とを有することを特徴とする双方向ワンタイムＩＤ認証方法である。

【0023】

本発明の請求項１９に記載の発明は、請求項１８に記載の双方向ワンタイムＩＤ認証方法について、前記認証サーバにおいて、前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成する工程と、前記セッションＩＤを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出す工程と、前記ゲートウェイサーバにおいて前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末が前記コンテンツを取得して表示する工程とを有することを特徴とする。

【0024】

本発明の請求項２０に記載の発明は、認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成する工程と、前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送る工程と、前記携帯端末において前記トークンを当該携帯端末とは異なる端末に入力する工程とを有することを特徴とする双方向ワンタイムＩＤ認証方法。

【0025】

本発明の請求項２１に記載の発明は、請求項２０に記載の双方向ワンタイムＩＤ認証方法について、前記トークンが入力された前記携帯端末とは異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに前記トークンを送る工程と、前記送られてくるトークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送る工程と、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送る工程と、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤ

をＣｏｏｋｉｅに登録する工程と、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求する工程とを有することを特徴とする。

【発明の効果】

【0026】

本発明によれば、ユーザＩＤやパスワードを入力しなくても自動的に認証を行うことができるので、第三者にユーザＩＤやパスワード等が知られることはなく、ユーザはコンテンツサーバが提供する電子商取引や金銭取引等のサービスを安心して利用することができる。

【0027】

また、本発明によれば、携帯端末にダウンロードしたアプリケーションプログラムを起動するとコンテンツサーバへの認証とアクセスが自動的に行われる。

【0028】

また、本発明によれば、認証をコンテンツサーバで行わないので、コンテンツサーバは情報を提供するだけでよく、認証システム構築の手間やコストを省くことができる。

【発明を実施するための最良の形態】

【0029】

以下、本発明を実施するための最良の形態を説明するが、本発明は以下の実施例の範囲に限定されるものではなく、その要旨を逸脱しない範囲であれば、適宜に変更及び実施できるものである。はじめに、ワンタイムＩＤと双方向ワンタイムＩＤ認証、ならびにアプリケーションプログラムと認証キーについて説明する。

【0030】

ワンタイムＩＤと双方向ワンタイムＩＤ認証について説明する。ワンタイムＩＤは認証において一回限り使用可能な識別情報であり、装置間あるいはアプリケーション間で共通な鍵や認証データを基に生成される。ワンタイムＩＤによる認証では、第三者が送信者・受信者を特定できなる一方で、正当な送信者・受信者であればワンタイムＩＤを識別情報として把握できるという匿名性を保障する効果が得られるとともに、送信者と受信者間で通信が行われる度にワンタイムＩＤが変更されるために、第三者が次回のワンタイムＩＤを予測できることができないという効果が得られる。双方向ワンタイムＩＤ認証では、このワンタイムＩＤを使って相互に認証を行うために、お互いになりすましを防ぐことができる。

【0031】

例えばワンタイムIDを使った鍵交換・認証方式であるＰ－ＳＩＧＭＡにおいては、図１に示すような手順で鍵交換および認証が行われている。先ず、クライアントが、ＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）の提案、乱数Ｒｃ、ＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）公開値ｇｘ　、ＯＩＤ（ワンタイムＩＤ）をサーバに対して送信する。なお、ＳＡの提案には、暗号アルゴリズムや認証方式、鍵交換に使用するパラメータ等に関する提案が含まれている。

【0032】

次いで、サーバが、受け取ったＯＩＤからクライアントを識別し、識別できない場合には、通信を拒否する。識別できる場合には、受諾したＳＡ、乱数Ｒｓ、ＤＨ公開値ｇｙ　、ＨＡＳＨｓ、セッション鍵ｅで暗号化したＩＤｓ（サーバＩＤ）をクライアントに対して送信する。なお、セッション鍵ｅは、既知共有鍵、乱数Ｒｓ、乱数ＲｃおよびＤＨ共通鍵ｇｘｙを引数とする鍵付きハッシュ関数の関数値であり、ＨＡＳＨｓは、既知共有鍵、乱数Ｒｓ、乱数Ｒｃ、ＤＨ公開値ｇｘ　、ｇｙ　およびＩＤｓを引数とする疑似乱数関数の関数値である。

【0033】

次いで、クライアントが、受け取ったＨＡＳＨｓを検証し、このＨＡＳＨｓに基づいてサーバの正当性を確認する。ＨＡＳＨｓが正しければ、ＨＡＳＨｃ、セッション鍵ｅで暗号化したＩＤｃ（クライアントＩＤ）をサーバに対して送信する。ここで、ＨＡＳＨｃは、既知共有鍵、乱数Ｒｓ、乱数Ｒｃ、ＤＨ公開値ｇｘ　、ｇｙ　およびＩＤｃを引数とす

る疑似乱数関数の関数値である。次いで、サーバが、受け取ったＨＡＳＨｃを検証し、このＨＡＳＨｃに基づいてクライアントの正当性を確認する。ＨＡＳＨｃが正しければ、当該プロトコルを終了する。

【0034】

このＰ－ＳＩＧＭＡにおいて、ＯＩＤ（ワンタイムＩＤ）は、次のように定義されている。

【0035】

ＯＩＤ１　＝ｐｒｆ（Ｋ、１）
ＯＩＤ２　＝ｐｒｆ（Ｋ、２）
・・・
ＯＩＤｎ　＝ｐｒｆ（Ｋ、ｎ）

【0036】

この定義式において、ＯＩＤｎ　はｎ番目のＳＡ確立時に用いられるワンタイムＩＤ、ｐｒｆは疑似乱数関数、Ｋは既知共有鍵、若しくは既知共有鍵から生成された値である。

【0037】

このため、上記Ｐ－ＳＩＧＭＡによれば、ＯＩＤを導入したことにより、第三者が送信者・受信者を特定できなくなる一方で、正当な送信者・受信者であればＯＩＤを識別情報として把握できるといった効果が得られるとともに、クライアント・サーバ間で通信が行われる度（すなわち、ＳＡの生成または更新毎）にＯＩＤが変更されるため、第三者が次回のＯＩＤを予測することができないといった効果が得られる。

【0038】

この他にセッション毎に変化する可変共有鍵を引数、あるいは可変共有鍵と通信順序を引数とするハッシュ関数の関数値をワンタイムＩＤ（ＳＩＧＮＡＬ）として用いるようにしたものもある（図２、図３参照）。これにより、例えば、可変共有鍵が第三者に漏れたとしても、セッション毎に可変共有鍵が変化することとなるので、漏れた可変共有鍵を用いて生成されたワンタイムＩＤ以外のワンタイムＩＤを予測できなくなる。すなわち、盗聴が困難で安全性に優れたワンタイムＩＤを生成することが可能になる。また、上記ワンタイムＩＤ（ＳＩＧＮＡＬ）を用いて、クライアント・サーバ間における認証を行うようにしたので、第三者が送信者・受信者を特定できなくなる一方で、正当な送信者・受信者であればワンタイムＩＤを識別情報として把握することができる。したがって、ＤｏＳ攻撃やなりすまし等に対する耐性を強化することができ、オープンなネットワーク環境下においても、ＩＤ情報の保護を図り、通信の安全性を向上させることができる。また、リモートアクセスが可能になり、利便性の向上を図ることもできる。

【0039】

つづいてアプリケーションプログラムについて説明する。本発明の双方向ワンタイムＩＤ認証システムは、携帯端末にアプリケーションプログラムをインストールすることで利用することができる。そして、インストールされたアプリケーションプログラムを起動させることにより、自動的に認証サーバとの間で双方向ワンタイムＩＤ認証を行い、コンテンツサーバから情報を得ることができる。ここでは、アプリケーションプログラムのインストール方法について説明し、具体的な動作についての説明は後述する。

【0040】

アプリケーションプログラムをインストールするには、次のような方法がある。ただし、インストールの方法はこれに限定されるものではない。

（１）携帯端末に認証アプリケーションソフトのダウンロード先が記載された電子メールが届き、そのダウンロード先をクリックすることにより、ダウンロードサイトからアプリケーションプログラムをダウンロードしてインストールする。

（２）郵送等でアプリケーションプログラムのダウンロードサイトが通知され、ユーザがダウンロードサイトを入力して、ダウンロードサイトからアプリケーションプログラムをダウンロードしてインストールする。

（３）郵送等でアプリケーションプログラムのソフトが送られ、それを用いてインストー

ルする。

【0041】

認証キーは、ワンタイムＩＤを生成して双方向ワンタイムＩＤ認証を行う際に用いる共有鍵である。双方向ワンタイムＩＤ認証を行う際には、予め認証キーをインストールすることで利用することができる。認証キーのインストール方法について説明する。コンテンツサーバでユーザの住所、電話番号、Ｅ－ｍａｉｌアドレス、生年月日、及びユーザＩＤ等のユーザ情報が登録されると、認証サーバにおいてオペレータの操作等により、コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤを登録し、これに従い初期認証コードを定義して認証キーと対応付けて対応表に登録する。郵送等でアプリケーションプログラムのダウンロードサイトあるいはソフトが送られてくる場合には、初期認証コードも同封されている。なお、必要な場合は認証キーのダウンロード先のサイトアドレスも同封されている。インストールされたアプリケーションプログラムを起動させると、初期認証コードと必要な場合は認証キーのダウンロード先のサイトアドレスの入力を要求する画面が表示され、クライアントが初期認証コードやダウンロード先のサイトアドレスを入力すると、初期認証コードはゲートウェイサーバを介して認証サーバへ送られて認証キーのダウンロードを要求する。一方、電子メールでアプリケーションプログラムのダウンロード先が送られてくる場合には、認証キーのダウンロード先と初期認証コードが記載されている。ユーザは認証キーのダウンロード先と初期認証コードを入力することにより、初期認証コードがゲートウェイサーバを介して認証サーバへ送られて認証キーのダウンロードを要求する。なお、認証キーのダウンロード先はそれをクリックすることにより、初期認証コードも一緒に送られるようになっていても良く、ユーザは認証キーのダウンロード先を入力またはクリックすることにより、自動的に初期認証コードがゲートウェイサーバを介して認証サーバへ送られて認証キーのダウンロードを要求するようにしても良い。

【0042】

そして、認証アプリケーションプログラムを起動させて初期認証コードや認証キーのダウンロード先サイトアドレスを入力、あるいは認証キーダウンロード先をクリックすると、初期認証コードを受信した認証サーバは、初期認証コードに対応付けられている認証キーを対応表から読み出し、認証キーをゲートウェイサーバを介してダウンロード要求のあったユーザの携帯端末に送る。携帯端末では認証キーがインストールされる。なお、認証キーには可変であるものとないものがあるが、本システムでは何れの認証キーを用いても使用することができる。

【0043】

以上の認証アプリケーションプログラムと認証キーを携帯端末にインストールしておくことで、携帯端末上のアプリケーションプログラムを起動させると、自動的にゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にゲートウェイサーバを介してコンテンツサーバへコンテンツを要求して取得することができる。

【実施例】

【0044】

以下、図面を用いて本発明の第１実施例について説明する。本実施例ではブラウザ型の双方向ワンタイムＩＤ認証システムについて説明する。図４乃至７に示すように、ブラウザ型の双方向ワンタイムＩＤ認証システムは、携帯端末と、認証サーバと、ゲートウェイサーバとを備え、携帯端末は、ゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にセッションＩＤを取得し、ゲートウェイサーバを介してコンテンツサーバへコンテンツを要求するシステムである。

【0045】

ここでセッションＩＤについて説明する。セッションＩＤは、認証サーバの中でユニークな値を割り当て、認証キーと対応付けられた識別子である。認証サーバの中で双方向ワ

ンタイムID認証が成功した場合、それ以降、携帯端末からコンテンツサーバへのアクセス要求時にセッションＩＤを付加し、セッションＩＤによりコンテンツサーバへのアクセスを認証サーバに認証してもらうようにしている。なお、ユーザはセッションＩＤの付加について意識する必要はなく、アプリケーションが自動的にセッションＩＤ付加するようにプログラムされている。

【0046】

すなわち、本システムでは、ユーザの認証を行うゲートウェイサーバ及び認証サーバと、コンテンツのサービスを提供するコンテンツサーバとを分離しており、携帯端末はコンテンツサーバと直接的に通信や認証を行っていない。

【0047】

以下、各構成について説明する。上記したように、携帯端末にはアプリケーションプログラムと認証キーをインストールしておく。ここではブラウザ型のアプリケーションプログラムをインストールしているものとする。携帯端末はゲートウェイサーバのみにアクセスする端末である。携帯端末には携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ（Ｄａｔａ）　Ａｓｓｉｓｔａｎｔｓ）等がある。認証サーバは、オペレータの操作等により、コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤを登録し、これに従い初期認証コードを定義して認証キーと対応付けて対応表に登録するサーバである。また、認証サーバは、ゲートウェイサーバを介して携帯端末との間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証サーバにおいて携帯端末のワンタイムＩＤ認証が成功した場合にセッションＩＤを生成する。

【0048】

認証サーバにおいて生成されたセッションＩＤは、認証キーと対応付けられて対応表にて管理される。すなわち、セッションＩＤは認証キーと対応付けられているので、認証キーと対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤとも対応付けることができる。また、生成されたセッションＩＤはゲートウェイサーバを介して携帯端末にワンタイムＩＤとともに送られる。そして認証サーバは、携帯端末からゲートウェイサーバを介して送られてくるセッションＩＤを確認した場合に、セッションＩＤに対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができる。ゲートウェイサーバは、携帯端末と認証サーバの間の通信、コンテンツサーバと携帯端末の間の通信を制御するものであり、本システムにおいて、携帯端末、認証サーバ、及びコンテンツサーバは、必ずゲートウェイサーバを介して通信を行う。コンテンツサーバは電子商取引や金銭取引等のサービスを提供するサーバである。コンテンツサーバには、当該サーバを利用するユーザのユーザＩＤが定義され、住所や電話番号、Ｅ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報が登録されて管理されている。本システムは、携帯端末上のブラウザ型のアプリケーションプログラムを起動させることにより、自動的に認証が行われ、コンテンツサーバのコンテンツを取得することができる。

【0049】

以下、図１０乃至１３を用いて、携帯端末にインストールされたブラウザ型のアプリケーションプログラムを起動したときのプログラムの動作を説明する。携帯端末上のアプリケーションプログラムを起動すると、はじめに認証キーを取得しているか否かについて判別される。認証キーが無い場合には、認証キーをインストールしなければならないので、認証キーダウンロードの動作（準備段階）に移り、上記のように初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力あるいは認証キーダウンロード先をクリックして、携帯端末上にインストールする（図１０参照）。認証キーが取得されている場合には認証キーを用いてワンタイムＩＤを生成する動作に移る（ステップ１）。

【0050】

以下、図１１を用いてステップ１の動作を説明する。認証キーを用いてワンタイムＩＤを生成すると、携帯端末は携帯端末認証用のワンタイムＩＤをゲートウェイサーバに送り、ゲートウェイサーバはワンタイムＩＤを認証サーバに送る。認証サーバでは対応表にて

管理されている認証キーを用いて、携帯端末から送られてくるワンタイムＩＤの認証を行い、認証が成功した場合にセッションＩＤを生成する。そして、生成されたセッションＩＤは、認証サーバで認証キーと対応付けられて対応表にて管理される。その一方、認証サーバで携帯端末の認証が行われると、認証サーバでは上記ワンタイムＩＤとは別の認証サーバ認証用のワンタイムＩＤが生成される。認証サーバは、生成されたワンタイムＩＤをセッションＩＤとともにゲートウェイサーバに送る。また、セッションＩＤはセッション時間を持っており、認証サーバではセッションＩＤを生成すると同時にその時間を計っている。そして、セッション時間が過ぎた場合には、セッションＩＤを無効にするようにプログラムされている。ゲートウェイサーバは認証サーバからワンタイムＩＤとセッションＩＤを受信すると、それらを携帯端末に送る。携帯端末はゲートウェイサーバを介して認証サーバから送られてくるワンタイムＩＤで認証サーバの認証を行い、認証が成功した場合にセッションＩＤを取得する。携帯端末上でセッションＩＤを取得するとコンテンツサーバへコンテンツを要求する動作に移る（ステップ２）。

【0051】

以下、図１２を用いてステップ２の動作を説明する。携帯端末上でセッションＩＤを取得すると携帯端末上ではコンテンツを要求するＨＴＴＰパケットを生成する。携帯端末はＨＴＴＰパケットをセッションＩＤとともにゲートウェイサーバに送り、ゲートウェイサーバはセッションＩＤを認証サーバへ送る一方、ＨＴＴＰパケットを一旦保持する。認証サーバではゲートウェイサーバから送られてくるセッションＩＤを取得し、当該セッションＩＤが対応表にて管理されているか否かを判別し、対応表にセッションＩＤがある場合には当該セッションＩＤに対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤを読み出す。すなわち、セッション時間内にセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができ、セッション時間内にセッションＩＤを読み出すことができなければ、対応表に対応するセッションＩＤが存在しないので、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができない。対応表に対応するセッションＩＤが存在しない場合、認証サーバはコンテンツを取得することができない旨（ＮＧ）をゲートウェイサーバに通知し、ゲートウェイサーバもその旨を携帯端末に通知する。その旨を通知された携帯端末は、図１３に示すように、自動的に再度、認証キーを用いてワンタイムＩＤを生成する動作（ステップ１）に移る。一方、対応表に対応するセッションＩＤがある場合、認証サーバでは、コンテンツサーバＵＲＬ及びユーザＩＤを読み出し、これらをゲートウェイサーバに送る。また、その時、認証サーバで計っていたセッション時間をリセットし、再度セッション時間を計る。これにより、携帯端末から同じセッションＩＤを用いてゲートウェイサーバを介して再度送られてくる場合、セッション時間内にセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができる。

【0052】

コンテンツサーバＵＲＬ及びユーザＩＤを受信したゲートウェイサーバは、一旦保持されているコンテンツを要求するＨＴＴＰパケットと合成し、これをコンテンツサーバに送る。コンテンツサーバはユーザＩＤを取得し、これを用いてコンテンツサーバで管理されている複数のユーザの中からユーザの認証を行い、ＨＴＴＰパケットを元に電子商取引や金銭取引等の電子取引を行いコンテンツを取得することができる。コンテンツサーバは、取得したコンテンツをゲートウェイサーバに送り、ゲートウェイサーバはそれを携帯端末に送る。携帯端末で取得したコンテンツは携帯端末上のブラウザを用いて表示することができる。

【0053】

本実施例のブラウザ型の双方向ワンタイムＩＤ認証システムでは、携帯端末上にインストールされたアプリケーションプログラムを起動させるだけで、ユーザＩＤやパスワード等を入力しなくても自動的にユーザの認証を行うことができる。これにより、第三者にユーザＩＤやパスワード等の個人情報が知られることはないので、ユーザはコンテンツサーバが提供する電子商取引や金銭取引等のサービスを安心して利用することができる。

【0054】
また、双方向ワンタイムＩＤ認証がされた時に受け取るセッションＩＤにセッション時間を持たせ、そのセッションＩＤのセッション時間が有効な間は、再度、双方向ワンタイムＩＤ認証をしなくて良いので、携帯端末とサーバの間での通信時間やパケットを削減することができる。
【実施例】
【0055】
以下、図面を用いて本発明の第２実施例について説明する。本実施例ではトークン型の双方向ワンタイムＩＤ認証システムについて説明する。図８および図９に示すように、トークン型の双方向ワンタイムＩＤ認証システムは、携帯端末と、パソコンと、認証サーバと、ゲートウェイサーバとを備え、携帯端末は、ゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にセッションＩＤに対応付けられたトークンを取得し、そのトークンを手入力、赤外線通信、シリアルケーブル、ＩＣカード、メモリカード、Ｂｌｕｅｔｏｏｔｈ、及びＵＳＢケーブル等の手段を用いてパソコンに入力し、そのトークンを用いてパソコンからゲートウェイサーバを介してコンテンツサーバへコンテンツを要求するシステムである。
【0056】
ここでトークンについて説明する。トークンは、双方向ワンタイムＩＤ認証が成功した場合に生成され、認証サーバの中でユニークな値を割り当て、認証キーとセッションＩＤに対応付けられた識別子である。トークンは携帯端末以外の端末からコンテンツ要求を行う場合に、認証サーバにおいて生成されたセッションＩＤと対応付けるために必要な識別子である。なお、トークンを携帯端末以外の端末に手入力する場合はユーザが認識できる文字列を使用する。
【0057】
すなわち、本システムでは、ゲートウェイサーバを介して携帯端末と認証サーバとの間で双方向ワンタイムＩＤ認証を行うことによりトークンを取得し、そのトークンを携帯端末とは異なるパソコン等の端末に入力し、パソコン等の端末からゲートウェイサーバを介してコンテンツサーバへコンテンツを要求するシステムである。なお、本システムでもユーザの認証を行うゲートウェイサーバ及び認証サーバと、コンテンツのサービスを提供するコンテンツサーバとを分離しており、携帯端末やパソコン等の端末はコンテンツサーバと直接的に通信や認証を行っていない。
【0058】
以下、各構成について説明する。上記したように、携帯端末にはアプリケーションプログラムと認証キーをインストールしておく。ここではトークン型のアプリケーションプログラムをインストールしているものとする。携帯端末はゲートウェイサーバのみにアクセスする端末である。携帯端末には携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ（Ｄａｔａ）　Ａｓｓｉｓｔａｎｔｓ）等がある。認証サーバは、オペレータの操作等により、コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤを登録し、これに従い初期認証コードを定義して認証キーと対応付けて対応表に登録するサーバである。また、認証サーバは、ゲートウェイサーバを介して携帯端末との間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証サーバにおいて携帯端末のワンタイムＩＤ認証が成功した場合にセッションＩＤとトークンを生成する。認証サーバにおいて生成されたセッションＩＤとトークンは、認証キーと対応付けられて対応表にて管理される。すなわち、セッションＩＤとトークンは認証キーと対応付けられているので、認証キーと対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤとも対応付けることができる。また、生成されたトークンはゲートウェイサーバを介して携帯端末に認証サーバの認証用ワンタイムＩＤとともに送られる。そのトークンは携帯端末からパソコン等の端末に入力され、認証サーバは、パソコン等の端末からゲートウェイサーバを介して送られてくるトークンを確認した場合に、トークンに対応付けられているセッションＩＤ、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができる。ゲートウェイサーバは、携帯端末と認証

サーバの間の通信、コンテンツサーバと携帯端末の間の通信を制御するものであり、本システムにおいて、携帯端末やパソコン、認証サーバ、及びコンテンツサーバは、必ずゲートウェイサーバを介して通信を行う。コンテンツサーバは電子商取引や金銭取引等のサービスを提供するサーバである。コンテンツサーバには、当該サーバを利用するユーザのユーザＩＤが定義され、住所や電話番号、Ｅ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報が登録されて管理されている。本システムは、携帯端末上のトークン型のアプリケーションプログラムを起動させることにより、トークンを取得し、そのトークンをパソコンに入力することにより、自動的に認証が行われ、コンテンツサーバのコンテンツを取得することができる。

【0059】

以下、図１４乃至１７をもちいて、携帯端末にインストールされたトークン型のアプリケーションプログラムを起動したときのプログラムの動作を説明する。はじめに、図１４に示すように、パソコンからゲートウェイサーバにアクセスすると、ゲートウェイサーバはパソコンにトークンの入力が要求される。パソコンで入力するトークンがわからない場合は、携帯端末にインストールされたトークン型のアプリケーションプログラムを起動し、トークンを取得する動作に移る（ステップ１）。一方、入力するトークンがわかっている場合は、パソコン上でトークンを入力してコンテンツサーバへコンテンツを要求する動作に移る（ステップ２）。

【0060】

携帯端末上のアプリケーションプログラムを起動すると、はじめに認証キーを取得しているか否かについて判別される。認証キーが無い場合には、認証キーをインストールしなければならないので、認証キーダウンロードの動作（準備段階）に移り、初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力あるいは認証キーダウンロード先をクリックして、携帯端末上にインストールする（図１０参照）。認証キーが取得されている場合には認証キーを用いてワンタイムＩＤを生成する動作に移る（図１４参照）。

【0061】

以下、図１４を用いてステップ１の動作を説明する。認証キーを用いてワンタイムＩＤを生成すると、携帯端末はワンタイムＩＤをゲートウェイサーバに送り、ゲートウェイサーバはワンタイムＩＤを認証サーバに送る。認証サーバでは対応表にて管理されている認証キーを用いて、携帯端末から送られてくるワンタイムＩＤの認証を行い、認証が成功した場合にセッションＩＤとトークンを生成する。そして、生成されたセッションＩＤとトークンは、認証サーバで認証キーと対応付けられて対応表にて管理される。その一方、認証サーバで携帯端末の認証が行われると、認証サーバでは上記ワンタイムＩＤとは別の認証サーバ認証用のワンタイムＩＤが生成される。認証サーバは、生成されたワンタイムＩＤをトークンとともにゲートウェイサーバに送る。また、セッションＩＤはセッション時間を持っており、認証サーバではセッションＩＤを生成すると同時にその時間を計っている。そして、セッション時間が過ぎた場合には、セッションＩＤを無効にするようにプログラムされている。ゲートウェイサーバは認証サーバからワンタイムＩＤとトークンを受信すると、それらを携帯端末に送る。携帯端末はゲートウェイサーバを介して認証サーバから送られてくるワンタイムＩＤで認証サーバの認証を行い、認証が成功した場合にトークンを取得する。携帯端末上でトークンを取得することにより、パソコン上でトークンを入力してコンテンツサーバへコンテンツを要求する動作に移る（ステップ２）

【0062】

以下、図１５を用いてステップ２の動作を説明する。パソコン上でトークンを入力し、それがゲートウェイサーバに送られると、ゲートウェイサーバにはコンテンツを要求するＨＴＴＰパケットも同時に送られる。ゲートウェイサーバはトークンを認証サーバへ送る一方、ＨＴＴＰパケットを一旦保持する。認証サーバではゲートウェイサーバから送られてくるトークンを取得し、当該トークンに対応付けられているセッションＩＤが対応表にて管理されているか否かを判別し、対応表にセッションＩＤがある場合には当該セッションＩＤに対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤを読み出す。すなわ

ち、セッション時間内に対応付けられているセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができ、セッション時間内にセッションＩＤを読み出すことができなければ、対応表に対応するセッションＩＤが存在しないので、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができない。対応表に対応するセッションＩＤが存在しない場合、認証サーバはコンテンツを取得することができない旨（ＮＧ）をゲートウェイサーバに通知し、ゲートウェイサーバもその旨をパソコンに通知する。その旨を通知されたユーザは、図１７に示すように、マニュアルで再度、トークンを取得するため、携帯端末上のトークン型のアプリケーションプログラムを起動させてトークンを取得する。一方、対応表に対応するセッションＩＤがある場合、認証サーバでは、セッションＩＤ、コンテンツサーバＵＲＬ及びユーザＩＤを読み出し、これらをゲートウェイサーバに送る。また、その時、認証サーバで計っていたセッション時間をリセットし、再度セッション時間を計る。

【0063】

コンテンツサーバＵＲＬ及びユーザＩＤを受信したゲートウェイサーバは、一旦保持されているコンテンツを要求するＨＴＴＰパケットと合成し、これをコンテンツサーバに送る。コンテンツサーバはユーザＩＤを取得し、これを用いてコンテンツサーバで管理されている複数のユーザの中からユーザの認証を行い、ＨＴＴＰパケットを元に電子商取引や金銭取引等の電子取引を行いコンテンツを取得することができる。コンテンツサーバは、取得したコンテンツをゲートウェイサーバに送り、ゲートウェイサーバはそれをパソコンに送る。パソコンでは取得したコンテンツをパソコン上のブラウザを用いて表示する。

【0064】

また、ゲートウェイサーバは、認証サーバでトークンを用いて読み出して取得したセッションＩＤをパソコンに送り、パソコンはパソコン上でセッションＩＤのＣｏｏｋｉｅを登録しておく。これにより、図１６に示すように、次回からＣｏｏｋｉｅに登録されたセッションＩＤを用いてパソコンからコンテンツを要求する。そして、パソコンは、セッションＩＤをゲートウェイサーバを介して認証サーバに送り、認証サーバがセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができ、コンテンツを取得することができる。

【0065】

本実施例のトークン型の双方向ワンタイムＩＤ認証システムでは、上記の説明のように携帯端末で双方向ワンタイムＩＤ認証を行い、トークンを入力することにより、Ｗｅｂブラウザを持っている端末ならどのような端末であっても、コンテンツサーバにアクセスできる。すなわち、専用のアプリケーションプログラムがインストールされていなくてもコンテンツサーバを利用することができる。

【0066】

なお、上記実施例１や実施例２でゲートウェイサーバとコンテンツサーバとがインターネットを介して接続されている場合には、ユーザＩＤが流出するのを防ぐため、ここでもゲートウェイサーバとコンテンツサーバの間で双方向ワンタイムＩＤ認証を行うことにより、経路上のユーザの匿名性をさらに保証することができる。また、ユーザを認証するサーバとコンテンツを提供するサーバとを分離するものとして説明しているが、これらを一体にしたコンテンツ提供システムを構築してもよい。また、本システムでは、携帯端末を紛失した場合に認証サーバで管理されている認証キーを無効にする装置を用意する。これは、万一、携帯端末を紛失してしまった場合に第三者により不正利用されるのを防ぐためである。

【産業上の利用可能性】

【0067】

本システムは、経路上のユーザの匿名性を保証してコンテンツサーバにおいてユーザを特定するモデルと、経路上及びコンテンツサーバにおいてユーザの匿名性を保証するモデルの２種類に利用することができる。

【0068】

経路上のユーザの匿名性を保証してコンテンツサーバにおいてユーザを特定するモデルは、経路上では匿名性が保障されているが、認証サーバによりコンテンツサーバのユーザＩＤを特定できるモデルとして構成される。コンテンツサーバには、必要な個人情報を登録しているため、ユーザＩＤから必要な個人情報を取り出すことができる。ユーザは個人情報を送信する必要はない。個人情報の例としては、名前、住所、生年月日、決済に使える銀行口座番号、クレジット番号などが挙げられる。このモデルとしては、インターネットバンキングモデル（図１８参照）や仮想店舗モデル（図１９参照）、競馬のインターネット投票モデル（図２０参照）、インターネット航空券発券モデル（図２１参照）等が挙げられる。

【0069】

インターネットバンキングモデルは、ユーザＩＤ、パスワード、口座番号などを携帯から入力することなくインターネットバンキングシステムが提供するサービスを利用することができる。また、仮想店舗モデルは、ユーザＩＤ、パスワード、銀行口座番号、クレジット番号などを携帯から入力することなく仮想店舗が提供するオンラインショッピングサービスを利用することができる。また、競馬のインターネット投票では、ユーザの指示でユーザの銀行口座で決済して馬券を購入し、レース終了後には自動的に配当金がユーザの銀行口座に振り込まれる。インターネット航空券発券では、銀行口座番号あるいはクレジット番号により航空券を購入すると、利用ポイントがユーザに加算される。また貯まった利用ポイントを景品に交換することもできる。

【0070】

一方、経路上及びコンテンツサーバにおいてユーザの匿名性を保証するモデルは、コンテンツサーバには、ユーザＩＤを含めて個人情報が何も登録されていない。そして、コンテンツサーバへは匿名性を保障したままアクセスできるモデルとして構成される。このモデルとしては、電子投票モデル（図２２参照）、電子アンケートモデル（図２３参照）等が挙げられる。電子投票モデルは、電子投票サーバでは投票された結果のみをデータベースに記録し、どのユーザが投票したかは知りえない。一度投票したユーザは再投票が出来ないように認証サーバで設定する。投票管理機関は、有権者が匿名性を保って電子投票システムにアクセスできるように、安全な方法で携帯端末用のアプリケーションと認証キーを有権者に配布する。また、電子アンケートモデルは、記入されたアンケートのみをデータベースに記録し、誰が記入したかは知りえない。一度アンケートに記入したユーザは再度記入が出来ないように認証サーバで設定する。アンケート実施機関は、アンケート回答者が匿名性を保って電子アンケートサーバにアクセスできるように、安全な方法で携帯端末用のアプリケーションと認証キーをアンケート回答者に配布する。

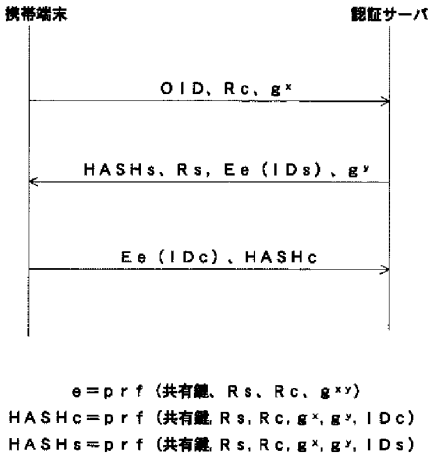
【図面の簡単な説明】

【0071】

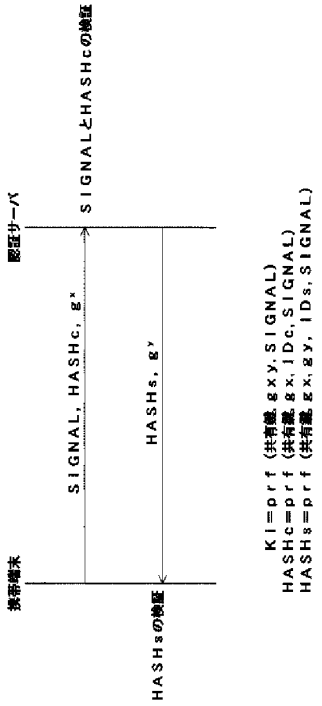
【図1】双方向ワンタイムＩＤ認証について説明するシーケンス図
【図2】双方向ワンタイムＩＤ認証について説明するシーケンス図
【図3】双方向ワンタイムＩＤ認証について説明するシーケンス図
【図4】本発明の第１及び第２実施例での初期段階を示す図
【図5】本発明の第１及び第２実施例での認証キーを取得するまでのプロセスを示す図
【図6】本発明の第１実施例でのセッションＩＤを取得するまでのプロセスを示す図
【図7】本発明の第１実施例でのコンテンツを取得するまでのプロセスを示す図
【図8】本発明の第２実施例でのトークンを取得するまでのプロセスを示す図
【図9】本発明の第２実施例でのコンテンツを取得するまでのプロセスを示す図
【図10】本発明の第１実施例での認証キーを取得するまでのシーケンスを示す図
【図11】本発明の第１実施例でのセッションＩＤを取得するまでのシーケンスを示す図
【図12】本発明の第１実施例でのコンテンツを取得するまでのシーケンスを示す図
【図13】本発明の第１実施例での自動的に再認証を行うシーケンスを示す図
【図14】本発明の第２実施例でのトークンを取得するまでのシーケンスを示す図
【図15】本発明の第２実施例でのセッションＩＤとコンテンツを取得するまでのシーケン

スを示す図
【図16】本発明の第２実施例でのＣｏｏｋｉｅ登録されたセッションＩＤを用いてコンテンツを取得するまでのシーケンスを示す図
【図17】本発明の第２実施例でのマニュアルで再認証を行うシーケンスを示す図
【図18】本発明のシステムをインターネットバンキングモデルに利用した様子を示す図
【図19】本発明のシステムを仮想店舗モデルに利用した様子を示す図
【図20】本発明のシステムを競馬のインターネット投票モデルに利用した様子を示す図
【図21】本発明のシステムをインターネット航空券発券モデルに利用した様子を示す図
【図22】本発明のシステムを電子投票モデルに利用した様子を示す図
【図23】本発明のシステムを電子アンケートモデルに利用した様子を示す図
【図24】従来のインターネット経由で電子商取引や金銭取引等のサービスを提供するコンテンツサーバとユーザとの間で行われる固定情報を使った認証手段を示す図

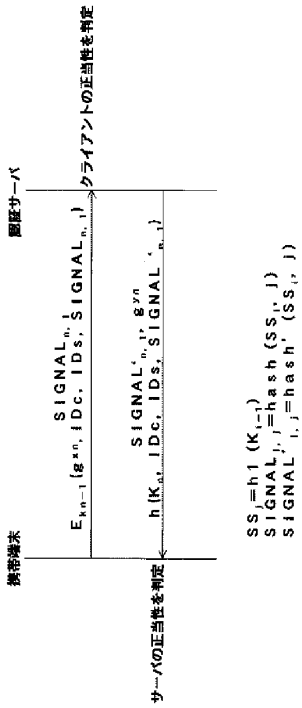
【図1】



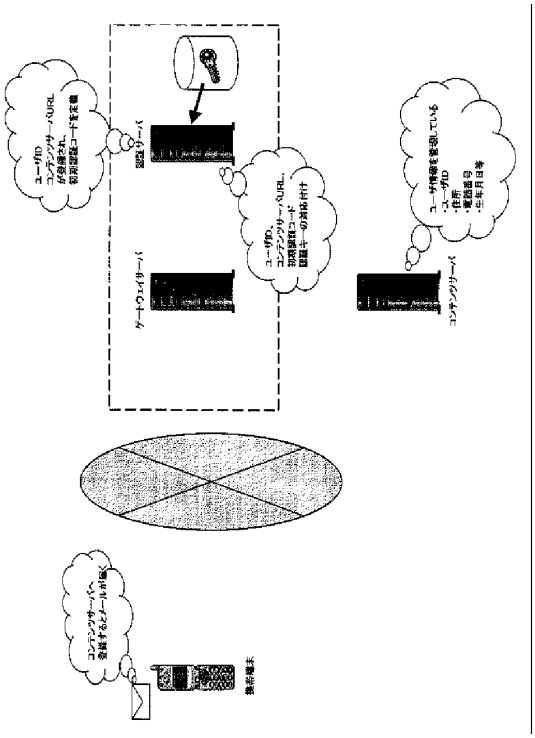
【図2】



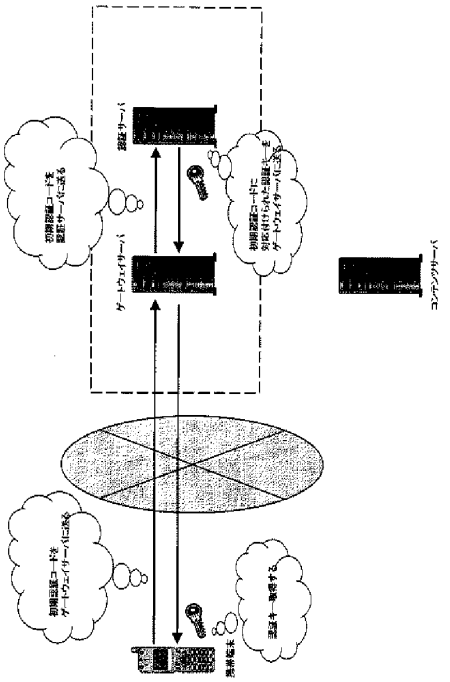
【図3】


認証サーバ
携帯端末
クライアントの正当性を判定
サーバの正当性を判定
SIGNAL n, 1
E k n-1 (g x n, IDc, IDs, SIGNAL n, 1)
SIGNAL' n, 1, g y n
h (K n, t, IDc, IDs, SIGNAL ' n, 1)
SS j=h1 (K i-1)
SIGNAL i, j=hash (SS i, j)
SIGNAL' i, j=hash' (SS i, j)

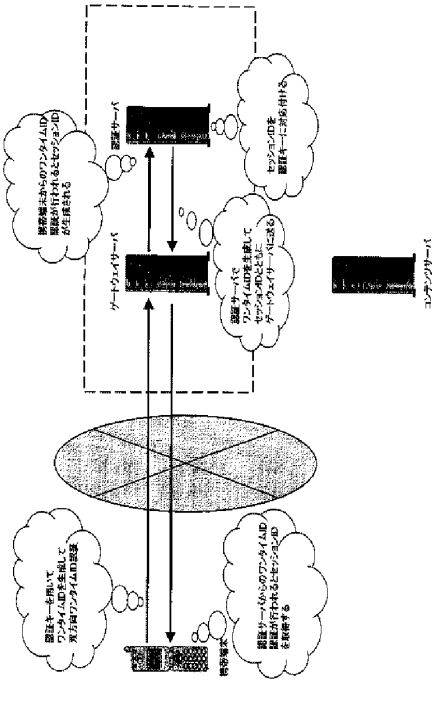
【図4】



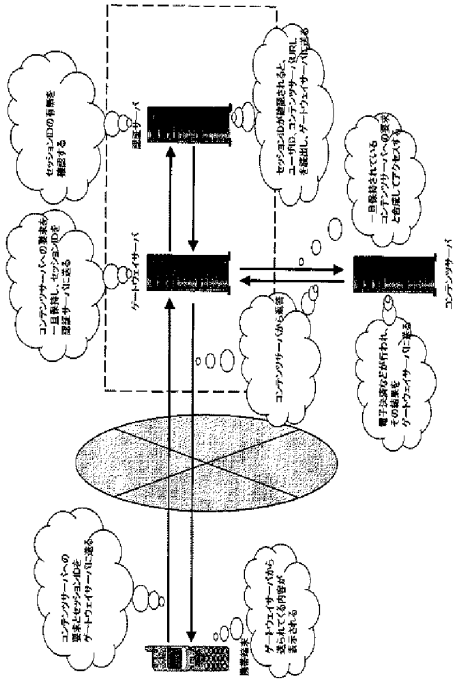
【図5】



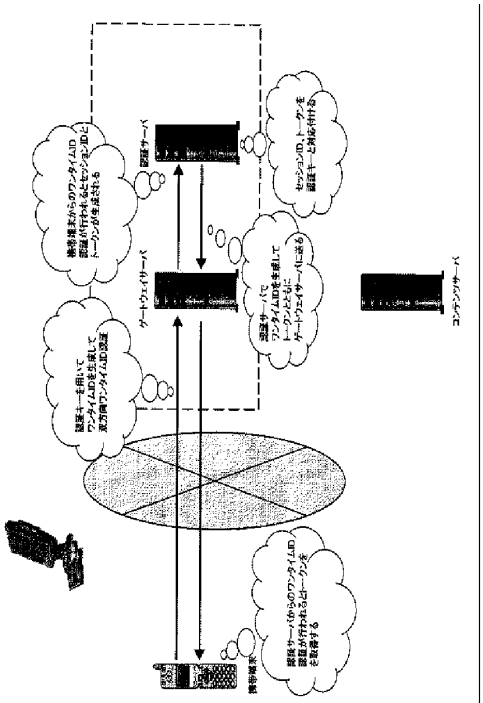
【図6】



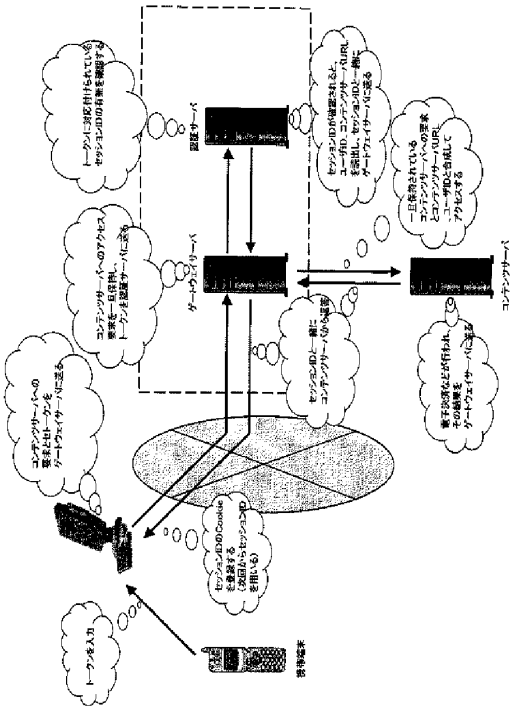
【図7】



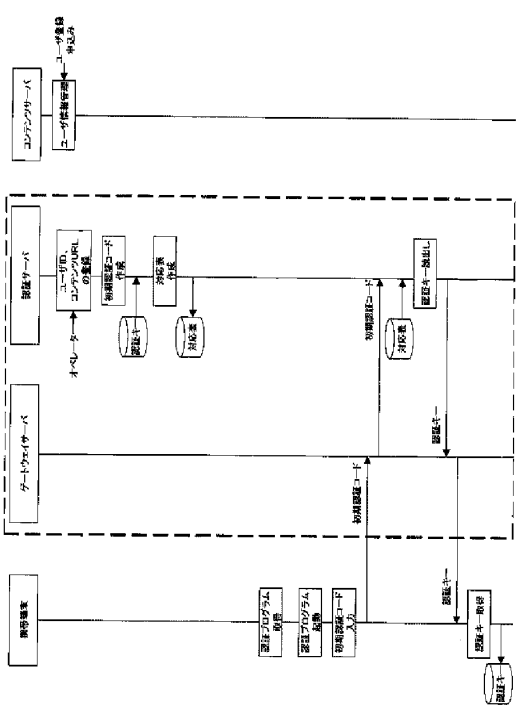
【図8】



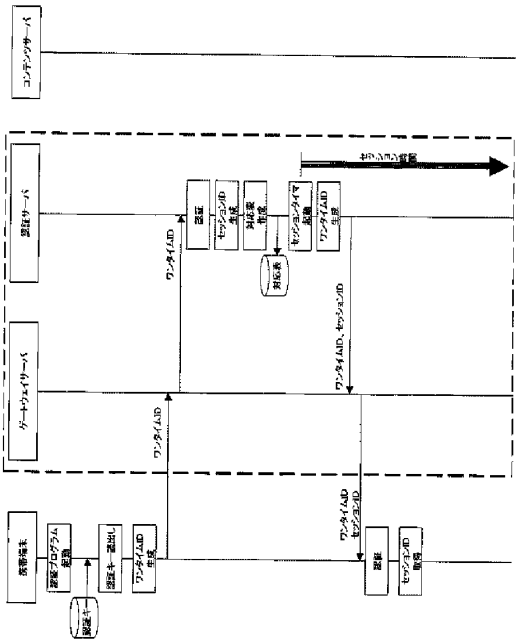
【図9】



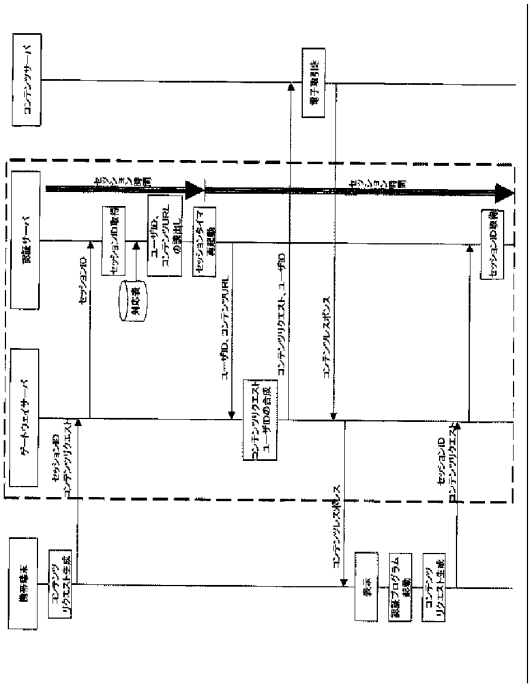
【図10】



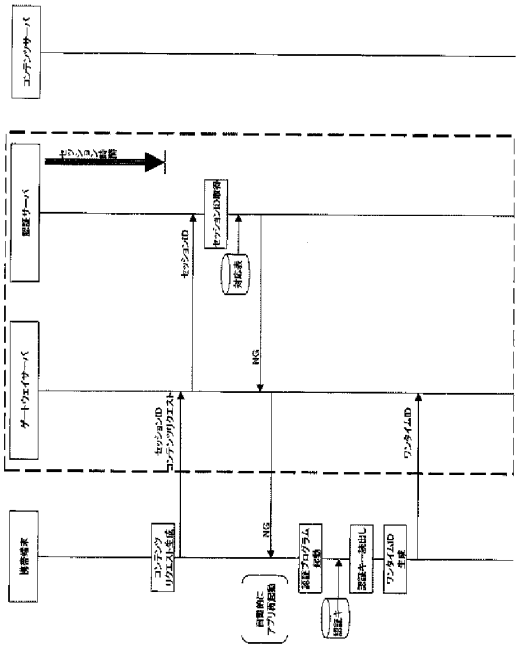
【図11】



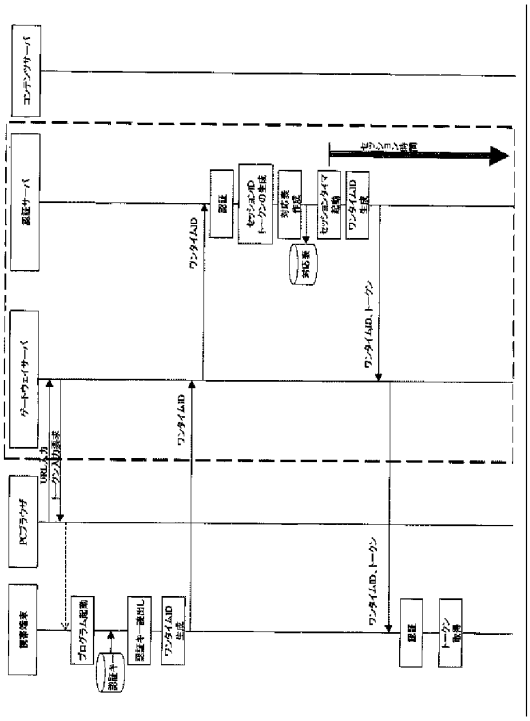
【図12】



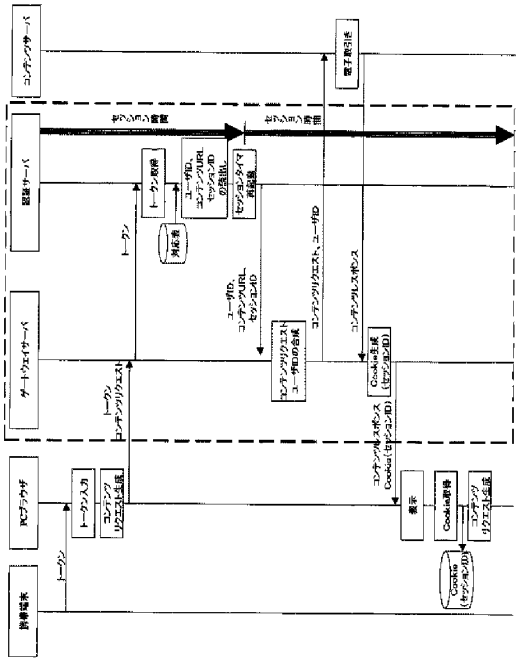
【図13】



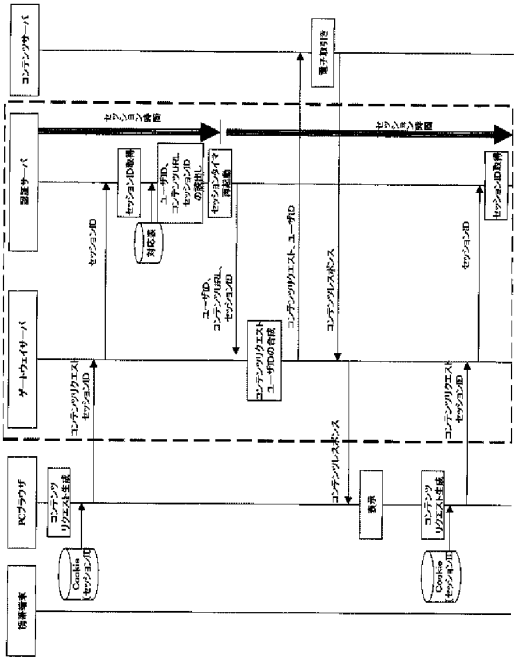
【図14】



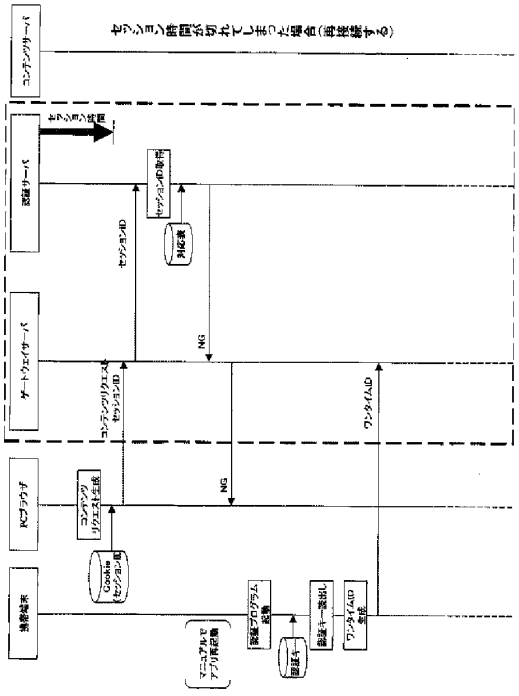
【図15】



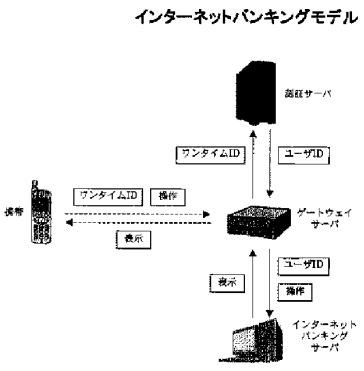
【図16】



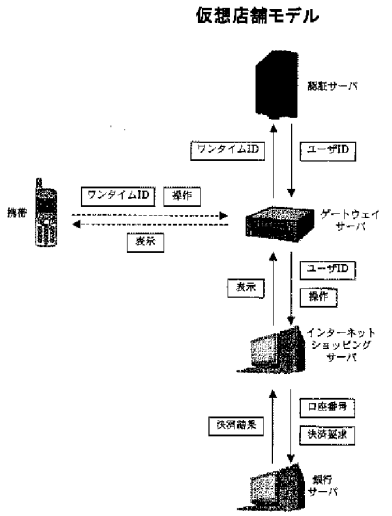
【図17】



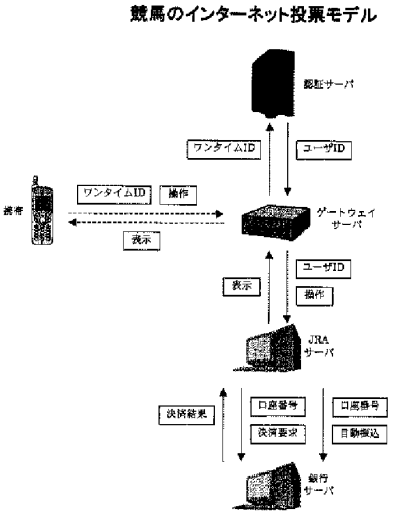
【図18】



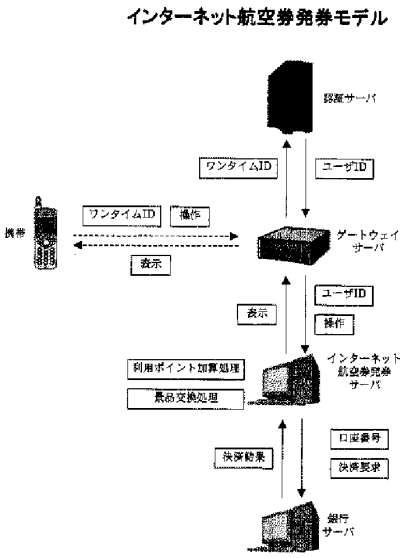
【図19】



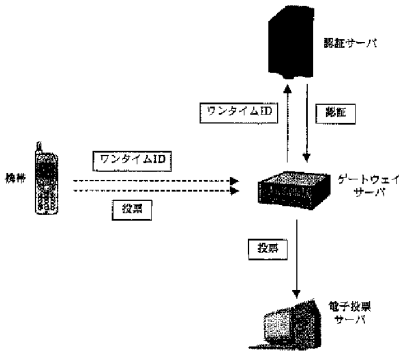
【図20】



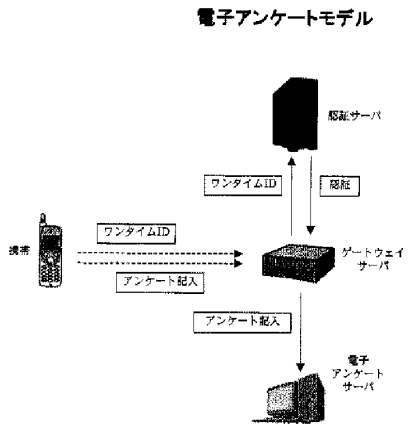
【図21】



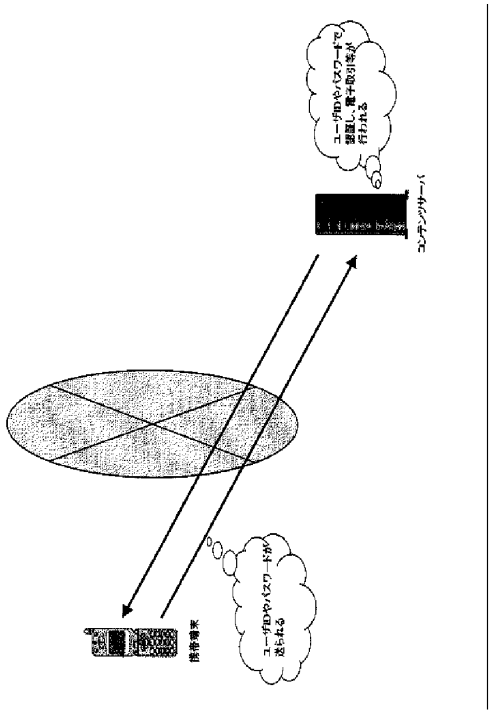
【図22】



【図23】


電子アンケートモデル
認証サーバ
ワンタイムID
認証
携帯
ワンタイムID
ゲートウェイ
サーバ
アンケート記入
アンケート記入
電子
アンケート
サーバ

【図24】


コンテンツサーバ
携帯電話

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JP2006155263

【課題】

The present invention utilizes existing authentication server for performing personal authentication based on the user ID and password, economical construction having high security authentication system using the one-time ID. A user is, in the case of performing the identity authentication, enter the user ID of its own to the one-time ID generation device 1 0. Onetime ID generating unit 1 0 generates the one-time ID and a user ID and the current time that has been input. The user then sends an authentication request including the above-described one-time ID and password from the terminal device 20 to the authentication server 30. Authentication server 30 transmits the including the one-time ID in the authentication request conversion request to the conversion server 40. The conversion server 40 calculates a user ID and a one-time ID and the current time is included in the conversion request, and returns the authentication server 30. The authentication server 30, by comparing the password registered in the authentication information storage section 35 in association with the user ID, and password in the authentication request, performs user authentication. .FIELD 7

One-time ID authentication system, an authentication server, the conversion server, one-time ID authentication method and program

[0001]

[0001] The present invention relates to a personal authentication technology in a network system, in particular, by using each time a different user ID for each logon (onetime ID), relates to personal authentication technology increase the security level.

[0002]

[0002] The personal authentication system in a network system, various ones have been known. 1 3 is a block diagram showing a conventional most commonly in the personal authentication system that is utilized configured. Referring to the figure, personal authentication system includes an authentication server 1 00, and a terminal device 200 used by a user, they are connected to each other via the Internet, a network 300 such as LAN.

[0003]

[0003] In personal authentication system shown in FIG. 1 3, the user of the terminal device 200, when performing authentication, an authentication request including the own user ID and password, and transmitted from the terminal device 200 to the authentication server 1 00 . Authentication means 1 01 of the authentication server 1 00, upon via the transmitting and receiving unit 1 02 receives an authentication request from the terminal apparatus 200, referring to the authentication information storage unit 1 03 and the user ID and password for each user is registered in association and, perform personal authentication. That is, a password in association with the user ID in the authentication request is registered in the authentication information storage unit 1 03, compares the password in the authentication request, if they match, the authentication succeeds, both the mismatch case, the authentication failure.

[0004]

[0004] However, personal authentication system shown in FIG. 1 3, for each use the same user ID and password, there is a problem in terms of security. Therefore, I like to use different passwords (one-time password) each time the personal authentication system shown in FIG. 1 4 has been proposed (e.g., see Patent Document 1).

[0005]

[0005] Referring to FIG. 14, personal authentication system includes an authentication server 400, the terminal device 500 used by a user, and a one-time password generation unit 600, the authentication server 400 and the terminal device 500, the Internet, They are connected to each other via a network 700 such as a LAN.

[0006]

User [0006] terminal 500, when performing personal authentication, first, the one-time password generation unit 600 inputs the user ID of its own. Thus, the one-time password generation unit 600 generates a one-time password based on the input user ID and the current time, and displays the generated one-time password on the display section (not shown). Incidentally, one-time password generation apparatus 600, for example, be realized by a mobile phone incorporating a program for the one-time password generation.

[0007]

[0007] The user inputs and one-time password is displayed, the same and the own user ID to the terminal device 500. Thus, the terminal device 500 transmits an authentication request including the one-time password and user ID to the authentication server 400.

[0008]

[0008] Authentication unit 401 in the authentication server 400 receives the authentication request through the transceiver unit 402, passes the user ID contained in the authentication request to the one-time password generation unit 403, generating a one-time password to instruct. Thus, the one-time password generation unit 403 receives the current time from the clock 404, and generates a one-time password based on the current time and the above user ID. Then, a one-time password generated is compared with the one-time password included in the authentication request, if they match, the authentication succeeds, if they do not match, the authentication failure. JP 2002-259344 JP

[0009]

[0009] According to the authentication system described in Patent Document 1 described above, since different passwords are used each time, it is possible to higher security.

[001 0]

[001 0] Incidentally, even in the engine have already introduced the authentication server 1 00 as shown in FIG. 1 3, increased security is desired. To improve security, may be introduced personal authentication system that performs authentication using the one-time password as shown in FIG. 1 4, then, the cost becomes very high.

[001 1]

[001 1] [purpose of the invention] It is an object of the present invention have the authentication information storage unit in which the user ID and password are registered in association, by utilizing the existing authentication server for performing personal authentication based on the user ID and password, It is to such a high security authentication system using the one-time ID can be economically constructed.

[001 2]

[001 2] The first one-time ID authentication system according to the present invention, And the terminal device, a one-time ID authentication system comprising an authentication server with authentication information storage unit in which the user ID and password of a user are registered in association, and a conversion server, It said terminal device, Has a one-time ID generated based on the user ID and the current time, a structure for transmitting an authentication request including the password to the authentication server, The authentication server, When the authentication request from the terminal device is sent, to generate a translation request including the one-time ID in the authentication request, and sends the converted request the generation to said conversion server, the conversion request from the conversion server when a user ID is sent as a conversion result for, by comparing the password of password and said in authentication request registered in the authentication information storage unit in association with the user ID, if they match, the authentication has a configuration

that success, The conversion server, When the conversion request from the authentication server is sent, calculates a user ID on the basis of the one-time ID and the current time in the conversion request, to have a structure to return the user ID the calculated to the authentication server the features.

[001 3]

[001 3] The second of the one-time ID authentication system according to the present invention, in the first of the one-time ID authentication system, The generates a one-time ID based on the user ID and the current time input by the user of the terminal device, the one-time ID generating apparatus including a one-time ID generating means for displaying on the display unit the one-time ID to the said generated characterized by comprising.

[001 4]

[001 4] Third one-time ID authentication system according to the present invention, in the first one-time ID authentication system, A user ID storage unit by the user ID of the user of the terminal device is registered, The generates a one-time ID based on the user ID and the current time registered in the user ID storage unit, the one-time ID generation including the one-time ID generating means for displaying on the display unit the one-time ID to the said generated characterized by comprising a device.

[001 5]

[001 5] The fourth one-time ID authentication system according to the present invention, in the first to the third one-time ID authentication system, The authentication server, When the authentication request from the terminal device is sent, and a conversion request means for generating a conversion request including the one-time ID in the authentication request, transmits the converted request the generation to said conversion server, When the user ID as a conversion result for the conversion request from the conversion server is sent, it compares the password of password and said in authentication request registered in the authentication information storage unit in association with the user ID, If they match, characterized by comprising a comparison means for the authentication succeeds.

[001 6]

[001 6] The fifth one-time ID authentication system according to the present invention, in the fourth one-time ID authentication system, The conversion server, When the conversion request from the authentication server is sent, it calculates a user ID on the basis of the one-time ID and the current time in the conversion request, provided with a conversion means for transmitting the user ID to the calculated to the authentication server characterized in that was.

[001 7]

[001 7] Sixth onetime ID authentication system according to the present invention, in the second or third one-time ID authentication system, The one-time ID generation device, And functions holding unit at the time of dividing the day into multiple time zones, the one-time ID generation function for each time zone is stored, Of the one-time ID generation function stored in the function number storing unit, generate a one-time ID generation function for time zone including the current time, and the current time, the one-time ID based on the user ID and a one-time ID generation computing means for, The conversion server, And inverse function holding unit at the time of dividing the day into a plurality of time zones, the user ID calculating function for each time period is stored, When the conversion request from the authentication server is sent, of the user ID calculating function for each time period stored in said inverse function holding unit, a user ID calculating function for time zone including the current time When, characterized by comprising a current time, a user ID calculating arithmetic means for calculating a user ID on the basis of the one-time ID in said conversion request.

[001 8]

[001 8] The authentication server according to the present invention, And authentication information storage unit in which the user of the user ID and password has been registered in association with, When the authentication request including the user ID and password sent from the terminal device, generating a conversion request including the one-time ID in the authentication request, a conversion request means for transmitting a conversion request the generation to the conversion server , When the user ID as a conversion result for the conversion request from the conversion server is sent, it compares the password of password and said in authentication request registered in the authentication information storage unit in association with the user ID, If they match, characterized by comprising a comparison means for the authentication succeeds.

[001 9]

[001 9] conversion server according to the present invention, When the conversion request including the one-time ID is sent from the authentication server calculates a user ID on the basis of the one-time ID and the current time in the conversion request, and transmits the user ID to the calculated to the authentication server characterized by comprising a conversion means.

[0020]

[0020] one-time ID authentication method according to the present invention, Terminal device transmits the one-time ID generated based on the user ID and the current time, the authentication request including the password to the authentication server, The authentication server having an authentication information storage unit in which the user having the user ID and password are registered in association with the, when an authentication request from the terminal device is sent, including the one-time ID in the authentication request conversion generate a request, sends the converted request the generation to the conversion server, Returning said conversion server, when a conversion request from the authentication server is sent, calculates a user ID on the basis of the one-time ID and the current time in the conversion request, the user ID the calculated to the authentication server and, The authentication server, when the user ID is sent as a conversion result for the conversion request from the conversion server, a password of password and said in authentication request registered in the authentication information storage unit in association with the user ID comparing the door, if they match, characterized by a successful authentication.

[0021]

[0021] The first program according to the present invention, The computer with the authentication information storage unit in which the user having the user ID and password are registered in association, When the authentication request including the user ID and password sent from the terminal device, generating a conversion request including the one-time ID in the authentication request, translation request means for transmitting a conversion request the generation to the conversion server, When the user ID as a conversion result for the conversion request from the conversion server is sent, it compares the password of password and said in authentication request registered in the authentication information storage unit in association

with the user ID, If they match, to function as a comparison means for a successful authentication.

[0022]

[0022] The second program according to the present invention, The computer, When the conversion request including the one-time ID is sent from the authentication server calculates a user ID on the basis of the one-time ID and the current time in the conversion request, and transmits the user ID to the calculated to the authentication server to function as a conversion means.

[0023]

[0023] [action] When the user performs the authentication, send the authentication request from its own terminal device to the authentication server. The authentication request, and the one-time ID generated based on the user ID and the current time of the user, contains the password for the user. One-time ID, for each its generation time, since the value is different, it is possible to higher security. The authentication server receives the authentication request, generates including the one-time ID in the authentication request conversion request, and sends the conversion server. Conversion server, based on the one-time ID and the current time in the conversion request, calculates a user ID of the user, and returns the user ID calculated in the authentication server. The authentication server performs the user ID is returned, and password in the authentication request, the utilizing the authentication information storage unit personal authentication.

[0024]

According to [0024] the present invention, it becomes possible to economically configure security high personal authentication system using the one-time ID. The reason is that the conversion server to return the one-time ID contained in the authentication request sent from the terminal device to the user ID is provided, the one-time ID to the existing authentication server for performing personal authentication by user ID and password This is because the available in personal authentication using.

[0025]

[0025] With reference to drawings, embodiments of the present invention will be described in detail.

[0026]

[0026] [Description of Configuration of First Embodiment 1 is a block diagram showing an overall configuration of a first embodiment of the one-time ID authentication system according to the present invention. Referring to the figure, the one-time ID authentication system of this embodiment, the one-time ID generation unit 10 used by a user, the terminal device 20 in which the user uses, the authentication server 30, a conversion server 40 wherein, the terminal apparatus 10, the authentication server 30 and the conversion server 40 are connected to each other via the Internet, a network 50 such as a LAN.

[0027]

[0027] onetime ID generating unit 10 generates a one-time ID based on the user ID and the current time input by the user, a function to be presented to the user.

[0028]

[0028] FIG. 2 is a block diagram showing a configuration example of a one-time ID generating apparatus 10 having the function described above, an input section 11 of the numeric keys or the like, a one-time ID generating unit 12, a clock that displays the current time 16, and a display portion 17 such as LCD.

[0029]

[0029] onetime ID generating unit 12 includes a function storage unit 13, a calculating unit 14, and a current time input means 15.

[0030]

[0030] time input unit 1 5 has a function of inputting the current time from the clock 1 6. In this embodiment, the time input unit 1 5, when the timepiece 1 6 is displaying: minutes: Of the second, time: shall enter a fraction only. In other words, time input means 1 5, to enter the time in minutes.

[0031]

[0031] in the function storage unit 1 3, the function to use in generating the one-time ID (one-time ID generation function) is stored.

[0032]

[0032] calculating means 1 4, the user ID input from the input unit 1 1, for the current time the time input unit 1 5 is input, according to the one-time ID generation function stored in the function storage section 1 3 It was calculated onetime ID by performing a calculation, a function of displaying the one-time ID calculated in the display unit 1 7.

[0033]

[0033] In addition, the one-time ID generation means 1 2 of the one-time ID generating device 1 0, are those that can be realized by a CPU (computer), if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as a one-time ID generating unit 1 2, a semiconductor memory, prepared other recording medium, to read the program in the computer. The computer, by controlling its operation according to the read program, on the self computer, to implement the one-time ID generating unit 1 2. Further, the one-time ID generation apparatus 1 0 may also be realized by utilizing a portable telephone with a built-in CPU. That is, providing a recording medium such as a recording disk a program for operating the CPU as a onetime ID generating unit 1 2, to read the program to the CPU. The CPU, by controlling its operation according to the read program to realize the one-time ID generating unit on the own CPU.

[0034]

[0034] The terminal device 20 has function for sending an authentication request including the one-time ID and the password to the authentication server 30, a function for presenting the authentication result sent from the authentication server 30 to the user.

[0035]

[0035] FIG. 3 is a block diagram showing a configuration example of a terminal device 20 having the function described above, a transmitting and receiving unit 21, a control unit 22, an input unit 23 such as a keyboard, a display unit 24 such as an LCD It is equipped with a.

[0036]

[0036] transmitting and receiving means 21 has a function of exchanging data via a network 50.

[0037]

[0037] The control unit 22 has a function of transmitting the input unit 23 function for generating an authentication request including the one-time ID and password input, the generated authentication request via the communication means 21 to the authentication server 30, having like function of displaying an authentication result sent from the authentication server 30 on the display unit 24.

[0038]

[0038] In addition, the terminal device 20 is as it can be implemented by a computer such as a personal computer, if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as a terminal device, a semiconductor memory, prepared other recording medium, to read the program in the computer. The computer, by controlling its operation according to the read program, on the self computer, realizes transmission and reception unit 21, the control unit 22.

[0039]

[0039] The authentication server 30, when the authentication request including the one-time ID and password sent from the terminal device 20 acquires the user ID corresponding to the one-time ID by using the conversion server 40, the user It has a function of performing authentication based on the ID and the password in the authentication request.

[0040]

[0040] FIG. 4 is a block diagram showing a configuration example of the authentication server 30 having the functions described above, a transmitting and receiving unit 31 , an authentication unit 32, and an authentication information storage unit 35.

[0041]

[0041] in the authentication information storage unit 35, as shown in FIG. 5, the user ID of the user, password, access rights, name, ... it is registered in association.

[0042]

[0042] transmitting and receiving means 31 has a function of exchanging data via a network 50.

[0043]

[0043] authentication means 32 includes a translation request unit 33, the comparing means 34.

[0044]

[0044] conversion request means 33, when receiving an authentication request from the terminal device 20 via the transmitting and receiving unit 31 transmits a containing the one-time ID in the authentication request conversion request to the conversion server 40, the conversion request having the ability to pass the user ID is returned from the conversion server 40 in response to the comparison means 34. Translation request unit 33 has a configuration that is not provided in the authentication server 100 shown in FIG. 13, in the case of realizing the authentication server 30 by using the existing authentication server 100 needs to incorporate this configuration.

[0045]

[0045] comparing means 34 compares the password in association with the user ID is registered in the authentication information storage section 35 passed from the translation request unit 33, and a password in the authentication request from the terminal device 20, If they match, the authentication succeeds, if they do not match, has the function of the authentication failure. Comparing means 34 has a configuration that is provided to the authentication server 100 shown in FIG. 13.

[0046]

[0046] In addition, the authentication server 30, are those that can be implemented by a computer, if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as the authentication server, a semiconductor memory, prepared other recording medium, to read the program in the computer. Computer controls its own operation in accordance with the read program, on its own computer, sending and receiving means 31, to achieve the authentication means 32.

[0047]

[0047] conversion server 40, when the conversion request from the authentication server 30 including the one-time ID is sent, it calculates a user ID on the basis of the above one-time ID and the current time, and returns the user ID calculated It has a function.

[0048]

[0048] FIG. 6 is a block diagram illustrating an exemplary configuration of a conversion server 40 having the function described above, comprises a transceiver unit 41, a conversion unit 42, and a clock 46 that displays the current time.

[0049]

[0049] transmitting and receiving means 41 has a function of transmitting and receiving data via the network 50.

[0050]

[0050] conversion unit 42 includes an operation unit 43, an inverse function storage unit 44, and a time input section 45.

[0051]

[0051] time input unit 45 has a function of inputting the current time in minutes from the clock 46.

[0052]

[0052] Conversely function storage unit 44, the one-time ID and the function for obtaining the user ID from the current time (user ID calculating functions) is stored.

[0053]

[0053] calculating means 43, upon receiving a conversion request sent from the authentication server 30 via the transmitting and receiving unit 41, the one-time ID contained in it, in minutes

time input unit 45 is input current has a time, a function of calculating a user ID on the basis of the functions for the user ID calculating held in the inverse function holding unit 44, and transmits the user ID, which is calculated to the authentication server 30.

[0054]

[0054] In addition, the conversion server 40, are those that can be implemented by a computer, if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as a conversion server, a semiconductor memory, prepared other recording medium, to read the program in the computer. The computer, by controlling its operation according to the read program, on the self computer, transceiver means 41 , realizing the conversion means 42.

[0055]

[0055] [Description of Operation of First Embodiment Next, with reference to the drawings, the operation of this embodiment will be described in detail.

[0056]

[0056] The user of the terminal device 20, when performing personal authentication, and starts the one-time ID generation unit 1 0, inputs the user ID of itself from the input unit. 1 1 (a in Fig. 7).

[0057]

[0057] One-time ID generating device 1 0 onetime ID generating means 1 2, when activated, becomes an input waiting state of the user ID, the user ID is input from the input unit 1 1 by the user, time input means 1 5 enter the current time in minutes from the clock 1 6 using the (step S81 , S82 in FIG. 8). Thereafter, generation operation means 1 4, the one-time ID generation function stored in the function storage unit 1 3, a user ID input by the user, time input means 1 5 the one-time ID on the basis of the current time entered (step S83). Here, the function for one-time ID generation, for example, may be employed functions such as (onetime ID) = (User ID) ×

(current time). Thereafter, computing unit 1 4 displays the one-time ID calculated in the display section 1 7 (step S 84).

[0058]

[0058] When the user has the one-time ID is displayed on the display unit 1 7, and inputs the one-time ID and password displayed on the terminal device 20 (b in FIG. 7, c). Control means 22 in the terminal device 20, when the one-time ID and a password are inputted from the input unit 23, and transmits the containing them authentication request to the authentication server 30 (d- in FIG. 7).

[0059]

[0059] conversion request means 33 of the authentication server 30 receives the authentication request sent from the terminal device 20 via the transmitting and receiving unit 31 , generates a conversion request including the one-time ID in the authentication request and it sends it to the conversion server 40 (e in step S 91 , S 92 and 7 in FIG. 9). Thereafter, conversion request means 33, a return waiting state of the conversion result (user IDs) (step S 93).

[0060]

[0060] On the other hand, converter 42 in the conversion server 40 receives the conversion request from the authentication server 30 via the transmitting and receiving unit 41 , as shown in the flowchart of FIG. 1 0, by using the first time input means 45 enter the current time in minutes from the clock 46 (step S1 01). Thereafter, computing unit 43, and functions for the user ID calculating held in the inverse function holding unit 44, and the current time in minutes time input unit 45 is input, the user ID based on the one-time ID in the conversion request calculates and returns the user ID which is calculated to the authentication server 30 (f in step S 1 02, S 1 03 and FIG. 7). Here, the user ID calculating functions stored in the inverse function holding unit 44 is an inverse function of the one-time ID generation function stored in the function storage unit 1 3 of the one-time ID generating device 1 0, for example, , one-time ID generation function is, if the (one-time ID) = (user ID) $\times$ (the current time), the function for the user ID calculation, (user ID) = (one-time ID) $\div$ (the current time) to become. However, the function holding unit 1 3, the one-time ID generation function held by the inverse function holding unit 44, the function for the user ID calculating, not limited to the example described above.

[0061]

[0061] conversion request means 33 of the authentication server 30 in the return waiting state of the conversion result, and a result conversion sent from the conversion server 40 (user ID) is received via the transmitting and receiving means 31 , comparison means it pass to the 34. Thus, comparing unit 34, the authentication information storage section 35, it retrieves the password registered in association with the user ID, and compared with the password in the authentication request sent from the terminal device 20 (in FIG. 9 step S94). Then, if they match notifies the authentication success to the authentication requesting terminal device 20 (step S95 is YES, S 96), in the case of disagreement, and notifies the authentication failure to the terminal device 20 (step S95 is NO , g of S97 and 9). Even if the user ID corresponding to the authentication information storage unit 35 is not registered, the authentication failure.

[0062]

[0062] Control unit 22 in the terminal device 20 receives via the communication means 21 an authentication result (authentication success or authentication failure), and displays it on the display unit 24. If the authentication success is displayed, the user of the terminal device 20, it means that acquired the access right to the system, it is possible to access the system. In contrast, if the authentication failure is displayed, the user performs the operation described above again.

[0063]

[0063] In the embodiment described above, converter 42 in the conversion server 40, upon receiving a conversion request from the authentication server 30, based on a one-time ID in the conversion request, to the present time user although the ID to calculate only one, and the user ID corresponding to the current time, asked two of the user ID of the user ID corresponding to one minute before the time than the current time, those two user ID it may be returned to the authentication server 30. Then, the comparison unit 34 within the authentication server 30 in which two user ID is returned, either one of the two password registered in the authentication information storage section 35 in association with the two user ID, if they match the password in the authentication request, it is determined that the authentication is successful. By doing so, the user of the operating time (time from the generation of the one-time ID, until the user inputs the

one-time ID and password to the terminal device 20), a generation time of the one-time ID, the conversion server even if the difference between the reception time of the conversion request occurs at 40, the difference is within the 1 minute, it can be a successful authentication.

[0064]

[0064] Further, in the embodiment described above, the function holding unit 1 3, inverse function holding unit 44 respectively onetime ID generation function have been adapted to store one by one function for the user ID calculating a plurality of one time ID generation function may be stored functions for the user ID calculating, it may be changed using function depending on the time zone. When doing so, for example, dividing one day into a plurality of time periods, different one-time ID generation function for each time period, a function for calculating a user ID function storage unit 1 3, the customer function storage unit 44 It is registered. In the computing unit 1 4 of the one-time ID generating device 1 0, when generating the one-time ID at step S83 in FIG. 8, of the one-time ID generation function for each time zone is stored in the function storage unit 1 3, and the one-time ID generation function for time zone including the current time, and the current time, and generates a one-time ID with the user ID. Further, the arithmetic unit 43 in the conversion server 40, when calculating the user ID in step S1 02 of FIG. 1 0, of the function for the user ID calculating stored in the inverse function holding unit 44, the time zone including the current time and user ID is calculated for the function of the use, to calculate the current time, the user ID from a one-time ID.

[0065]

[0065] [Effect of the First Embodiment According to this embodiment, it is possible to economically configure security high personal authentication system using the one-time ID. This is because, by providing the conversion server 40 for returning the one-time ID contained in the authentication request sent from the terminal device 20 to the user ID, existing authentication server 30 for authentication by the user ID and password the is because the available in personal authentication using the one-time ID.

[0066]

[0066] Further, according to the present embodiment, it is possible to extremely high security. The reason is because they like to use a different one-time ID generation function, a function for

the user ID calculated for each time.

[0067]

[0067] Second Embodiment Next, a description will be given of a second embodiment of the one-time ID authentication system according to the present invention. One-time ID authentication system of this embodiment, the one-time ID authentication system shown in FIG. 1, in place of the one-time ID generating apparatus 10 shown in FIG. 2, the one-time ID generator 10a shown in FIG. 11 It is achieved by the use.

[0068]

[0068] onetime ID generator 10a shown in FIG 11 used in this embodiment, instead of the one-time ID generating unit 12, that it includes a one-time ID generating unit 12a, and a user ID storage unit 19 There points are added are different from the one-time ID generating unit 12 shown in FIG.

[0069]

The [0069] user ID holding unit 19, the user ID of the user of the terminal device 20 is registered.

[0070]

[0070] onetime ID generating 12a are that the user ID input means 18 for inputting a user ID stored in the user ID holding unit 19 has been added, is different from the one-time ID generating unit 12.

[0071]

[0071] Next, the operation of this embodiment. The operation other than the one-time ID

generator 1 2a are the same as the first embodiment, here will be described only the operation of the one-time ID generator 1 2a.

[0072]

User [0072] The terminal device 20, when performing personal authentication, activates the one-time ID generator 1 0a. As a result, the one-time ID generating means 1 2a of the one-time ID generating device 1 0a, enter the current time in minutes from the clock 1 6 using the time input means 1 5, further, a user ID by using the user ID input means 1 8 from the holding portion 1 9 to enter a user ID (step S1 21 , S1 22 in FIG. 1 2). Thereafter, computing unit 1 4 of the one-time ID generating means in 1 2a is a one-time ID generation function stored in the function storage unit 1 3, the current time the time input unit 1 5 is input, the user ID input unit 1 8 inputs and based on the user ID, and generates a one-time ID, and displays the generated one-time ID on the display section 1 7 (step S1 23, S1 24).

[0073]

[0073] [Effects of the Second Embodiment According to the present embodiment, in addition to the effects of the first embodiment, it can be made easier to generate operation onetime ID performed by the user. The reason is that the one-time ID generation unit 1 2a is provided with a user ID storage unit 1 9 by the user ID is registered, when the user the one-time ID generation, there is no need to input the user ID.

[0074]

[0074] can be used for authentication systems required high security.

[0075]

[0075] is a block diagram showing an overall configuration example of a first embodiment of the one-time ID authentication system according to the present invention. Configuration example of the one-time ID generating apparatus 1 0 is a block diagram showing the. It is a block diagram showing a configuration example of the terminal device 20. It is a block diagram showing a

configuration example of the authentication server 30. Is a diagram showing an example of contents of the authentication information storing section 35. It is a diagram illustrating a configuration example of a conversion server 40. It is a diagram for explaining the operation of the first embodiment. It is a flowchart illustrating a processing example of the one-time ID generator 1 0. It is a flowchart illustrating a processing example of the authentication server 30. It is a flowchart illustrating a processing example of a conversion server 40. A configuration example of a one-time ID generator 1 0a used in the second preferred embodiment of a one-time ID authentication system in the present invention is a block diagram showing. It is a block diagram showing a processing example of the one-time ID generator 1 0a. Using a conventional user ID and password is a block diagram showing an example of a personal authentication system. Is a diagram showing an example of a personal authentication system that uses a conventional user ID and one-time password.

Description of the code

[0076] 1 0,1 0a ... one-time ID generation device 1 1 ... input section 1 2,1 2a ... one-time ID generating means 1 3 ... function holding section 1 4 ... computing means 1 5 ... time input means 1 6 ... Clock 1 7 ... display unit 1 8 ... user ID input means 1 9 ... user ID holding section 20 ... terminal equipment 21 ... transmitting and receiving means 22 ... control means 23 ... input section 24 ... display unit 30 ... authentication server 31 ... transmitting and receiving means 32 ... authentication means 33 ... conversion request means 34 ... comparison means 35 ... authentication information storage unit 40 ... conversion server 41 ... transmitting and receiving means 42 ... conversion means 43 ... computing means 44 ... inverse function holding section 45 ... time input means 46 ... Clock 50 ... Network

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-155263
(P2006-155263A)
(43)公開日　平成18年6月15日(2006.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B085
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104

審査請求 有　請求項の数 11　ＯＬ　（全 16 頁）

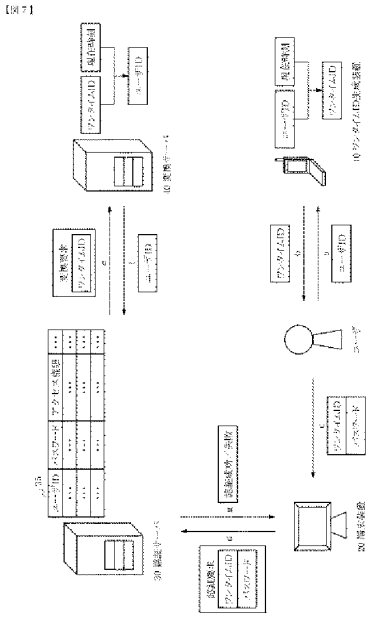
(21)出願番号　特願2004-345458 (P2004-345458)
(22)出願日　平成16年11月30日 (2004.11.30)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088959
弁理士　境　廣巳
(72)発明者　緒方　真一郎
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B085 AE02 AE03 AE23 BA06 BG07
5J104 KA01 NA05 PA07

(54)【発明の名称】ワンタイムＩＤ認証システム、認証サーバ、変換サーバ、ワンタイムＩＤ認証方法及びプログラム

(57)【要約】
【課題】　ユーザIDとパスワードとに基づいた本人認証を行う既存の認証サーバを利用し、ワンタイムIDを用いたセキュリティの高い本人認証システムを経済的に構成する。
【解決手段】　ユーザは、本人認証を行う場合、ワンタイムID生成装置10に自身のユーザIDを入力する。ワンタイムID生成装置10は、入力されたユーザIDと現在時刻とからワンタイムIDを生成する。その後、ユーザは、上記ワンタイムIDとパスワードとを含む認証要求を端末装置20から認証サーバ30へ送る。認証サーバ30は、認証要求中のワンタイムIDを含んだ変換要求を変換サーバ40へ送信する。変換サーバ40は、変換要求に含まれているワンタイムIDと現在時刻とからユーザIDを算出し、認証サーバ30に返却する。認証サーバ30は、上記ユーザIDに対応付けて認証情報記憶部35に登録されているパスワードと、認証要求中のパスワードとを比較することにより、本人認証を行う。
【選択図】　図7



【特許請求の範囲】
【請求項1】
端末装置と、ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えた認証サーバと、変換サーバとを含むワンタイムＩＤ認証システムであって、
前記端末装置が、
ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を前記認証サーバへ送信する構成を有し、
前記認証サーバが、
前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を前記変換サーバへ送信し、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする構成を有し、
前記変換サーバが、
前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却する構成を有することを特徴とするワンタイムＩＤ認証システム。
【請求項2】
請求項１記載のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザによって入力されたユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段を含むワンタイムＩＤ生成装置を備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項3】
請求項１記載のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザのユーザＩＤが登録されているユーザＩＤ記憶部と、
該ユーザＩＤ記憶部に登録されているユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段とを含むワンタイムＩＤ生成装置を備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項4】
請求項１、２または３記載のワンタイムＩＤ認証システムにおいて、
前記認証サーバが、
前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を前記変換サーバへ送信する変換要求手段と、
前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項5】
請求項４記載のワンタイムＩＤ認証システムにおいて、
前記変換サーバが、
前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項6】
請求項２または３記載のワンタイムＩＤ認証システムにおいて、
前記ワンタイムＩＤ生成装置が、
一日を複数の時間帯に分けた際の、各時間帯用のワンタイムＩＤ生成用関数が格納された関数保持部と、
該関数保持部に格納されているワンタイムＩＤ生成用関数の内の、現在時刻を含む時間

帯用のワンタイムＩＤ生成用関数と、現在時刻と、ユーザＩＤとに基づいてワンタイムＩＤを生成するワンタイムＩＤ生成用演算手段とを備え、

前記変換サーバが、

一日を複数の時間帯に分けた際の、各時間帯用のユーザＩＤ算出用関数が格納された逆関数保持部と、

前記認証サーバから変換要求が送られてきたとき、前記逆関数保持部に保持されている各時間帯用のユーザＩＤ算出用関数の内の、現在時刻を含む時間帯用のユーザＩＤ算出用関数と、現在時刻と、前記変換要求中のワンタイムＩＤとに基づいてユーザＩＤを算出するユーザＩＤ算出用演算手段とを備えたことを特徴とするワンタイムＩＤ認証システム。

【請求項7】

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部と、

端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段と、

前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とする認証サーバ。

【請求項8】

認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とする変換サーバ。

【請求項9】

端末装置が、ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を認証サーバへ送信し、

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を有する前記認証サーバが、前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を変換サーバへ送信し、

前記変換サーバが、前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却し、

前記認証サーバが、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とすることを特徴とするワンタイムＩＤ認証方法。

【請求項10】

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えたコンピュータを、

端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段、

前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段として機能させるためのプログラム。

【請求項11】

コンピュータを、

認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】
【0001】
本発明は、ネットワークシステムにおける本人認証技術に関し、特に、ログオン毎に毎回異なるユーザＩＤ（ワンタイムＩＤ）を使用することにより、セキュリティレベルを高めた本人認証技術に関する。
【背景技術】
【0002】
ネットワークシステムにおける本人認証システムとしては、従来から種々のものが知られている。図１３は、従来最も一般的に利用されている本人認証システムの構成を示したブロック図である。同図を参照すると、本人認証システムは、認証サーバ１００と、ユーザが利用する端末装置２００とを含み、両者はインターネット，ＬＡＮなどのネットワーク３００を介して相互に接続されている。
【0003】
この図１３に示した本人認証システムでは、端末装置２００のユーザは、本人認証を行う場合、自身のユーザＩＤとパスワードとを含む認証要求を、端末装置２００から認証サーバ１００へ送信する。認証サーバ１００内の認証手段１０１は、送受信手段１０２を介して端末装置２００からの認証要求を受信すると、各ユーザのユーザＩＤとパスワードとが対応付けて登録されている認証情報記憶部１０３を参照し、本人認証を行う。即ち、認証要求中のユーザＩＤと対応付けて認証情報記憶部１０３に登録されているパスワードと、認証要求中のパスワードとを比較し、両者が一致する場合は、認証成功とし、両者が不一致の場合は、認証失敗とする。
【0004】
しかしながら、図１３に示した本人認証システムは、毎回同じユーザＩＤ及びパスワードを使用するため、セキュリティの点に問題がある。そこで、毎回異なるパスワード（ワンタイムパスワード）を使用するようにした、図１４に示すような本人認証システムが提案された（例えば、特許文献１参照）。
【0005】
図１４を参照すると、本人認証システムは、認証サーバ４００と、ユーザが利用する端末装置５００と、ワンタイムパスワード生成装置６００とを含み、認証サーバ４００と端末装置５００とは、インターネット，ＬＡＮ等のネットワーク７００を介して相互に接続されている。
【0006】
端末装置５００のユーザは、本人認証を行う場合、先ず、ワンタイムパスワード生成装置６００に、自身のユーザＩＤを入力する。これにより、ワンタイムパスワード生成装置６００は、入力されたユーザＩＤと現在時刻とに基づいてワンタイムパスワードを生成し、生成したワンタイムパスワードを表示部（図示せず）に表示する。尚、ワンタイムパスワード生成装置６００は、例えば、ワンタイムパスワード生成用のプログラムを組み込んだ携帯電話機などにより実現される。
【0007】
ユーザは、ワンタイムパスワードが表示されると、それと自身のユーザＩＤとを端末装置５００に入力する。これにより、端末装置５００は、上記ワンタイムパスワード及びユーザＩＤを含む認証要求を認証サーバ４００へ送信する。
【0008】
認証サーバ４００内の認証手段４０１は、送受信手段４０２を介して認証要求を受信すると、上記認証要求に含まれているユーザＩＤをワンタイムパスワード生成手段４０３に渡し、ワンタイムパスワードの生成を指示する。これにより、ワンタイムパスワード生成手段４０３は、時計４０４から現在時刻を入力し、この現在時刻と上記ユーザＩＤとに基づいてワンタイムパスワードを生成する。そして、生成したワンタイムパスワードと、認証要求に含まれていたワンタイムパスワードとを比較し、両者が一致する場合は、認証成功とし、両者が不一致の場合は、認証失敗とする。
【特許文献1】

特開２００２－２５９３４４号公報
【発明の開示】
【発明が解決しようとする課題】
【0009】
上述した特許文献１に記載されている本人認証システムによれば、毎回異なるパスワードが使用されるため、セキュリティを高いものにすることが可能になる。
【0010】
ところで、既に図１３に示すような認証サーバ１００を導入している機関においても、セキュリティの向上が望まれている。セキュリティを向上させるためには、図１４に示すようなワンタイムパスワードを利用して認証を行う本人認証システムを導入すればよいが、それでは、コストが非常に高くなってしまう。
【0011】
〔発明の目的〕
そこで、本発明の目的は、ユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を有し、ユーザＩＤとパスワードとに基づいた本人認証を行う既存の認証サーバを利用することにより、ワンタイムＩＤを用いたセキュリティの高い本人認証システムを経済的に構成できるようにすることにある。
【課題を解決するための手段】
【0012】
本発明にかかる第１のワンタイムＩＤ認証システムは、
端末装置と、ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えた認証サーバと、変換サーバとを含むワンタイムＩＤ認証システムであって、
前記端末装置が、
ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を前記認証サーバへ送信する構成を有し、
前記認証サーバが、
前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を前記変換サーバへ送信し、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする構成を有し、
前記変換サーバが、
前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却する構成を有することを特徴とする。
【0013】
本発明にかかる第２のワンタイムＩＤ認証システムは、第１のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザによって入力されたユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段を含むワンタイムＩＤ生成装置を備えたことを特徴とする。
【0014】
本発明にかかる第３のワンタイムＩＤ認証システムは、第１のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザのユーザＩＤが登録されているユーザＩＤ記憶部と、
該ユーザＩＤ記憶部に登録されているユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段とを含むワンタイムＩＤ生成装置を備えたことを特徴とする。
【0015】
本発明にかかる第４のワンタイムＩＤ認証システムは、第１～第３のワンタイムＩＤ認

証システムにおいて、
　前記認証サーバが、
　前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を前記変換サーバへ送信する変換要求手段と、
　前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とする。
【0016】
　本発明にかかる第５のワンタイムＩＤ認証システムは、第４のワンタイムＩＤ認証システムにおいて、
　前記変換サーバが、
　前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とする。
【0017】
　本発明にかかる第６のワンタイムＩＤ認証システムは、第２または第３のワンタイムＩＤ認証システムにおいて、
　前記ワンタイムＩＤ生成装置が、
　一日を複数の時間帯に分けた際の、各時間帯用のワンタイムＩＤ生成用関数が格納された関数保持部と、
　該関数保持部に格納されているワンタイムＩＤ生成用関数の内の、現在時刻を含む時間帯用のワンタイムＩＤ生成用関数と、現在時刻と、ユーザＩＤとに基づいてワンタイムＩＤを生成するワンタイムＩＤ生成用演算手段とを備え、
　前記変換サーバが、
　一日を複数の時間帯に分けた際の、各時間帯用のユーザＩＤ算出用関数が格納された逆関数保持部と、
　前記認証サーバから変換要求が送られてきたとき、前記逆関数保持部に保持されている各時間帯用のユーザＩＤ算出用関数の内の、現在時刻を含む時間帯用のユーザＩＤ算出用関数と、現在時刻と、前記変換要求中のワンタイムＩＤとに基づいてユーザＩＤを算出するユーザＩＤ算出用演算手段とを備えたことを特徴とする。
【0018】
　本発明にかかる認証サーバは、
　ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部と、
　端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段と、
　前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とする。
【0019】
　本発明にかかる変換サーバは、
　認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とする。
【0020】
　本発明にかかるワンタイムＩＤ認証方法は、
　端末装置が、ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を認証サーバへ送信し、

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を有する前記認証サーバが、前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を変換サーバへ送信し、

前記変換サーバが、前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却し、

前記認証サーバが、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とすることを特徴とする。

【0021】

本発明にかかる第１のプログラムは、

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えたコンピュータを、

端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段、

前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段として機能させる。

【0022】

本発明にかかる第２のプログラムは、

コンピュータを、

認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段として機能させる。

【0023】

〔作用〕

ユーザは、本人認証を行う場合、自身の端末装置から認証サーバへ認証要求を送る。この認証要求には、ユーザのユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、上記ユーザのパスワードとが含まれている。ワンタイムＩＤは、その生成時刻毎に、その値が異なるものになるので、セキュリティを高いものにすることができる。認証サーバは、認証要求を受信すると、認証要求中のワンタイムＩＤを含んだ変換要求を生成し、変換サーバに送る。変換サーバは、変換要求中のワンタイムＩＤと現在時刻とに基づいて、ユーザのユーザＩＤを算出し、算出したユーザＩＤを認証サーバに返却する。認証サーバは、返却されたユーザＩＤと、認証要求中のパスワードと、認証情報記憶部とを利用して本人認証を行う。

【発明の効果】

【0024】

本発明によれば、ワンタイムＩＤを利用したセキュリティの高い本人認証システムを経済的に構成することが可能になる。その理由は、端末装置から送られてきた認証要求に含まれているワンタイムＩＤをユーザＩＤに戻す変換サーバを設け、ユーザＩＤとパスワードとによる本人認証を行う既存の認証サーバをワンタイムＩＤを用いた本人認証に利用できるようにしたからである。

【発明を実施するための最良の形態】

【0025】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【0026】

〔第１の実施の形態の構成の説明〕

図１は本発明にかかるワンタイムＩＤ認証システムの第１の実施の形態の全体構成を示すブロック図である。同図を参照すると、本実施の形態のワンタイムＩＤ認証システムは、ユーザが利用するワンタイムＩＤ生成装置１０と、上記ユーザが利用する端末装置２０と、認証サーバ３０と、変換サーバ４０とを含み、端末装置１０，認証サーバ３０および変換サーバ４０は、インターネット，ＬＡＮ等のネットワーク５０を介して相互に接続されている。

【0027】

ワンタイムＩＤ生成装置１０は、ユーザが入力したユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、ユーザに提示する機能を有する。

【0028】

図２は、上記した機能を有するワンタイムＩＤ生成装置１０の構成例を示すブロック図であり、テンキー等の入力部１１と、ワンタイムＩＤ生成手段１２と、現在時刻を表示する時計１６と、ＬＣＤなどの表示部１７とを備えている。

【0029】

ワンタイムＩＤ生成手段１２は、関数保持部１３と、演算手段１４と、現在時刻入力手段１５を備えている。

【0030】

時刻入力手段１５は、時計１６から現在時刻を入力する機能を有する。尚、本実施の形態では、時刻入力手段１５は、時計１６が表示している時：分：秒の内、時：分のみを入力するものとする。即ち、時刻入力手段１５は、分単位の時刻を入力する。

【0031】

関数保持部１３には、ワンタイムＩＤを生成する際に利用する関数（ワンタイムＩＤ生成用関数）が格納されている。

【0032】

演算手段１４は、入力部１１から入力されたユーザＩＤと、時刻入力手段１５が入力した現在時刻とに対して、関数保持部１３に保持されているワンタイムＩＤ生成用関数に従った演算を行うことによりワンタイムＩＤを算出し、算出したワンタイムＩＤを表示部１７に表示する機能を有する。

【0033】

尚、ワンタイムＩＤ生成装置１０内のワンタイムＩＤ生成手段１２は、ＣＰＵ（コンピュータ）によって実現可能なものであり、コンピュータによって実現する場合は、例えば、次のようにする。コンピュータをワンタイムＩＤ生成手段１２として機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御することにより、自コンピュータ上に、ワンタイムＩＤ生成手段１２を実現する。また、ワンタイムＩＤ生成装置１０は、ＣＰＵを内蔵した携帯電話機を利用して実現することもできる。即ち、上記ＣＰＵをワンタイムＩＤ生成手段１２として機能させるためのプログラムを記録したディスクなどの記録媒体を用意し、ＣＰＵに上記プログラムを読み取らせる。ＣＰＵは、読み取ったプログラムに従って自身の動作を制御することにより、自ＣＰＵ上にワンタイムＩＤ生成手段を実現する。

【0034】

端末装置２０は、ワンタイムＩＤ及びパスワードを含んだ認証要求を認証サーバ３０へ送信する機能や、認証サーバ３０から送られてきた認証結果をユーザに提示する機能等を有する。

【0035】

図３は、上記した機能を有する端末装置２０の構成例を示すブロック図であり、送受信手段２１と、制御手段２２と、キーボード等の入力部２３と、ＬＣＤ等の表示部２４とを備えている。

【0036】

送受信手段２１は、ネットワーク５０を介してデータをやり取りする機能を有する。

【0037】
制御手段２２は、入力部２３から入力されたワンタイムＩＤ及びパスワードを含む認証要求を生成する機能や、生成した認証要求を送受信手段２１を介して認証サーバ３０へ送信する機能や、認証サーバ３０から送られてきた認証結果を表示部２４に表示する機能などを有する。
【0038】
尚、端末装置２０はパーソナルコンピュータ等のコンピュータによって実現可能なものであり、コンピュータによって実現する場合は、例えば、次のようにする。コンピュータを端末装置として機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御することにより、自コンピュータ上に、送受信手段２１、制御手段２２を実現する。
【0039】
認証サーバ３０は、端末装置２０からワンタイムＩＤ及びパスワードを含む認証要求が送られてきたとき、変換サーバ４０を利用して上記ワンタイムＩＤに対応するユーザＩＤを取得し、このユーザＩＤと上記認証要求中のパスワードとに基づいて認証を行う機能を有する。
【0040】
図４は、上述した機能を有する認証サーバ３０の構成例を示すブロック図であり、送受信手段３１と、認証手段３２と、認証情報記憶部３５とを備えている。
【0041】
認証情報記憶部３５には、図５に示すように、ユーザのユーザＩＤ，パスワード，アクセス権限，氏名，…が対応付けて登録されている。
【0042】
送受信手段３１は、ネットワーク５０を介してデータをやり取りする機能を有する。
【0043】
認証手段３２は、変換要求手段３３と、比較手段３４とを備えている。
【0044】
変換要求手段３３は、送受信手段３１を介して端末装置２０からの認証要求を受信したとき、認証要求中のワンタイムＩＤを含んだ変換要求を変換サーバ４０へ送信し、この変換要求に応答して変換サーバ４０から返却されたユーザＩＤを比較手段３４に渡す機能を有する。変換要求手段３３は、図１３に示した認証サーバ１００には備わっていない構成であり、既存の認証サーバ１００を利用して認証サーバ３０を実現する場合には、この構成を組み込む必要がある。
【0045】
比較手段３４は、変換要求手段３３から渡されたユーザＩＤに対応付けて認証情報記憶部３５に登録されているパスワードと、端末装置２０からの認証要求中のパスワードとを比較し、両者が一致する場合は、認証成功とし、両者が不一致の場合は、認証失敗とする機能を有する。比較手段３４は、図１３に示した認証サーバ１００に備わっている構成である。
【0046】
尚、認証サーバ３０は、コンピュータによって実現可能なものであり、コンピュータによって実現する場合は、例えば、次のようにする。コンピュータを認証サーバとして機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御し、自コンピュータ上に、送受信手段３１，認証手段３２を実現する。
【0047】
変換サーバ４０は、認証サーバ３０からワンタイムＩＤを含む変換要求が送られてきたとき、上記ワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、算出したユーザ

ＩＤを返却する機能を有する。
【0048】
図６は上記した機能を有する変換サーバ４０の構成例を示すブロック図であり、送受信手段４１と、変換手段４２と、現在時刻を表示する時計４６とを有する。
【0049】
送受信手段４１は、ネットワーク５０を介してデータを送受信する機能を有する。
【0050】
変換手段４２は、演算手段４３と、逆関数保持部４４と、時刻入力手段４５とを備えている。
【0051】
時刻入力手段４５は、時計４６から分単位の現在時刻を入力する機能を有する。
【0052】
逆関数保持部４４には、ワンタイムＩＤと現在時刻とからユーザＩＤを求めるための関数（ユーザＩＤ算出用関数）が格納されている。
【0053】
演算手段４３は、送受信手段４１を介して認証サーバ３０から送られてきた変換要求を受信したとき、それに含まれているワンタイムＩＤと、時刻入力手段４５が入力した分単位の現在時刻と、逆関数保持部４４に保持されているユーザＩＤ算出用関数とに基づいてユーザＩＤを算出し、算出したユーザＩＤを認証サーバ３０へ送信する機能を有する。
【0054】
尚、変換サーバ４０は、コンピュータによって実現可能なものであり、コンピュータによって実現する場合は、例えば次のようにする。コンピュータを変換サーバとして機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御することにより、自コンピュータ上に、送受信手段４１、変換手段４２を実現する。
【0055】
〔第１の実施の形態の動作の説明〕
次に、本実施の形態の動作について各図を参照して詳細に説明する。
【0056】
端末装置２０のユーザは、本人認証を行う場合、ワンタイムＩＤ生成装置１０を起動し、入力部１１から自身のユーザＩＤを入力する（図７のａ）。
【0057】
ワンタイムＩＤ生成装置１０内のワンタイムＩＤ生成手段１２は、起動されると、ユーザＩＤの入力待ち状態となり、ユーザによって入力部１１からユーザＩＤが入力されると、時刻入力手段１５を用いて時計１６から分単位の現在時刻を入力する（図８のステップＳ８１，Ｓ８２）。その後、演算手段１４が、関数保持部１３に格納されているワンタイムＩＤ生成用関数と、ユーザが入力したユーザＩＤと、時刻入力手段１５が入力した現在時刻とに基づいてワンタイムＩＤを生成する（ステップＳ８３）。ここで、ワンタイムＩＤ生成用関数としては、例えば、（ワンタイムＩＤ）＝（ユーザＩＤ）×（現在時刻）などの関数を採用することができる。その後、演算手段１４は、算出したワンタイムＩＤを表示部１７に表示する（ステップＳ８４）。
【0058】
ユーザは、表示部１７にワンタイムＩＤが表示されると、表示されたワンタイムＩＤとパスワードとを端末装置２０に入力する（図７のｂ，ｃ）。端末装置２０内の制御手段２２は、入力部２３からワンタイムＩＤ及びパスワードが入力されると、それらを含んだ認証要求を認証サーバ３０へ送信する（図７のｄ）。
【0059】
認証サーバ３０内の変換要求手段３３は、送受信手段３１を介して端末装置２０から送られてきた認証要求を受信すると、上記認証要求中のワンタイムＩＤを含んだ変換要求を

生成し、それを変換サーバ４０へ送信する（図９のステップＳ９１，Ｓ９２及び図７のｅ）。その後、変換要求手段３３は、変換結果（ユーザＩＤ）の返却待ち状態となる（ステップＳ９３）。

【0060】

一方、変換サーバ４０内の変換手段４２は、認証サーバ３０からの変換要求を送受信手段４１を介して受信すると、図１０のフローチャートに示すように、先ず時刻入力手段４５を使用して時計４６から分単位の現在時刻を入力する（ステップＳ１０１）。その後、演算手段４３が、逆関数保持部４４に保持されているユーザＩＤ算出用関数と、時刻入力手段４５が入力した分単位の現在時刻と、変換要求中のワンタイムＩＤに基づいてユーザＩＤを算出し、算出したユーザＩＤを認証サーバ３０へ返却する（ステップＳ１０２，Ｓ１０３及び図７のｆ）。ここで、逆関数保持部４４に保持されているユーザＩＤ算出用関数は、ワンタイムＩＤ生成装置１０内の関数保持部１３に保持されているワンタイムＩＤ生成用関数の逆関数であり、例えば、ワンタイムＩＤ生成用関数が、（ワンタイムＩＤ）＝（ユーザＩＤ）×（現在時刻）であれば、ユーザＩＤ算出用関数は、（ユーザＩＤ）＝（ワンタイムＩＤ）÷（現在時刻）となる。但し、関数保持部１３，逆関数保持部４４に保持されるワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数は、上記した例に限られるものではない。

【0061】

変換結果の返却待ち状態にある認証サーバ３０内の変換要求手段３３は、変換サーバ４０から送られてくる変換結果（ユーザＩＤ）を送受信手段３１を介して受信すると、それを比較手段３４に渡す。これにより、比較手段３４は、認証情報記憶部３５から、上記ユーザＩＤに対応付けて登録されているパスワードを取り出し、端末装置２０から送られてきた認証要求中のパスワードと比較する（図９のステップＳ９４）。そして、両者が一致する場合は、認証要求元の端末装置２０に認証成功を通知し（ステップＳ９５がＹＥＳ，Ｓ９６）、不一致の場合は、端末装置２０に認証失敗を通知する（ステップＳ９５がＮＯ，Ｓ９７及び図９のｇ）。尚、認証情報記憶部３５に該当するユーザＩＤが登録されていない場合も、認証失敗とする。

【0062】

端末装置２０内の制御手段２２は、送受信手段２１を介して認証結果（認証成功或いは認証失敗）を受信すると、それを表示部２４に表示する。認証成功が表示された場合、端末装置２０のユーザは、システムに対するアクセス権を獲得したことになり、システムにアクセスすることが可能になる。これに対して、認証失敗が表示された場合は、ユーザは、前述した操作を再度行う。

【0063】

尚、上述した実施の形態では、変換サーバ４０内の変換手段４２は、認証サーバ３０からの変換要求を受信したとき、変換要求中のワンタイムＩＤと、現在時刻とに基づいてユーザＩＤを１つだけ算出するようにしたが、現在時刻に対応するユーザＩＤと、現在時刻よりも１分前の時刻に対応するユーザＩＤとの２つのユーザＩＤを求め、それら２つのユーザＩＤを認証サーバ３０に返却するようにしても良い。そして、２つのユーザＩＤが返却された認証サーバ３０内の比較手段３４では、上記２つのユーザＩＤに対応付けて認証情報記憶部３５に登録されている２つのパスワードの内の何れか一方が、認証要求中のパスワードと一致していれば、認証成功と判定する。このようにすることにより、ユーザの操作時間（ワンタイムＩＤの生成時から、ユーザがワンタイムＩＤ及びパスワードを端末装置２０に入力するまでの時間）により、ワンタイムＩＤの生成時刻と、変換サーバ４０における変換要求の受信時刻とに差が生じた場合であっても、その差が１分以内であれば、認証成功とすることができる。

【0064】

また、上述した実施の形態では、関数保持部１３，逆関数保持部４４にそれぞれワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を１つずつ格納するようにしたが、複数のワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を格納しておき、時間帯に応じて使用す

る関数を変更するようにしても良い。このようにする場合は、例えば、１日を複数の時間帯に分け、各時間帯用のそれぞれ異なるワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を関数保持部１３，客関数保持部４４に登録しておく。ワンタイムＩＤ生成装置１０内の演算手段１４では、図８のステップＳ８３でワンタイムＩＤを生成する際、関数保持部１３に格納されている各時間帯のワンタイムＩＤ生成用関数の内の、現在時刻を含む時間帯用のワンタイムＩＤ生成用関数と、現在時刻と、ユーザＩＤとを使用してワンタイムＩＤを生成する。また、変換サーバ４０内の演算手段４３では、図１０のステップＳ１０２においてユーザＩＤを算出する際、逆関数保持部４４に格納されているユーザＩＤ算出用関数の内の、現在時刻を含む時間帯用のユーザＩＤ算出用関数と、現在時刻と、ワンタイムＩＤとからユーザＩＤを算出する。

【0065】

〔第１の実施の形態の効果〕

本実施の形態によれば、ワンタイムＩＤを利用したセキュリティの高い本人認証システムを経済的に構成することが可能になる。その理由は、端末装置２０から送られてきた認証要求に含まれているワンタイムＩＤをユーザＩＤに戻す変換サーバ４０を設けることにより、ユーザＩＤとパスワードとによる本人認証を行う既存の認証サーバ３０を、ワンタイムＩＤを用いた本人認証に利用できるようにしたからである。

【0066】

更に、本実施の形態によれば、セキュリティを極めて高いものにすることが可能になる。その理由は、時間毎に異なるワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を使用するようにしているからである。

【0067】

〔第２の実施の形態〕

次に、本発明にかかるワンタイムＩＤ認証システムの第２の実施の形態について説明する。本実施の形態のワンタイムＩＤ認証システムは、図１に示したワンタイムＩＤ認証システムにおいて、図２に示したワンタイムＩＤ生成装置１０の代わりに、図１１に示すワンタイムＩＤ生成装置１０ａを用いることにより実現される。

【0068】

本実施の形態で使用する図１１に示すワンタイムＩＤ生成装置１０ａは、ワンタイムＩＤ生成手段１２の代わりに、ワンタイムＩＤ生成手段１２ａを備えている点、およびユーザＩＤ保持部１９が追加されている点が図２に示したワンタイムＩＤ生成手段１２と相違している。

【0069】

ユーザＩＤ保持部１９には、端末装置２０のユーザのユーザＩＤが登録されている。

【0070】

ワンタイムＩＤ生成１２ａは、ユーザＩＤ保持部１９に格納されているユーザＩＤを入力するユーザＩＤ入力手段１８が追加されている点が、ワンタイムＩＤ生成手段１２と相違している。

【0071】

次に、本実施の形態の動作について説明する。尚、ワンタイムＩＤ生成装置１２ａ以外の動作は、第１の実施の形態と同様であるので、ここでは、ワンタイムＩＤ生成装置１２ａの動作についてのみ説明する。

【0072】

端末装置２０のユーザは、本人認証を行う場合、ワンタイムＩＤ生成装置１０ａを起動する。これにより、ワンタイムＩＤ生成装置１０ａ内のワンタイムＩＤ生成手段１２ａは、時刻入力手段１５を用いて時計１６から分単位の現在時刻を入力し、更に、ユーザＩＤ入力手段１８を用いてユーザＩＤ保持部１９からユーザＩＤを入力する（図１２のステップＳ１２１，Ｓ１２２）。その後、ワンタイムＩＤ生成手段１２ａ内の演算手段１４が、関数保持部１３に保持されているワンタイムＩＤ生成用関数と、時刻入力手段１５が入力した現在時刻と、ユーザＩＤ入力手段１８が入力したユーザＩＤとに基づいて、ワンタイ

ムＩＤを生成し、生成したワンタイムＩＤを表示部１７に表示する（ステップＳ１２３，Ｓ１２４）。

【0073】

〔第２の実施の形態の効果〕

本実施の形態によれば、第１の実施の形態の効果に加え、ユーザが行うワンタイムＩＤの生成操作を簡単なものとすることができる。その理由は、ワンタイムＩＤ生成装置１２ａが、ユーザＩＤが登録されたユーザＩＤ保持部１９を備えており、ユーザがワンタイムＩＤ生成時に、ユーザＩＤを入力する必要がないからである。

【産業上の利用可能性】

【0074】

高いセキュリティが求められる認証システムに利用することができる。

【図面の簡単な説明】

【0075】

【図1】本発明にかかるワンタイムＩＤ認証システムの第１の実施の形態の全体構成例を示すブロック図である。

【図2】ワンタイムＩＤ生成装置１０の構成例を示すブロック図である。

【図3】端末装置２０の構成例を示すブロック図である。

【図4】認証サーバ３０の構成例を示すブロック図である。

【図5】認証情報記憶部３５の内容例を示す図である。

【図6】変換サーバ４０の構成例を示す図である。

【図7】第１の実施の形態の動作を説明するための図である。

【図8】ワンタイムＩＤ生成装置１０の処理例を示すフローチャートである。

【図9】認証サーバ３０の処理例を示すフローチャートである。

【図10】変換サーバ４０の処理例を示すフローチャートである。

【図11】本発明にかかるワンタイムＩＤ認証システムの第２の実施の形態で使用するワンタイムＩＤ生成装置１０ａの構成例を示すブロック図である。

【図12】ワンタイムＩＤ生成装置１０ａの処理例を示すブロック図である。

【図13】従来のユーザＩＤとパスワードとを使用する本人認証システムの一例を示すブロック図である。

【図14】従来のユーザＩＤとワンタイムパスワードとを使用する本人認証システムの一例を示す図である。

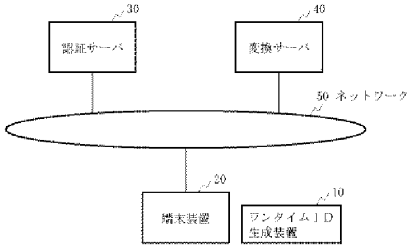
【符号の説明】

【0076】

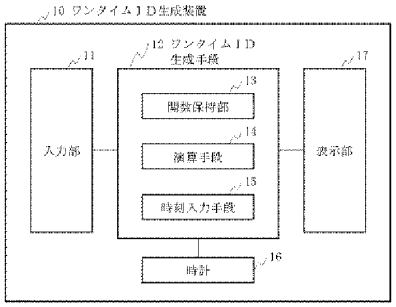
１０，１０ａ…ワンタイムＩＤ生成装置
１１…入力部
１２，１２ａ…ワンタイムＩＤ生成手段
１３…関数保持部
１４…演算手段
１５…時刻入力手段
１６…時計
１７…表示部
１８…ユーザＩＤ入力手段
１９…ユーザＩＤ保持部
２０…端末装置
２１…送受信手段
２２…制御手段
２３…入力部
２４…表示部
３０…認証サーバ
３１…送受信手段

３２…認証手段
３３…変換要求手段
３４…比較手段
３５…認証情報記憶部
４０…変換サーバ
４１…送受信手段
４２…変換手段
４３…演算手段
４４…逆関数保持部
４５…時刻入力手段
４６…時計
５０…ネットワーク

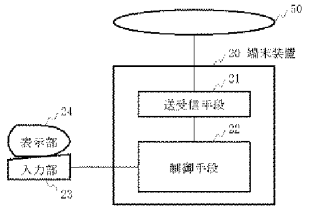
【図1】



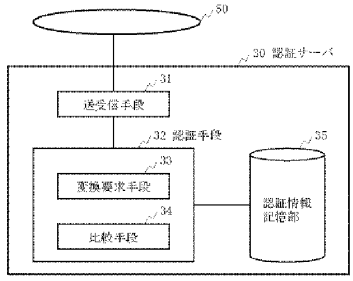
【図2】



【図3】



【図4】



【図5】

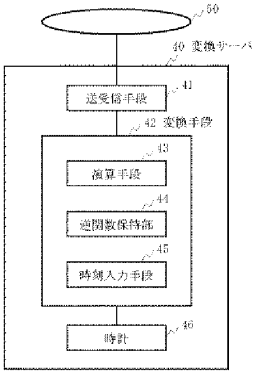
【図５】

35 認証情報記憶部

ユーザＩＤ	パスワード	アクセス権限	氏名	・・・
ｉｄ１	ｐ１	ａ１	ｘｘｘ	・・・
ｉｄ２	ｐ２	ａ２	ｙｙｙ	・・・
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

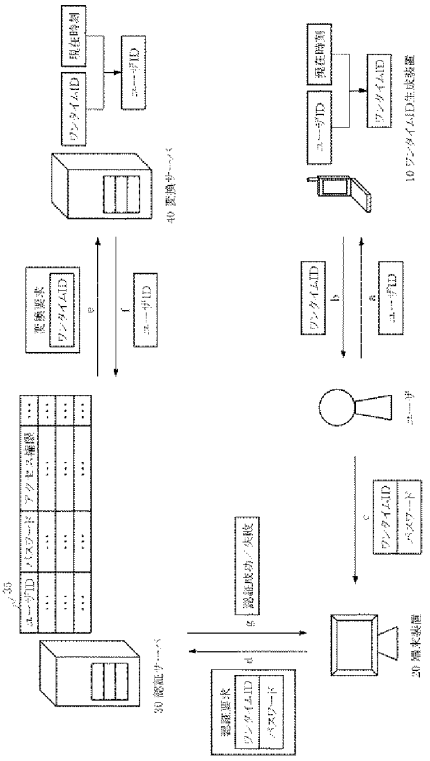
【図6】

【図６】



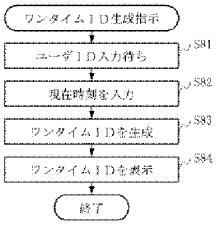
【図7】

【図７】



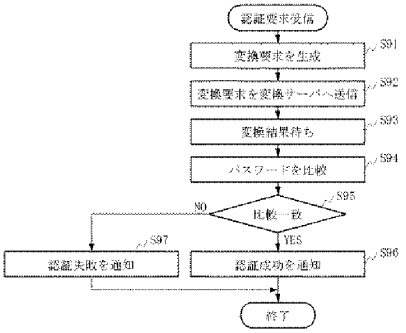
【図8】

【図８】



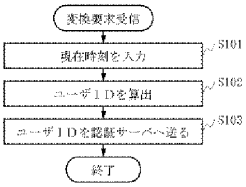
【図9】

【図９】



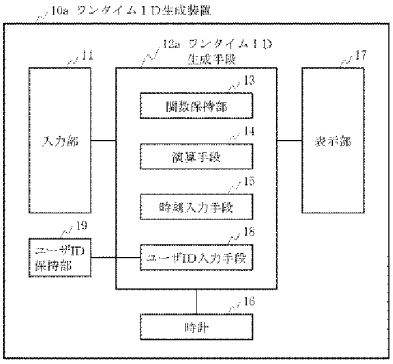
【図10】

【図１０】



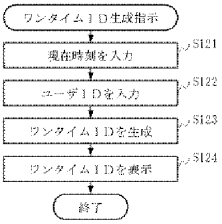
【図11】

【図１１】



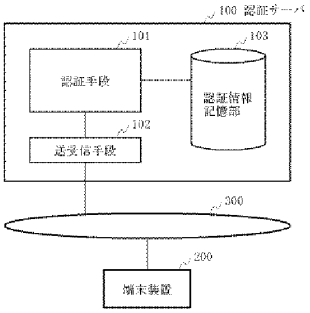
【図12】

【図１２】



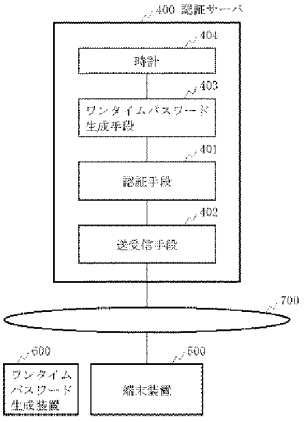
【図13】

【図１３】



【図14】

【図１４】



Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Air download method of increment business of user identifying module

CN 1345154 A

Publication number	CN1345154 A
Publication type	Application
Application number	CN 01134713
Publication date	Apr 17, 2002
Filing date	Nov 8, 2001
Priority date	Nov 8, 2001
Inventors	赵文军, 姜旻, 王志红
Applicant	大唐微电子技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (15), Classifications (2), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invnetion discloses a method used to download on-air a value added service to subscriber identification module (SIM) in digital mobile phone. The STK and application program is directly downloaded to subscriber's SIM card by using CLASS 2 SIM-specific message format. The STK menu data is provided for SIM card to add new service, and the application program is used for realizing STK application. The invented method takes full advantage of existing software and hardware facility, making user apply for new service without need to replace STK card, also without need going to appointed business hall.

DESCRIPTION translated from Chinese

VAS Subscriber Identity Module aerial download methods

Field of the Invention This invention relates to a digital mobile communication system of the new technology, particularly, relates to a value-added services digital mobile telephone SIM (Subscriber Identity Module) card over the air method, the technology can move expanding communications, mobile banking, mobile securities, and mobile e-commerce and many other value-added services in mobile phones widely applied, is a digital mobile phone and record carrier with conductive marks, printed circuits or semiconductor circuit elements (such as credit cards or identification Card) Technical Field.

Due to limited STK technology can meet the different requirements of various customers personalized to meet the diverse needs of people on the information queries, so that the data service downsizing, personal computer and mobile from PC to mobile phones, but also for commercial advertising bring success and more market opportunities, so the market has achieved some success. Currently around STK ISP has been able to provide weather forecasts, news, check train schedules, aircraft flight information, stock inquiries and other aspects of business, and more value-added services are around STK gradually opened. However, the contradiction between the limited capacity of the rapidly growing business needs and unlimited scope for each SIM card between them has become increasingly prominent.

At present, various value-added services are usually one-time use of STK technology advance to write a variety of business needs of the user STK SIM card, if the user wants to change or add four new value-added services to a fixed place of business must By setting hall where computer and Internet connection of 2 and front terminal (POS machines) 3, to download the server from a new business STK download relevant business data and procedures (see Figure 1), or simply replace another Zhang STK cards. Due to the limited number of such pre-terminal (POS machines), and are usually placed in a fixed location - Fixed mobile phone operating room, so the user can only to a fixed location can only add value to the business of deletions, modifications tedious the process is bound to give it a lot of trouble, will inevitably affect the user to use various STK business initiative, which adversely affect competition in the market for operators.

CLAIMS (5) translated from Chinese

1. A digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method, characterized in that: the method is implemented by STK menu data and the SIM card provided to add new services to the STK application application which together with two short messages (CLASS 2SIM-specific message) in the form of downloaded to the user's SIM card achieved.

The digital mobile telephone subscriber identification module (SIM card) of the value-added services over the air method according to claim 1, characterized in that: the method comprises at least the following steps: (1) by an ordinary user short message service provider, namely STK new business download server sends "New Business Download List" application requesting service providers to provide a list of available download services; (2) STK new business download server after receipt of the application, The new services STK download list with two short messages sent to the application user; (3) the application user to download a list of these new services based on STK received, you can choose to add one of them STK business, but also can choose The new service is added STK position, and after a good choice, the information is sent back to the server to download STK new business; (4) STK new business download server after receiving the application needs of users of information, related processing and then through the secondary short message data and procedures that apply STK business users need to download to the user to specify the location of the SIM card, to complete the download process STK business.

The digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method according to claim 1, characterized in that: the method may also include the steps of: in the SIM card STK menu Preset Multiple content is empty menu, the user can be classified add in these menus change according to personal preferences menu name and download business.

4. According to the digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method according to claim 1, characterized in that: the method *may further*

The present invention is a digital mobile telephone in the subscriber identification module (SIM card) of the value-added services over the air method is implemented as follows: it is to add new services through the menu to the SIM card STK menu data and applications to achieve STK together with two applications both short message (CLASS 2SIM-specific message) in the form of downloaded to the user's SIM card achieved.

The method includes at least the following steps: (1) a short message to the user through common service providers, namely STK new business download server sends "New Business Download List" application, request service providers to provide a list of services available for download; (2) STK new business download server after receiving the application, the new business will STK download list with a secondary message is sent to the application user; (3) the application user to download a list of new services based on STK received above, You can choose to add one of them STK business, but you can also choose to add the location of the new STK business, and after a good choice, the information is sent back to the server to download STK new business; (4) STK new business download servers Upon receipt of the application needs of users of information, related processing, and then through the secondary short message data and procedures that apply STK business users need to download to the user to specify the location of the SIM card, to complete STK Business download process.

The method may also include the following steps: pre more content in the SIM card STK menu is empty menu, the user can be classified add in these menus change according to personal preferences menu name and download business.

The method may further comprise the steps of: STK business has been downloaded, the user can choose to delete to make room to download other new business.

The secondary display is a short message on the screen is not in ME, as the data is transferred directly and transparently to the SIM card storage, data processing; and only STK card supports sending and receiving short messages of this kind.

Using the method of the invention, a mobile communications company and value-added business service providers can leverage existing software and hardware devices, without adding more investment, as long as the development of the corresponding supporting software to download the application and make the business has been expanding . And users do not have to replace the STK card, do not have to specify the operating room to use the pre-terminal (POS machines) download new business, you can freely, easily and flexibly select the STK services they need. For example, users can be based on individual needs and preferences anytime, anywhere-air download STK business; and its existing SIM card STK services, users can also choose to delete, to free up more space to download new business. Thus, to some extent, also solves the contradiction between limited and unlimited capacity needs of users between SIM card and can save users the associated costs. Users can also according to their habits and preferences, will assign various STK business into different groups, in order to facilitate their use; moreover, the group name can also be modified by the user. In summary, the present invention has a fairly optimistic about market prospects.

Figure 2 is a digital mobile telephone of the present invention in VAS STK SIM card over the air network system connection diagram.

Figure 3 is a realization of the method of the present invention is a digital mobile telephone in VAS STK SIM card over the air. Fig.

STK menu both an application STK application implemented method of the present invention is a digital mobile telephone in the subscriber identification module (SIM card) of value-added services over the air is to add new services provided by the SIM card to be implemented together with the data and two short message (CLASS 2) in the form of downloaded to the user's SIM card achieved.

See Fig. 3 a schematic view of the operation: (1) First, by the user by using an ordinary short message to their mobile phone via the GSM network service provider, i.e. STK "new business download list" application download server sends a new service; (2) Then, the network operator via SMS center its digital mobile telephone exchange received the application user and transparently passed to the new business STK ISP download server, and the server to download the new business after receipt of the application, then by SMSC digital mobile telephone exchange will STK new business list with a secondary message is sent to the application user; (3) the application of new business users based on the above list STK received, you can choose to add one of them STK business , but you can also choose to add a new STK business location; and a good selection, and then together with the relevant information needs to be sent back to the server to download STK new business; (4) STK new business application download server receives the user's Related demand information after appropriate treatment, then the original data and programs through the network link to the secondary short message to the application desired to download user STK service to the subscriber's SIM card, i.e. complete business STK download process.

comprise the steps of: STK downloaded service, The user can choose to delete to make room to download other new business.

The digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method according to claim 1, wherein: said second short message is a screen display is not on ME directly as the data is transferred transparently to the SIM card storage, data processing; and only STK card supports sending and receiving short messages of this kind.

Here the secondary short message different from ordinary short message, is displayed on the screen is an ME is not directly transmitted to the SIM card as a data storage, data processing; STK card supports only send and receive short messages of this kind.

In addition, the method of the present invention can also be preset in the SIM card STK menu is empty multiple menus, the user can choose according to your preferences and change the menu name and downloadable business class to add in these menu section . For already downloaded STK services, users can also choose to delete to make room to download other new business.

Between devices constituting a network system of the present invention has a SIM card in a digital mobile telephone set, GSM networks and new services STK downloading server simulation experiment, the effect of the test was successful, to achieve the object of the invention.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100334914C *	Dec 21, 2004	Aug 29, 2007	乐金电子(中国)研究开发中心有限公司	Device and method for maintaining applied information consistency of portable terminal
CN100334917C *	Dec 31, 2004	Aug 29, 2007	大唐微电子技术有限公司	A method and system for compatibility test of subscriber identification module tool kit card
CN100405864C	Aug 4, 2006	Jul 23, 2008	浙江省电信有限公司	Implementing method for air loading technology based on PAS network
CN100450279C	Mar 22, 2005	Jan 7, 2009	华为技术有限公司	Method for realizing user data management based on wireless system
CN100452893C	Aug 4, 2006	Jan 14, 2009	凤凰微电子（中国）有限公司	System and method for realizing value-added business based on user identification module
CN100454932C	Jun 8, 2004	Jan 21, 2009	雅斯拓（北京）智能卡科技有限公司	Method for realizing short-message memory on expanded SIM card
CN100459737C	Feb 25, 2005	Feb 4, 2009	北京握奇数据系统有限公司	Information transmitting/receiving method and system
CN101217728B	Dec 29, 2007	Jan 30, 2013	北京握奇数据系统有限公司	A blank card for wireless card writing, wireless card writing server and wireless card writing method
CN101257682B	Mar 6, 2008	Dec 15, 2010	上海展趣网络科技有限公司; 上海长丰智能卡有限公司	External control method for SIM card
CN101453714B	Dec 3, 2007	Mar 27, 2013	中兴通讯股份有限公司	Method and system for application download of near-field communication mobile payment system
CN101557580B	May 15, 2009	Oct 26, 2011	中兴通讯股份有限公司	Data processing method and system
US7734707	Aug 1, 2006	Jun 8, 2010	Beijing Watch Data System Co., Ltd.	Don't disturb service management system and implementation thereof
US8255706	Dec 7, 2007	Aug 28, 2012	Beijing Watch Data System Co., Ltd.	Dual usage smart card of CPU and logical encryption and its data synchronization method
US8266619	Jan 25, 2007	Sep 11, 2012	Beijing Watch Data System Co., Ltd.	Embedded operating system architecture for smart card
WO2012152031A1 *	Dec 26, 2011	Nov 15, 2012	Zte Corporation	Wireless communication terminal and its software upgrade method

* Cited by examiner

CLASSIFICATIONS

International Classification	H04M1/66, H04M3/42

LEGAL EVENTS

Date	Code	Event	Description
Feb 20, 2002	C10	Request of examination as to substance	
Apr 17, 2002	C06	Publication	
Sep 8, 2004	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

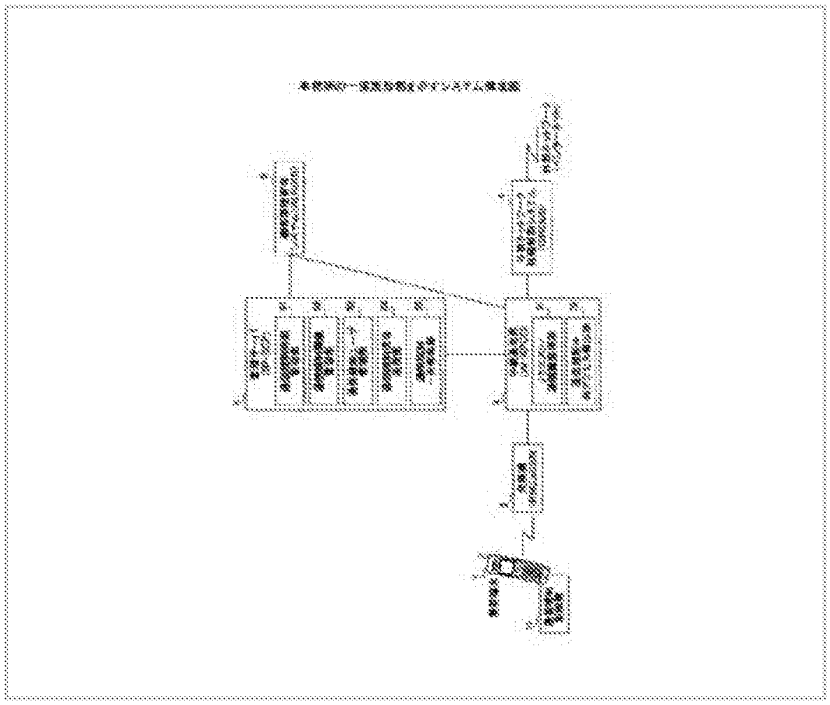
(11)Publication number	2006-197137
(43)Date of publication of application	27.07.2006
(51)Int.Cl.	H04M 3/42 (2006.01) H04M 11/00 (2006.01) H04M 15/00 (2006.01) H04Q 7/38 (2006.01)
(21)Application number	2005-005684
(22)Date of filing	12.01.2005
(71)Applicant	NTT DOCOMO INC
(72)Inventor	TANIGUCHI HIROTO ASANO YOSHITOKI

(54)DATA COMMUNICATION REGULATING METHOD OF FIXED RATE SYSTEM USER, DATA COMMUNICATION REGULATION CONTROLLER AND PORTABLE TERMINAL

(57)Abstract

PROBLEM TO BE SOLVED: To provide a fixed rate system user communication regulating method for finitely applying communication regulation to a specific user, and for applying firm communication regulation which can not be easily released at a portable terminal side at the time of defining data communication such as packet communication as an object.

SOLUTION: This data communication regulating method comprises a process for monitoring the data communication status of a fixed rate system user, and for judging whether or not the number of times of request or communication quantity within a predetermined period exceed a predetermined threshold, a process for setting the fixed rate system user as the object of communication regulation when it is judged that they exceed the predetermined threshold and a process for transmitting a communication regulation signal including the information of a communication regulation time to the portable terminal of the fixed rate system user when access is performed again from the fixed rate system user set as the object of communication regulation. The data communication of the portable terminal of the fixed rate system user is put in an inhibited status across the communication regulation time.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-197137
(P2006-197137A)
(43)公開日　平成18年7月27日(2006.7.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04M 3/42	(2006.01)	H04M	3/42	A	5K024
H04M 11/00	(2006.01)	H04M	11/00	303	5K025
H04M 15/00	(2006.01)	H04M	15/00	G	5K067
H04Q 7/38	(2006.01)	H04B	7/26	109K	5K101

審査請求 未請求　請求項の数 9　ＯＬ　（全 9 頁）

(21)出願番号　特願2005-5684(P2005-5684)
(22)出願日　平成17年1月12日(2005.1.12)

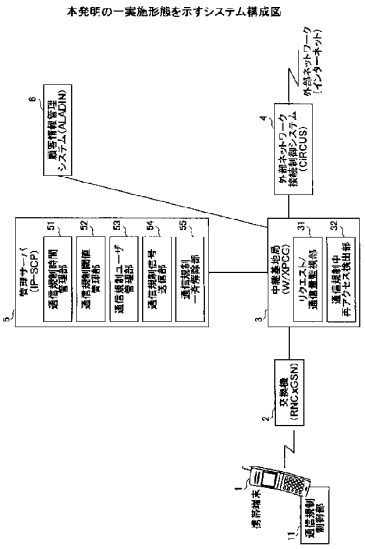
(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　谷口　博人
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　浅野　義時
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

Ｆターム(参考)　5K024 AA61 AA63 CC11 FF03
5K025 AA05 AA08 BB01 CC01 JJ02
KK06

最終頁に続く

(54)【発明の名称】定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末

(57)【要約】
【課題】　パケット通信等のデータ通信を対象とし、特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末側で簡単に通信規制を解除することのできない強固な規制をかけることができる定額制ユーザ通信規制方法等を提供する。
【解決手段】　定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する工程と、上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する工程と、上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する工程とを備え、上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にする。
【選択図】　図３



【特許請求の範囲】
【請求項１】
定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する工程と、
上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する工程と、
上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する工程とを備え、
上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にすることを特徴とする定額制ユーザのデータ通信規制方法。
【請求項２】
上記閾値および上記通信規制時間は基地局毎に設定されることを特徴とする請求項１に記載の定額制ユーザのデータ通信規制方法。
【請求項３】
上記通信規制信号はショートメッセージサービスにより送信されることを特徴とする請求項１または２のいずれか一項に記載の定額制ユーザのデータ通信規制方法。
【請求項４】
通信規制の一斉解除時に、通信規制解除信号を通信規制の対象となっている定額制ユーザの携帯端末に送信する工程を備え、
上記定額制ユーザの携帯端末のデータ通信を通常使用可能状態にすることを特徴とする請求項１乃至３のいずれか一項に記載の定額制ユーザのデータ通信規制方法。
【請求項５】
上記通信規制解除信号はショートメッセージサービスにより送信されることを特徴とする請求項４に記載の定額制ユーザのデータ通信規制方法。
【請求項６】
定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する手段と、
上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する手段と、
上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する手段とを備え、
上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にすることを特徴とするデータ通信規制制御装置。
【請求項７】
基地局側から通信規制時間の情報を含む通信規制信号を受信した場合に、データ通信を上記通信規制時間にわたって禁止状態にする手段を備えたことを特徴とする携帯端末。
【請求項８】
上記通信規制信号を受信した場合に、通信規制中である旨を画面に表示する手段を備えたことを特徴とする請求項７に記載の携帯端末。
【請求項９】
基地局側から通信規制解除信号を受信した場合に、データ通信を通常使用可能状態にする手段を備えたことを特徴とする請求項７または８のいずれか一項に記載の携帯端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末に関する。
【背景技術】

【０００２】
昨今、携帯電話等の携帯端末によるインターネットアクセスの利用が拡大しており、ユーザの通信料（パケット料金）の負担を軽減すべく、「定額制」と呼ばれる、通信量にかかわらず料金を一定としたサービスが導入されるに至っている。しかし一方で通信料が一定になるためデータ通信の過剰利用が懸念されるようになった。
【０００３】
そこで定額制サービスに於いては、特定の定額制ユーザによる必要以上のデータ通信リソースの独占を禁止すべく、過度のアクセスを行う特定のユーザに対しては通信事業者側で強制的に通信を切断することが契約上において一般に許容されている。一方で、通信量に応じて課金される「従量制」のユーザに対しては、その通信品質を保証する義務があり、定額制ユーザの通信を犠牲にしても従量制ユーザの通信を保証する必要がある。
【０００４】
ただしこのデータ通信規制は、あくまでもデータ通信と音声通信を同時に規制するのではなく、データ通信に特化した通信規制方法である。従って、通信規制を受けているユーザも、音声通信に関しては通常通り実施することが可能である。
【０００５】
図１は従来における通信規制の概念図であり、通常の利用にあっては携帯端末１０１から交換機１０２および中継基地局１０３を介してインターネット等の外部ネットワークにアクセスが行われるものであるが、中継基地局１０３において携帯端末１０１から過度のアクセスを検出した場合、携帯端末１０１から交換機１０２を介して中継基地局１０３に与えられるアクセス要求（リクエスト）を中継基地局１０３において許否することで通信規制を行うようにしていた。
【０００６】
一方、従来から各種通信における輻輳時の通信規制方法については様々な技術が開示されている（例えば、特許文献１を参照。）。特許文献１には、基地局が無線ゾーンの輻輳状態を常に監視し、輻輳レベルを算出して輻輳情報として移動端末に通知し、輻輳レベルに応じて移動端末の発信規制を行う技術が開示されている。
【特許文献１】特開２００１－７８２６０号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
図１に示した従来の通信規制方法では、通信規制により中継基地局１０３後段の通信リソースの独占は防止することができるが、携帯端末１０１から繰り返し行われるリクエスト（外部ネットワークに接続できないことで行われるリクエストのリトライ）が全て交換機１０２を経由することとなり、交換機１０２の負荷を低減することができないという問題があった。
【０００８】
一方、特許文献１に記載される技術は、無線ゾーンの輻輳状態に応じて多くのユーザに対して一律に規制をかけるものであり、定額制ユーザの中でも過度なアクセスを行う特定のユーザだけを対象とした規制を行えるものではない。また、特許文献１に記載される技術はパケット通信等のデータ通信に特化したものではない。
【０００９】
本発明は上記の従来の問題点に鑑み提案されたものであり、その目的とするところは、パケット通信等のデータ通信を対象とし、特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末側で簡単に通信規制を解除することのできない強固な規制をかけることができる定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末を提供することにある。
【課題を解決するための手段】
【００１０】
上記の課題を解決するため、本発明にあっては、請求項１に記載されるように、定額制

ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する工程と、上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する工程と、上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する工程とを備え、上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にする定額制ユーザ通信規制方法を要旨としている。

【００１１】

また、請求項２に記載されるように、上記閾値および上記通信規制時間は基地局毎に設定されるものとすることができる。

【００１２】

また、請求項３に記載されるように、上記通信規制信号はショートメッセージサービスにより送信されるものとすることができる。

【００１３】

また、請求項４に記載されるように、通信規制の一斉解除時に、通信規制解除信号を通信規制の対象となっている定額制ユーザの携帯端末に送信する工程を備え、上記定額制ユーザの携帯端末のデータ通信を通常使用可能状態にすることができる。

【００１４】

また、請求項５に記載されるように、上記通信規制解除信号はショートメッセージサービスにより送信されるものとすることができる。

【００１５】

また、請求項６に記載されるように、定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する手段と、上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する手段と、上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する手段とを備え、上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にする通信規制制御装置として構成することができる。

【００１６】

また、請求項７に記載されるように、基地局側から通信規制時間の情報を含む通信規制信号を受信した場合に、データ通信を上記通信規制時間にわたって禁止状態にする手段を備えた携帯端末として構成することができる。

【００１７】

また、請求項８に記載されるように、上記通信規制信号を受信した場合に、通信規制中である旨を画面に表示する手段を備えるようにすることができる。

【００１８】

また、請求項９に記載されるように、基地局側から通信規制解除信号を受信した場合に、データ通信を通常使用可能状態にする手段を備えるようにすることができる。

【発明の効果】

【００１９】

本発明の定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末にあっては、パケット通信等のデータ通信を対象とし、特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末側で簡単に通信規制を解除することのできない強固な規制をかけることができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の好適な実施形態について説明する。

【００２１】

図２は本発明における通信規制の概念図である。図２において、通常の利用にあっては定額制ユーザの所持する携帯電話のごとき携帯端末１から交換機２および中継基地局３を

介してインターネット等の外部ネットワークにアクセスが行われるものであるが、中継基地局３において定額制ユーザの携帯端末１から過度のアクセスを検出した場合、その定額制ユーザを通信規制の対象に設定し、再び同じユーザからアクセスが行われた場合、通信規制時間の情報を含む通信規制信号を定額制ユーザの携帯端末１に交換機２を介して送信する。これにより携帯端末１は指定された通信規制時間にわたり外部ネットワークへのアクセスのためのデータ通信が禁止状態となる。従って、通信規制時間により規定された期間は携帯端末１から交換機２にリクエストが発生することがなくなり、交換機２の負荷を有効に低減させることができる。

【００２２】

図３は本発明の一実施形態を示すシステム構成図である。図３において、携帯端末１には、通常の音声通話、データ通信等の機能の他に、基地局側から通信規制時間の情報を含む通信規制信号を受信した場合に、データ通信を指定された通信規制時間にわたって禁止状態にするとともに、通信規制中である旨を画面に表示する等の処理を行う通信規制制御部１１が設けられている。なお、通信規制制御部１１は主としてソフトウェア（コンピュータプログラム）によって実現される。

【００２３】

一方、基地局側の構成として、ＲＮＣ(Radio Network Controller)、ｘＧＳＮ(GPRS Support Node, GPRS: General Packet Radio Service)等の交換機２と、Ｗ／ＸＰＣＧ(Wireless/eXtended wireless Protocol Conversion Gateway)等の中継基地局３と、ＣｉＲＣＵＳ(treasure Casket of i-mode（登録商標） service, high Reliability platform for CUStomer)等の外部ネットワーク接続制御システム４と、ＩＰ－ＳＣＰ(IP-based Service Control Point)等の管理サーバ５と、ＡＬＡＤＩＮ(ALl Around DoCoMo INformation system)等の顧客情報管理システム６とが設けられている。

【００２４】

中継基地局３には、通常の中継機能の他に、定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断し、閾値を超えた場合に管理サーバ５に通知を行うリクエスト／通信量監視部３１と、通信規制対象に設定された定額制ユーザから再びアクセスが行われたことを検出して管理サーバ５に通知を行う通信規制中再アクセス検出部３２とを備えている。

【００２５】

管理サーバ５には、中継基地局３の存在するエリアのデータ通信の輻輳状態に応じて通信規制時間を個別に設定管理する通信規制時間管理部５１と、同じく中継基地局３の存在するエリアのデータ通信の輻輳状態に応じて、通信規制の対象とすべき定額制ユーザのリクエスト回数およびもしくは通信量の超過を判断する閾値を個別に設定管理する通信規制閾値管理部５２と、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたと判断された場合にその定額制ユーザを通信規制対象に設定し、中継基地局３におけるその定額制ユーザの通信を規制する通信規制ユーザ管理部５３と、通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号をその定額制ユーザの携帯端末１に送信する通信規制信号送信部５４と、災害発生時等に、通信規制を一斉解除すべく、通信規制解除信号を通信規制の対象となっている定額制ユーザの携帯端末１に送信する通信規制一斉解除部５５とを備えている。

【００２６】

図４は上記の実施形態の動作例を示すシーケンス図であり、以下、図４に沿って上記の実施形態の動作を説明する。

【００２７】

先ず、通常の利用にあっては、定額制ユーザの所持する携帯端末１から交換機２、中継基地局３、外部ネットワーク接続制御システム４を介してインターネット等の外部ネットワークにアクセスが行われる（ステップＳ１～Ｓ８）。

【００２８】

ここで、中継基地局３はリクエスト／通信量監視部３１により定額制ユーザの携帯端末

１の通信状態を監視している。なお、携帯端末１のユーザが定額制ユーザであるかどうかは、顧客情報管理システム６から管理サーバ５を介して、あるいは、顧客情報管理システム６から直接に、契約情報を取得することで判断が可能である。また、リクエスト回数および通信量の超過を判断する閾値は、予め管理サーバ５から通知される。

【００２９】

そして、定額制ユーザの携帯端末１による所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えた場合、中継基地局３のリクエスト／通信量監視部３１は管理サーバ５に対して閾値の超過を通知する（ステップＳ９）。

【００３０】

管理サーバ５では、中継基地局３から特定の定額制ユーザのリクエスト回数およびもしくは通信量の超過の通知を受けると、その定額制ユーザを通信規制対象に設定するとともに（ステップＳ１０）、中継基地局３に対してその定額制ユーザの通信を規制するよう通知を行う（ステップＳ１１）。中継基地局３では、以後、その定額制ユーザの通信規制が解除されるまでデータ通信の中継を行わない。

【００３１】

次いで、通信規制の対象となった定額制ユーザの携帯端末１から交換機２を介して中継基地局３に再びアクセスがあると（ステップＳ１２、Ｓ１３）、中継基地局３の通信規制中再アクセス検出部３２はその再アクセスを検出し、管理サーバ５に通知する（ステップＳ１４）。

【００３２】

再アクセスの通知を受けた管理サーバ５では、通信規制信号送信部５４により、通信規制対象に設定された定額制ユーザの携帯端末１に対し、通信規制時間管理部５１で管理される通信規制時間の情報を含む通信規制信号を、例えばＳＭＳ(Short Message Service)の機能により送信する（ステップＳ１５～Ｓ１７）。

【００３３】

通信規制信号を受信した携帯端末１は、通信規制制御部１１によりデータ通信の機能を通信規制時間で指定された時間にわたって禁止状態にするとともに（ステップＳ１８）、例えば図５に示すような「規制中のためしばらくたってからご利用ください」といったメッセージを画面に表示する。通信規制時間は管理サーバ５において中継基地局３の存在するエリアのデータ通信の輻輳状態に応じて設定管理されるものであり、例えば、ユーザの多い繁華街では長く設定される。リクエスト回数および通信量の超過を判断する閾値は、ユーザの多い繁華街では低めに設定される。

【００３４】

データ通信が禁止状態となっている期間において、携帯端末１からは通常では外部ネットワークへのアクセスは行えないが、プログラムをリセットする等により強引に通信規制を解除した場合であっても、中継基地局３においてそのユーザの中継が許否されるため、アクセスを行うことはできない。通信規制時間が終了すると、携帯端末１の通信規制制御部１１はデータ通信の機能を通常使用可能状態に復帰させる。

【００３５】

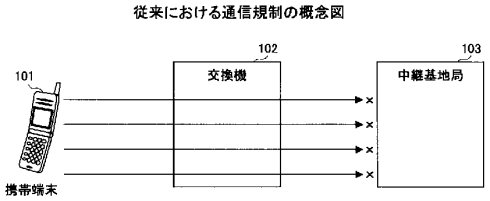
一方、災害発生時等において広くデータ通信を許容する必要がある場合、管理サーバ５は通信規制一斉解除部５５により通信規制を一斉解除し（ステップＳ１９）、通信規制ユーザ管理部５３における規制対象を削除するとともに、その時点で通信規制の対象となっている定額制ユーザの携帯端末１に対して中継基地局３を介してＳＭＳ等により通信規制解除信号を送信する（ステップＳ２０～Ｓ２２）。

【００３６】

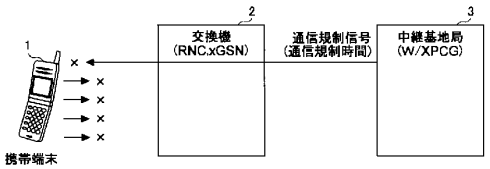
通信規制解除信号を受信した中継基地局３は定額制ユーザの規制を解除するとともに、同じく通信規制解除信号を受信した携帯端末１は、通信規制制御部１１によりデータ通信を通常使用可能状態に復帰させる（ステップＳ２３）。これにより携帯端末１は交換機２、中継基地局３、外部ネットワーク接続制御システム４を介した外部ネットワークへのアクセスが可能となる。

【００３７】
このように、パケット通信等のデータ通信を対象として、リクエスト、データ通信量の多い特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末１側で簡単に通信規制を解除することのできない強固な規制をかけることができる。また、災害発生時等における通信規制の解除を適切に行うことができる。
【００３８】
以上、本発明の好適な実施の形態により本発明を説明した。ここでは特定の具体例を示して本発明を説明したが、特許請求の範囲に定義された本発明の広範な趣旨および範囲から逸脱することなく、これら具体例に様々な修正および変更を加えることができることは明らかである。すなわち、具体例の詳細および添付の図面により本発明が限定されるものと解釈してはならない。
【図面の簡単な説明】
【００３９】
【図１】従来における通信規制の概念図である。
【図２】本発明における通信規制の概念図である。
【図３】本発明の一実施形態を示すシステム構成図である。
【図４】実施形態の動作例を示すシーケンス図である。
【図５】携帯端末における表示画面の例を示す図である。
【符号の説明】
【００４０】
１　携帯端末
１１　通信規制制御部
２　交換機
３　中継基地局
３１　リクエスト／通信量監視部
３２　通信規制中再アクセス検出部
４　外部ネットワーク接続制御システム
５　管理サーバ
５１　通信規制時間管理部
５２　通信規制閾値管理部
５３　通信規制ユーザ管理部
５４　通信規制信号送信部
５５　通信規制一斉解除部
６　顧客情報管理システム

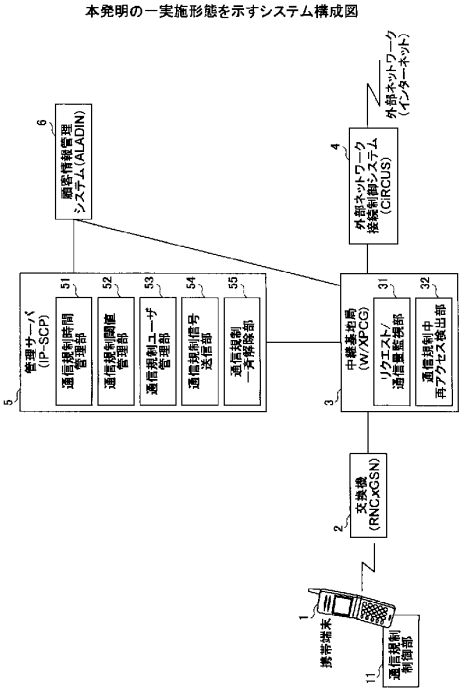
【図１】


従来における通信規制の概念図
101
102
交換機
103
中継基地局
携帯端末

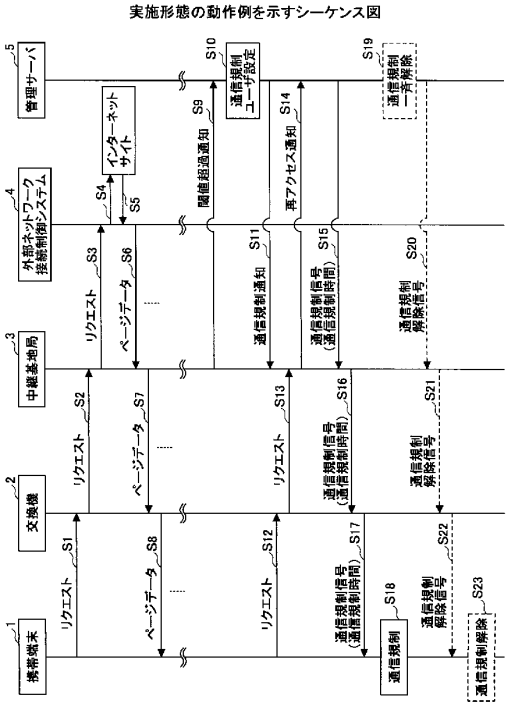
【図２】


本発明における通信規制の概念図
1
携帯端末
2
交換機
(RNC,xGSN)
通信規制信号
(通信規制時間)
3
中継基地局
(W/XPCG)

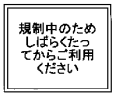
【図３】


本発明の一実施形態を示すシステム構成図
外部ネットワーク
(インターネット)
6
機密情報管理
システム(ALADIN)
4
外部ネットワーク
接続制御システム
(CIRCUS)
5
管理サーバ
(IP-SCP)
51
通信規制閾値
管理部
52
通信規制開始
管理部
53
通信規制ユーザ
管理部
54
通信規制信号
送信部
55
通信規制
一斉解除部
3
中継基地局
(W/XPCG)
31
リクエスト/
通信量監視部
32
通信規制中
再アクセス検出部
2
交換機
(RNC,xGSN)
1
携帯端末
11
通信規制
制御部

【図４】


実施形態の動作例を示すシーケンス図
5
管理サーバ
4
外部ネットワーク
接続制御システム
3
中継基地局
2
交換機
1
携帯端末
インターネット
サイト
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
S21
S22
S23
リクエスト
ページデータ
閾値超過通知
通信規制
ユーザ設定
再アクセス通知
通信規制通知
通信規制信号
(通信規制時間)
通信規制
一斉解除
通信規制
解除信号
通信規制解除

【図５】


携帯端末における表示画面の例を示す図
規制中のため
しばらくたって
からご利用
ください

フロントページの続き

Ｆターム(参考) 5K067 AA28 BB04 BB21 CC08 DD27 DD53 EE02 EE10 EE12 EE16
GG01 HH12 HH22
5K101 LL12 MM07 NN18 NN21 PP03 TT06

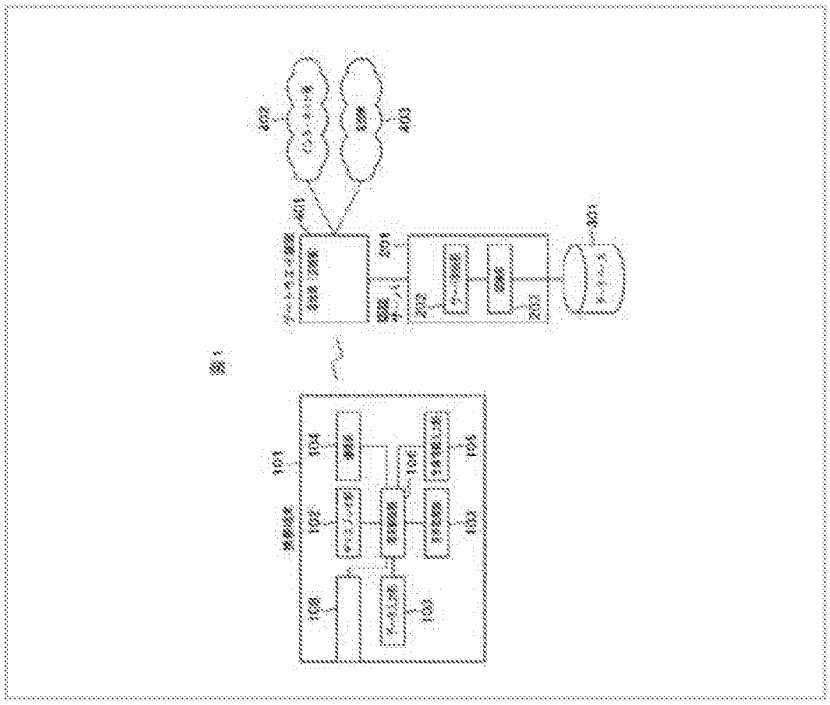
(11)Publication number	2006-344007
(43)Date of publication of application	21.12.2006
(51)Int.Cl.	G06F 21/20 (2006.01) H04L 9/32 (2006.01) H04Q 7/38 (2006.01) H04M 1/67 (2006.01)
(21)Application number	2005-169118
(22)Date of filing	09.06.2005
(71)Applicant	HITACHI LTD
(72)Inventor	OKAWA SATOICHI WATABE YOSHIRO YAMAKAWA YASUAKI TANGE TOMOYUKI HASEGAWA ATSUSHI

(54)PORTABLE TERMINAL IDENTIFICATION SYSTEM

(57)Abstract

PROBLEM TO BE SOLVED: To easily and surely carry out identification for a prepaid portable terminal.

SOLUTION: The portable terminal is equipped with; a biological information input section 105; a data input section 103; a storage section 108; a portable terminal 102 having a radio transmission section 104; a gateway device 401 having a function to decide a signal path of a data signal and a voice signal transmitted from this portable terminal and a function to set permission and inhibit of connection of the portable terminal; a database 301; and an authentication server 201 which authenticates a user by collating data of user's biological information already registered into the database and data of user's biological information transmitted from the portable terminal with the user's telephone number, when the effective period of the portable terminal registered in the database has not expired and sets permission and inhibit of the connection of the portable terminal to the gateway device based on the result of the authentication process.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-344007
(P2006-344007A)
(43)公開日　平成18年12月21日(2006.12.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285
H04L 9/32	(2006.01)	H04L	9/00	673D	5J104
H04Q 7/38	(2006.01)	H04B	7/26	109R	5K027
H04M 1/67	(2006.01)	H04M	1/67		5K067

審査請求 未請求　請求項の数 7　OL　（全 12 頁）

(21)出願番号　特願2005-169118 (P2005-169118)
(22)出願日　平成17年6月9日 (2005.6.9)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
特許業務法人　日東国際特許事務所
(72)発明者　大川　諭一
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(72)発明者　渡部　喜朗
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内

最終頁に続く

(54)【発明の名称】携帯端末本人確認システム

(57)【要約】　(修正有)
【課題】プリペイド携帯端末の本人確認を、簡単で確実に行う。
【解決手段】生体情報入力部１０５、データ入力部１０３、記憶部１０８、無線送信部１０４を有する携帯端末１０２と、該携帯端末から送信されたデータ信号や音声信号の信号経路を決定する機能及び前記携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置４０１と、データベース３０１と、該データベースに登録されている前記携帯端末利用の期限が有効である場合において、前記データベースに既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバ２０１とを備えた。
【選択図】図１

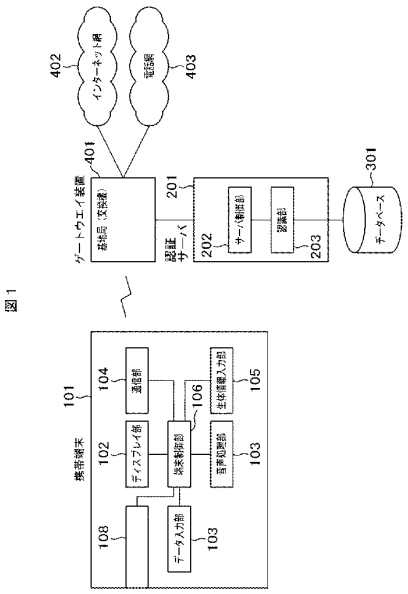


図１

【特許請求の範囲】
【請求項１】
利用者の生体情報を読み込むための生体情報入力部、サービスを受けるためのデータ信号や音声信号を入力する入力部及び利用者の電話番号に関する情報を記憶した記憶部を有し、前記生体情報入力部で読み込まれた利用者の生体情報に関するデータおよび前記記憶部に記憶された利用者の電話番号に関する情報並びに前記入力部から入力されたデータ信号や音声信号を通信部から無線通信によって送信する機能を有する携帯端末と、
該携帯端末がサービスを受けるために携帯端末から送信されたデータ信号や音声信号の信号経路を決定する機能及び前記携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置と、
前記利用者の生体情報に関するデータを前記利用者の電話番号に関する情報および前記携帯端末利用の有効期限と関連付けて登録して管理するデータベースと、
該データベースに登録されている前記携帯端末利用の期限が有効である場合において、前記データベースに既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバとを備えたことを特徴とする携帯端末本人確認システム。
【請求項２】
前記認証サーバは、更に、前記データベースに登録された前記携帯端末利用の有効期限に基づいて前記携帯端末が利用の有効期限が近づいたことを検出し、これを前記携帯端末に通知する機能を有し、
前記携帯端末は、更に、前記認証サーバから前記通知を受けた際、表示または音声により、前記携帯端末が利用の有効期限が近づいたことおよび該有効期限の延長を促すことを知らせる機能を有することを特徴とする請求項１記載の携帯端末本人確認システム。
【請求項３】
前記携帯端末は、更に、前記有効期限が近づいたことの通知を受けて利用者が確認した際、前記生体情報入力部より利用者の生体情報に関するデータを入力し、該入力された利用者の生体情報に関するデータを前記認証サーバへ送信する機能を有し、
前記認証サーバは、更に、前記データベースに既に登録されている利用者の生体情報に関するデータと前記携帯端末から送信を受けた利用者の生体情報に関するデータとの照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものであることを確認できた場合に限り前記データベースに対して前記携帯端末の利用有効期限の延長設定を行う機能を有することを特徴とする請求項２記載の携帯端末本人確認システム。
【請求項４】
前記認証サーバは、更に、前記照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものとは認められなかった場合には、前記携帯端末の有効期限延長が設定されなかったことを前記携帯端末に通知する機能を有することを特徴とする請求項３記載の携帯端末本人確認システム。
【請求項５】
前記認証サーバは、更に、前記携帯端末から応答が無く、有効期限切れが検出されたとき、前記ゲートウエイ装置に対して前記携帯端末の回線使用の禁止設定を行う機能を有することを特徴とする請求項２又は４記載の携帯端末本人確認システム。
【請求項６】
前記認証サーバは、更に、有効期限切れが発生して使用できなくなったことを前記携帯端末に通知する機能を有することを特徴とする請求項５記載の携帯端末本人確認システム。
【請求項７】
前記携帯端末は、プリペイド式携帯端末で構成されることを特徴とする請求項１乃至６の何れか一つに記載の携帯端末本人確認システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、生体情報を使用して、プリペイド式携帯端末を持つ利用者に対して、本人確認を確実で簡単に行うことのできる認証技術に関する。
【背景技術】
【０００２】
端末販売店舗のみならず、コンビニエンスストア等でも購入でき、契約時の手続きが容易なことから、プリペイド式携帯電話が普及しつつある。このようなプリペイド式携帯電話サービスを今後も維持していくためには、不正利用をできるだけ抑止することが可能な方法を導入することが必須となってきている。
【０００３】
ところで、現在、提供されているプリペイド携帯電話サービスにおいて、本人確認を行うには、運転免許証、パスポート、外国人登録証明書など写真入の公的書類の提示が必要になっている。そのため、利用者は、本人確認のため、定期的に店舗等に出向き、写真入公的書類との照会をする必要がある。また、各利用者の登録状態を一人ずつ手入力にて管理する必要がある。
【０００４】
また、個々の携帯端末の操作制限を実現する方法として、生体情報を利用する方法が一部メーカより提供されている携帯端末で採用されている。この方法は、携帯端末内部に登録された生体情報と携帯端末に装備されている読取装置から入力された生体情報とを照合することにより、操作制限あるいは解除の設定を行うというものである。
【０００５】
携帯端末利用サービスにおいて、生体情報を利用した適用例として、例えば特開２００４－１３７５３号公報（従来技術１）に記載の技術が知られている。この従来技術１は、管理制限区域への入隊室管理に応用している。あらかじめ生体情報を記録したＩＣカードを用意しておき、カードリーダが装備されている携帯端末に挿入し、携帯端末からドアの開錠要求を行う。送られた情報は、管理制限区域入口にあるドアコントローラに送信される。ドアコントローラには、生体情報の読取装置があり、ここから生体情報を入力し、先に送った生体情報との照合により、ドア開錠・施錠を制御するものである。
【０００６】
また、従来技術１に類似する技術としては、例えば特開２００１－１１７８７８号公報（従来技術２）がある。この従来技術２は、携帯電話から入力された生体情報を、サービスプロバイダへ送信し、さらに認証サーバへ送信される。そして、認証サーバには、あらかじめ登録してある利用者の生体情報が保存されており、このデータとサービスプロバイダから送られてきた生体情報と照合し、結果をサービスプロバイダに返信する、といった適用例である。
【０００７】
上記従来技術１及び２は、いずれも認証をその都度行う必要があり、現行のプリペイド携帯電話サービスの本人確認の方法としては、手続きが煩雑で使い勝手がよくない。
【０００８】
また、一度の本人確認を行うことにより、有効期限内であれば何度でもサービス提供を受けることが可能となるシステムの公知例としては、特開２００１－２９８７７９号公報（従来技術３）が知られている。この従来技術３においては、指紋データおよび有効期限情報は、携帯端末側で管理することになっている。
【０００９】
【特許文献１】特開２００４－１３７５３号公報
【特許文献２】特開２００１－１１７８７８号公報
【特許文献３】特開２００１－２９８７７９号公報
【発明の開示】

【発明が解決しようとする課題】
【００１０】
上記従来技術１及び２では、サービスの利用が必要になるたびに、その都度認証が必要であるという課題がある。プリペイド携帯端末のサービスを考えると、一度認証されたら、ある一定期間は認証することなく、サービス提供されることが望ましい。さらに、なりすまし等の不正利用問題を回避しつつ、店舗等まで出向く手間を省くことが可能な認証方法が要求される。
【００１１】
また、従来技術３においては、生体情報および有効期限管理を携帯端末側で行うため、第３世代携帯端末で一般的になってきているＵＳＩＭカード等の差し替えにより携帯端末を切り替えるたびに、各携帯端末に対して再設定を行う必要があるという課題を有していた。
【００１２】
本発明の目的は、上記課題を解決すべく、携帯端末の切り替えに対しても特別な手続き等を行うことなく、プリペイド携帯端末等の本人確認を、簡単で確実に行うことができるようにした携帯端末本人確認システムを提供することにある。
【課題を解決するための手段】
【００１３】
上記目的を達成するために、本発明は、利用者の生体情報を読み込むための生体情報入力部、サービスを受けるためのデータ信号や音声信号を入力する入力部及び利用者の電話番号に関する情報を記憶した記憶部（例えばＵＳＩＭカード等）を有し、前記生体情報入力部で読み込まれた利用者の生体情報に関するデータおよび前記記憶部に記憶された利用者の電話番号に関する情報並びに前記入力部から入力されたデータ信号や音声信号を通信部から無線通信によって送信する機能を有する携帯端末と、該携帯端末がサービスを受けるために携帯端末から送信されたデータ信号や音声信号の信号経路を決定する機能及び前記携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置と、前記利用者の生体情報に関するデータを前記利用者の電話番号に関する情報および前記携帯端末利用の有効期限と関連付けて登録して管理するデータベースと、該データベースに登録されている前記携帯端末利用の期限が有効である場合において、前記データベースに既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバとを備えたことを特徴とする携帯端末本人確認システムである。
【００１４】
また、本発明は、前記認証サーバは、更に、前記データベースに登録された前記携帯端末利用の有効期限に基づいて前記携帯端末が利用の有効期限が近づいたことを検出し、これを前記携帯端末に通知する機能を有し、前記携帯端末は、更に、前記認証サーバから前記通知を受けた際、表示または音声により、前記携帯端末が利用の有効期限が近づいたことおよび該有効期限の延長を促すことを知らせる機能を有することを特徴とする。
【００１５】
また、本発明は、前記携帯端末は、更に、前記有効期限が近づいたことの通知を受けて利用者が確認した際、前記生体情報入力部より利用者の生体情報に関するデータを入力し、該入力された利用者の生体情報に関するデータを前記認証サーバへ送信する機能を有し、前記認証サーバは、更に、前記データベースに既に登録されている利用者の生体情報に関するデータと前記携帯端末から送信を受けた利用者の生体情報に関するデータとの照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものであることを確認できた場合に限り前記データベースに対して前記携帯端末の利用有効期限の延長設定を行う機能を有することを特徴とする。
【００１６】

また、本発明は、前記認証サーバは、更に、前記照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものとは認められなかった場合には、前記携帯端末の有効期限延長が設定されなかったことを前記携帯端末に通知する機能を有することを特徴とする。

【００１７】

また、本発明は、前記認証サーバは、更に、前記携帯端末から応答が無く、有効期限切れが検出されたとき、前記ゲートウエイ装置に対して前記携帯端末の回線使用の禁止設定を行う機能を有することを特徴とする。

【００１８】

また、本発明は、前記認証サーバは、更に、有効期限切れが発生して使用できなくなったことを前記携帯端末に通知する機能を有することを特徴とする。

【００１９】

また、本発明は、前記携帯端末は、プリペイド式携帯端末で構成されることを特徴とする。

【発明の効果】

【００２０】

本発明によれば、プリペイド式携帯電話サービス等において、わざわざ店舗等に出向くことなく、簡単で確実な方法で本人確認を行うことができる。

【００２１】

また、本発明によれば、ＵＳＩＭカード等による携帯端末の切り替えに対しても、特別な手続き等を行うことなく適用可能である。

【発明を実施するための最良の形態】

【００２２】

本発明に係る、不正使用をできるだけ抑制でき、しかも端末販売店舗のみならず、コンビニエンスストア等でも購入でき、契約時の手続きが容易なプリペイド式携帯電話サービス等を受けることができ、さらに利用者の電話番号と生体情報を用いて関連付けてシステム全体で利用制限の管理を実現できる携帯端末本人確認システムの実施の形態について図面を用いて説明する。

【００２３】

上記利用者の電話番号としては、例えば、携帯端末へのＵＳＩＭ（Universal Subscriber Identity Module：汎用加入者識別モジュール）カード等の差し替えにより、複数端末の使い分け（例えば、一般通信用端末とデータ通信用端末の使い分け）、端末の更新（端末の機種変更）、さらには海外事業者端末との使い分け（チップ・イン・ローミング）が可能となる。

【００２４】

図１は、本発明に係る、不正使用をできるだけ抑制したプリペイド式携帯電話サービス等を受けることにできる携帯端末本人確認システムの一実施の形態の全体機能構成を示す図である。

【００２５】

本発明に係る携帯端末本人確認システムは、プリペイド式携帯電話サービス等を受けることにでき、さらに利用者固有の電話番号に関する情報を格納したＵＳＩＭカード等の差し替え可能で、生体情報を入力可能な携帯端末１０１と、上記利用者固有の電話番号によって携帯端末１０１がサービスを受けるために携帯端末１０１から送信されたデータ信号や音声信号の信号経路（インターネット網４０２や電話網４０３等からなる通信網を介したサービス装置への信号経路）を決定する機能及び認証サーバ２０１からの制御信号により上記電話番号（例えばＵＳＩＭカード等固有の電話番号）を持つ携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置（基地局（交換機））４０１と、新規登録時にあらかじめ携帯端末から取り込んだ利用者の生体情報に関するデータを上記携帯端末から得られる電話番号に関する情報と前記携帯端末利用の有効期限とを関連付けて登録して管理する機能を有するデータベース３０１を有し、該データベース３０１

に登録されている前記携帯端末利用の期限が有効である場合において、前記データベース３０１に既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバと、
該データベース３０１に登録されているデータと上記電話番号を持つ携帯端末１０１より送られてきた生体情報を照合し、携帯端末の本人確認時に認証処理を行い、該認証結果によりゲートウエイ装置に対し使用許可あるいは使用停止の設定を行う認証サーバ２０１とを備えて構成される。なお、携帯端末１０１とゲートウエイ装置４０１とは無線通信によって接続される。またゲートウエイ装置４０１と認証サーバ２０１との間は有線或いは無線によって接続される。

【００２６】

携帯端末１０１は、データ信号を入力するデータ入力部１０７と、メッセージを表示するディスプレイ部１０２と、音声信号の入出力を行う音声処理部１０３と、上記データ信号や音声信号の変復調処理を行って、ゲートウエイ装置（基地局（交換機））４０１との間で無線通信を行うための通信部１０４と、利用者固有の指紋などに代表される生体情報を読み込むための生体情報入力部１０５と、前記ディスプレイ部１０２、音声処理部１０３、通信部１０４、生体情報入力部１０５が相互にデータをやり取りするための端末制御部１０６とを有し、プリペイド式携帯電話サービス等を受けることにでき、さらに利用者固有の電話番号に関する情報を記憶したＵＳＩＭカード等（記憶部）１０８の差し替え可能に構成される。ここで、音声処理部１０３は、図２に示すように、音声を入力するマイク１０３１と、音声を出力するスピーカ１０３２と、上記マイク１０３１からの入力音声信号を入力音声データに変換して例えば端末制御部１０６に入力し、例えば端末制御部１０６から得られる出力音声データを上記スピーカ１０３２への出力音声信号に変換するデータ変換部１０３３とを有して構成される。生体情報入力部１０５は、図３に示すように、利用者本人の指紋などに代表される生体情報を読み込むスキャナ部１０５１と、該スキャナ部１０５１から読み込まれた生体情報を生体データに変換して例えば端末制御部１０６に出力するデータ変換部１０５２とを有して構成される。なお、データ入力部１０７及び音声処理部１０３のマイク１０３１などは、携帯端末がサービスを受けるためのデータ信号や音声信号を入力する入力部を構成する。また、上記通信部１０４は、更に、生体情報入力部１０５で読み込まれた利用者本人の生体情報に関するデータおよびＵＳＩＭカード等（記憶部）１０８に記憶された利用者の電話番号に関する情報もゲートウエイ装置（基地局（交換機））４０１へ無線通信によって送信されることになる。

【００２７】

ゲートウエイ装置４０１は、上記携帯端末１０１がサービスを受けるために携帯端末１０１から送信されたデータ信号や音声信号の信号経路（通信網を介したサービス装置への信号経路）を決定する機能及び認証サーバ２０１内のサーバ制御部２０２からの制御信号により、上記電話番号を持つ携帯端末の回線使用の許可設定及び禁止設定を行う機能を有する。ここでいうゲートウエイ装置とは、一般的な意味で使われているゲートウエイトは異なり、当該携帯端末の使用許可および使用停止を制御できる装置という位置付けの意味で用いている。

【００２８】

データベース３０１は、新規登録時にあらかじめ取り込んだ利用者本人の生体情報に関するデータを上記携帯端末から得られる電話番号に関する情報と上記携帯端末利用の有効期限とを関連付けて登録して管理する機能を有する。

【００２９】

認証サーバ２０１は、接続された上記データベース３０１に登録されているデータと上記電話番号を持つ携帯端末１０１より送られてきた生体情報を照合し、携帯端末の本人確認時に認証処理を行う認証部２０３と、該認証部２０３からの認証結果によりゲートウエイ装置４０１に対し使用許可あるいは使用停止の設定を行うサーバ制御部２０２とを有し

て構成される。

【００３０】

次に、本発明に係る携帯端末本人確認システムにおける新規登録処理の一実施例について図４を用いて説明する。図４は、新規登録処理の一実施例を示す流れ図である。新規登録時においては、まだ本発明に係る携帯端末１０１は使用できないので、この部分は、上記ディスプレイ部１０２、音声処理部１０３、通信部１０４、生体情報入力部１０５の機能を含む登録装置１０１に置き換わる。このとき、登録装置１０１がＵＳＩＭカード等（記憶部）１０８の差し替え可能に構成される場合にはＵＳＩＭカード固有の電話番号に関する情報が設定されることになる。ステップ６０１で、利用者は登録装置１０１に対して、新規登録要求送信を行う。新規登録要求を受信した認証サーバ２０１は、ステップ６０２でデータベース３０１を検索し、ステップ６０３で、これから登録しようとしている上記電話番号に対応した利用者のデータがすでにデータベース３０１に登録されていないかどうか確認する。すでに登録されていると判断された場合、認証サーバ２０１は登録装置１０１に対し、ステップ６０４で、新規登録の拒否通知を行う。ステップ６０３で、未登録データと判断された場合、認証サーバ２０１は登録装置１０１に対し、ステップ６０５で上記電話番号に対応した利用者の生体情報の入力要求を行う。生体情報の入力要求を受けた登録装置１０１は、ステップ６０６で登録装置１０１上に生体情報の入力を促すメッセージを出す。これに対し、利用者はステップ６０７で、登録装置１０１より上記電話番号に対応した生体情報信号を入力・送信する。登録装置１０１より送信された上記電話番号に関する情報に対応した生体情報信号を認証サーバ２０１が受信すると、認証サーバ２０１はステップ６０８でデータベース３０１に対し、ステップ６０９で上記電話番号に関する情報対応した生体情報の登録および上記携帯端末使用の有効期限設定を行うと同時に、ゲートウエイ装置４０１に対し、上記電話番号による携帯端末の使用許可設定を行う。使用許可設定が完了すると、ゲートウエイ装置４０１は、認証サーバ２０１に対して、ステップ６１０で使用許可応答を行う。使用許可応答を受信した認証サーバ２０１は、ステップ６１１で登録装置１０１に対して使用許可応答信号を送信し、該使用許可応答信号を受信した登録装置１０１は、ステップ６１２で使用が許可されたことをディスプレイ部１０２又は／及び音声処理部１０３を用いて利用者に通知する。なお、登録装置１０１と認証サーバ２０１との信号の送受信はゲートウエイ装置４０１を介して行われる。以上が新規登録時の流れとなり、認証サーバ２０１は定期的にデータベース３０１にアクセスを行い、有効期限が近づくまではゲートウエイ装置４０１に対して上記電話番号による携帯端末の使用を許可したままとなる。利用者も有効期限内であれば、利用の都度本人確認を行うことなく、上記電話番号による携帯端末を利用することができる。

【００３１】

次に、本発明に係る携帯端末本人確認システムにおける継続手続きの一実施例について図５を用いて説明する。図５は、継続手続きの一実施例を示す流れ図である。認証サーバ２０１内部において、システム内の通信トラヒィックが低い時間帯（例えば深夜など）に例えば１日１回、サーバ制御部２０２は認証部２０３に対して、既に登録されている携帯端末について、有効期限との関係を調べるよう指示する。該指示を受けた認証部２０３は、データベース３０１にアクセスし、登録されている全ての携帯端末について、現在日と有効期限日との関係を調査し、その結果を一括して把握することができる。調査した結果は、認証部２０３よりサーバ制御部２０２に通知される。このようにして、認証サーバ２０１は有効期限切れが近づいている電話番号の携帯端末および有効期限切れが発生している電話番号の携帯端末に関するデータを取得する。この結果、認証サーバ２０１は、新規登録時または前回の継続手続き時に設定された有効期限まで、規定の日数以内になると、ステップ６２１で上記電話番号による携帯端末１０１に対して有効期限切れが近づいていることを通知することができる。通知を受信した携帯端末１０１は、ステップ６２２で利用者に対して期限切れが近づいていることをディスプレイ部１０２又は音声処理部１０３を用いて通知する。図７は、ステップ６２２に対応するメッセージをディスプレイ部１０２に表示させた実施例である。利用者は、ステップ６２３で上記電話番号による携帯端末

１０１より認証サーバ２０１に対して、有効期限延長要求を行う。要求を受けた認証サーバ２０１は、ステップ６２４でデータベース３０１を検索し、ステップ６２５で要求を送信してきた上記電話番号による携帯端末１０１に関する情報が登録されているかどうかを確認する。データベース３０１に未登録の上記電話番号による携帯端末からの要求であると判断された場合、ステップ６２６で利用者に対し期限延長拒否通知を行う。この後、利用者が有効期限の延長手続きを行わずに有効期限が切れてしまうと、ゲートウエイ装置４０１により使用が禁止され、上記電話番号による携帯端末１０１は利用できなくなる。使用禁止の流れについては、図６の説明において具体的に述べる。ステップ６２５で認証サーバ２０１が、データベース３０１に登録済の上記電話番号による携帯端末からの要求であると判断したときは、ステップ６２７で上記電話番号による携帯端末１０１に対し、生体情報の入力要求を送信する。生体情報入力要求を受信した上記携帯端末１０１は、利用者に対し生体情報の入力を促すメッセージを出力する。利用者は、上記携帯端末１０１より生体情報を入力し、認証サーバ２０１に送信する。生体情報信号を受信した認証サーバ２０１は、ステップ６３０でデータベース３０１に登録されている上記電話番号に関する情報に対応した生体情報に関するデータと、いま上記電話番号による携帯端末１０１から送信されてきた生体情報に関するデータとを照合する。該生体情報に関するデータの照合を行った結果、同じ利用者の生体情報のデータではないと判断されたとき、認証サーバ２０１は上記電話番号による携帯端末１０１に対し、期限延長が拒否されたことを通知する。通知を受けた上記電話番号による携帯端末１０１は利用者に対し、ステップ６３１で有効期限の延長が拒否されたことを通知する。この後、利用者が有効期限の延長手続きを行わずに有効期限が切れてしまうと、ゲートウエイ装置４０１で禁止され、上記電話番号による携帯端末１０１は利用できなくなる。使用禁止の流れについては、図６の説明において具体的に述べる。ステップ６３０で同じ利用者の生体情報のデータであると判断すると、認証サーバ２０１は、上記電話番号による携帯端末１０１から送信されてきた生体情報のデータは利用者本人からの要求であると判断し、ステップ６３２でデータベース３０１に対し、期限延長の設定を行う。期限延長の設定が完了すると、認証サーバ２０１はステップ６３３で上記電話番号による携帯端末１０１に対し、有効期限の延長が許可されたことを通知する。許可信号を受信した上記携帯端末１０１は、利用者に対し、ステップ６３４で有効期限が延長されたことをディスプレイ部１０２又は音声処理部１０３を用いて通知する。

【００３２】

次に、本発明に係る携帯端末本人確認システムにおける使用禁止処理の一実施例について図６を用いて説明する。図６は、使用禁止処理の一実施例を示す流れ図である。認証サーバ２０１は、新規登録時または前回の継続手続き時に設定された有効期限まで、規定の日数以内になると、ステップ６４１で電話番号による携帯端末１０１に対して有効期限切れが近づいていることをゲートウエイ装置４０１を介して通知する。有効期限切れが近づいていることを調べる方法は上記図５の説明で述べた通りである。通知を受信した電話番号による携帯端末１０１は、ステップ６４２で利用者に対して期限切れが近づいていることをディスプレイ部１０２又は音声処理部１０３を用いて通知する。期限切れが近づいているにもかかわらず、利用者が、上記図５で説明した、有効期限延長期限の手続きを行わなかった場合、さらに日数が経過すると、認証サーバ２０１がステップ６４３で有効期限切れを検出する。有効期限切れを検出した認証サーバ２０１は、ステップ６４４でゲートウエイ装置４０１に対し、当該携帯端末の使用禁止設定指示を行う。使用禁止設定の指示を受けたゲートウエイ装置４０１は、ステップ６４５で使用禁止設定の処理を行い、処理が終わると認証サーバ２０１に対して応答する。応答信号を受信した認証サーバ２０１は、ステップ６４６で上記電話願号による携帯端末１０１に対して使用禁止応答信号を送信する。応答信号を受信した上記携帯端末１０１は、ステップ６４７で利用者に対し、当該携帯端末の使用が禁止されたことを例えばディスプレイ部１０２又は音声処理部１０３を用いて通知する。図８は、ステップ６４７に対応するメッセージをディスプレイ部１０２に表示させた実施例である。

【００３３】
以上説明したように本実施の形態は、プリペイド携帯電話における本人確認の方法に関する発明であるが、これを管理区域への入退室管理システムにも応用できる。また、本実施の形態によれば、電話番号と生体情報をリンクさせて、サーバ側でまとめて情報を管理するため、第３世代携帯端末で一般的になっている、ＵＳＩＭカード等による携帯端末切り替えに対しても、特別な手続き等を行うことなく適用可能である。

【図面の簡単な説明】

【００３４】
【図１】本発明に係る携帯端末本人確認システムの一実施の形態を示すシステム構成図である。
【図２】図１に示す携帯端末における、音声処理部の一実施例を示す構成図である。
【図３】図１に示す携帯端末における、生体情報入力部の一実施例を示す構成図である。
【図４】本発明に係る携帯端末本人確認システムにおいて、新規登録処理の一実施例を示すフロー図である。
【図５】本発明に係る携帯端末本人確認システムにおいて、継続手続きの一実施例を示すフロー図である。
【図６】本発明に係る携帯端末本人確認システムにおいて、使用禁止処理の発生の一実施例を示すフロー図である。
【図７】本発明に係る、利用者に対して有効期限切れが近づいていることをメッセージにてディスプレイ部に出力した表示の実施例を示す図である。
【図８】本発明に係る、利用者に対して有効期限が切れてしまったことをメッセージにてディスプレイ部に出力した表示の実施例を示す図である。

【符号の説明】

【００３５】
１０１…携帯端末、１０２…ディスプレイ部、１０３…音声処理部、１０３１…マイク部、１０３２…スピーカ部、１０３３…音声データ変換部、１０４…通信部、１０５…生体情報入力部、１０５１…スキャナ部、１０５２…生体情報データ変換部、１０６…端末制御部、１０７…データ入力部、１０８…記憶部（ＵＳＩＭカード等）、２０１…認証サーバ、２０２…サーバ制御部、２０３…認証部、３０１…データベース、４０１…ゲートウエイ装置（基地局（交換機））、４０２…インターネット網、４０３…電話網。

【図１】

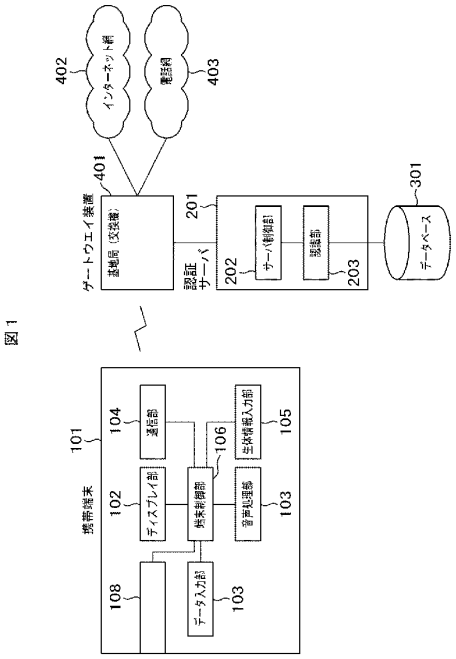
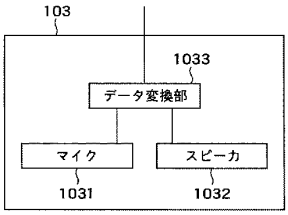


図１

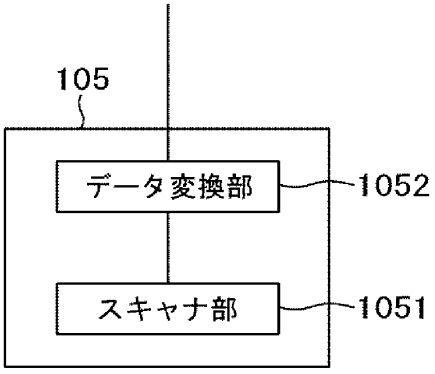
【図２】

図２



【図３】

図３



【図４】

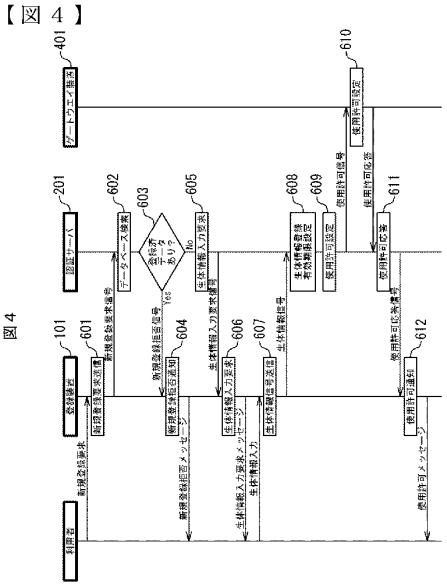


図４

【図５】

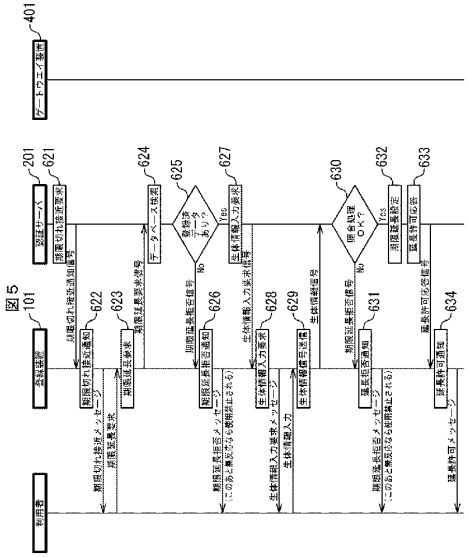


図５

【図６】

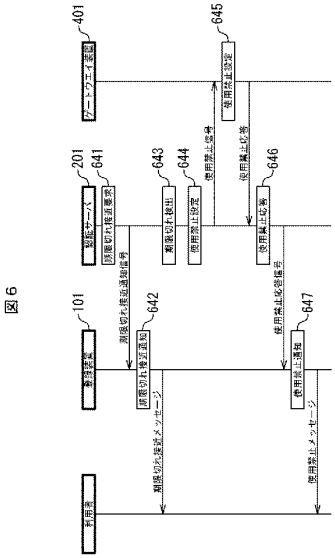


図６

【図７】

図７

To:USER @aaa.bbb.jp
Fm: ADMIN @xxx.yyy.jp
Message:
この端末は、有効期限が近づいております。
(期限： yyyy 年 mm 月 dd 日)
下記リンク先にアクセスして、有効期限延長の手続きを行ってください。
ここをクリック

【図８】

図８

To:USER @aaa.bbb.jp
Fm: ADMIN @xxx.yyy.jp
Message:
この端末は、有効期限切れになっております。
(期限： yyyy 年 mm 月 dd 日)
引き続きご利用を希望される場合は、最寄のzzzショップまでご連絡下さい。

フロントページの続き

(72)発明者　山川　泰明
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(72)発明者　丹下　智之
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(72)発明者　長谷川　篤
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内

Fターム(参考)　5B285 AA04　CB12
5J104 AA07　KA16　PA01　PA02　PA07
5K027 AA11　BB09　HH23
5K067 AA32　AA33　BB04　DD17　DD27　EE02　EE10　EE16　FF02　HH22
HH36　KK15

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 September 2005 (09.09.2005)

PCT

(10) International Publication Number
WO 2005/083934 A1

(51) International Patent Classification[7]: H04L 12/16, H04Q 7/20

(21) International Application Number: PCT/CA2005/000286

(22) International Filing Date: 25 February 2005 (25.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/548,096 27 February 2004 (27.02.2004) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Philip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SHENFIELD, Michael** [CA/CA]; 38 Stockdale Crescent, Richmond Hill, Ontario L4C 3S9 (CA). **GORING, Bryan** [CA/CA]; 1542 Morse Place, Milton, Ontario L9T 5V4 (CA). **TSENTER, Igor** [CA/CA]; 62 Hawkview, Woodbridge, Ontario L4H 2E2 (CA).

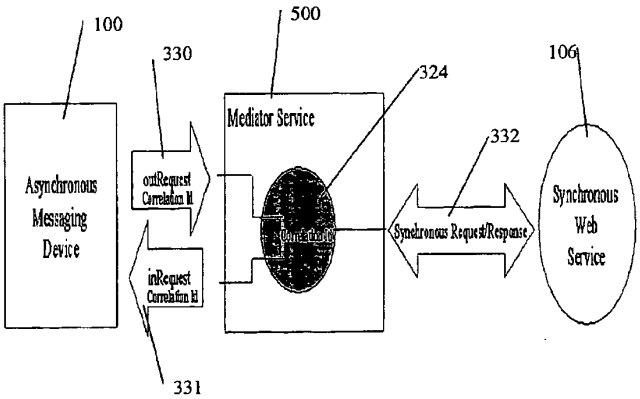
(74) Agent: **TISDALL, Grant**; Gowling Lafleur Henderson LLP, Suite 4900, Commerce Court West, Toronto, Ontario M5L 1J3 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR COMMUNICATING ASYNCHRONOUSLY WITH WEB SERVICES USING MESSAGE SET DEFINITIONS



(57) Abstract: A system and method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages. The system and method comprising: a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier; a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

WO 2005/083934 A1

BNSDOCID: <WO_____2005083934A1_I_>

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

System and Method for Communicating Asynchronously with Web Services Using Message Set Definitions

BACKGROUND

This application relates generally to wireless communication and specifically to network messaging for mobile communication devices.

There is a continually increasing number of mobile communication devices in use today, such as mobile telephones, PDAs with wireless communication capabilities, and two-way pagers. Software applications which run on these mobile communication devices increase their utility. For example, a mobile phone may include an application which retrieves the weather for a range of cities, or a PDA may include an application that allows a user to shop for groceries. These software applications take advantage of the mobility of these devices and connectivity to a wireless network in order to provide timely and useful services to users, regardless of where the users are. However, due to the restricted resources of mobile communications devices, and the complexity of delivering data wirelessly to a mobile communication device, developing software applications for mobile communications devices remains a difficult and time-consuming task.

Web Services are emerging as the de-facto mechanism to allow disjoint parties to collaborate on the Internet. Web services allow businesses and other parties to collaborate in a universal, platform and language neutral way and promise to overcome traditional barriers encountered in linking numerous and diverse information systems. Web services are still in their relative infancy, with many technology players cooperating to define the emerging standards, and corporations beginning to throw their weight behind the thrust to link disparate systems over the web using this standard approach. A common model employed in web service offerings is the traditional synchronous request-response type interaction whereby the consumer of the service passes some information and receives something in response. In this scenario the user of the device requests or **"pulls"** the content from the network. In other words, the content is

BNSDOCID: <WO____2005083934A1_I_>

constantly present in the network, but the user needs to issue a retrieval request to access the information (e.g. using a browser on the mobile device).

In real-life applications there is a lot of information that is available to a user but hardly accessible, as the user doesn't know when the information is posted or when there is a change in the status of the posted content. Such information ideally needs to be **"pushed"** to the user either periodically or when certain predefined events occur. Some examples of possible push situations are unrequested arrival of new e-mail, stock market information, multi-user game updates, etc. This ability to push information spontaneously implies an asynchronous messaging framework. From a practical point of view, wireless communications have higher cost than wired communications and usually are characterized by higher latency times, making a 'pull' from a wireless device inherently expensive. Slow connection times sometimes might be critical to the user's experience. Push technology can be wireless friendly. Its users can benefit in a number of ways: push technology can make useful data instantly available, can improve user perception of the wireless network; can make data delivery cost effective (since the device does not have to repeatedly poll for data); and can extend battery life.

Wireless push would involve a server that, given a user's specific one-time request to be notified with specific data on predefined conditions, would send this data to the user's device as soon as the data is available and/or the conditions have been met. The communication protocol and user/device addressing are device-specific and the server must be aware of them. Web Services have become a ubiquitous standard for access to content resources as well as communicating to back-end servers. Their number and complexity have increased considerably in recent years. However, invoking Web Service operations from a wireless device using the synchronous communication method exclusively can be expensive and impractical.

SUMMARY OF THE INVENTION

Systems and methods disclosed herein provide a correlated asynchronous messaging environment to obviate or mitigate at least some of the above presented disadvantages.

BNSDOCID: <WO____2005083934A1_I_>

Wireless push would involve a server that, given a user's specific one-time request to be notified with specific data on predefined conditions, would send this data to the user's device as soon as the data is available and/or the conditions have been met. The communication protocol and user/device addressing are device-specific and the server must be aware of them. Web Services have become a ubiquitous standard for access to content resources as well as communicating to back-end servers. Their number and complexity have increased considerably in recent years. However, invoking Web Service operations from a wireless device using the synchronous communication method exclusively can be expensive and impractical. Contrary to current systems and methods there is provided a system and method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages. The system and method comprising: a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier; a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

There is provided a system for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the system comprising: a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in

BNSDOCID: <WO_____2005083934A1_I_>

the asynchronous response message when received, the first identifier different from the second identifier; a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

There is further provided a method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the method comprising the steps of: sending an asynchronous request message of the communication messages; receiving an asynchronous response message of the communication messages; linking the asynchronous request message with the corresponding asynchronous response message by employing a message correlation set including a set of correlation definitions, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier; associating a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

There is further provided a computer program product for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the computer program product comprising: a computer readable medium; a message correlation set module stored on the medium and configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in

BNSDOCID: <WO____2005083934A1_I_>

the asynchronous response message when received, the first identifier different from the second identifier; a message manager module for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set module, the first and second data parameters also part of the message correlation set as data definitions.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features will become more apparent of embodiments of the present invention in the following detailed description, in which reference is made to the appended drawings by way of example wherein:

Figure 1 is a block diagram of a communication system;

Figure 2 is a block diagram of a mobile communication device of Figure 1;

Figure 3 is an asynchronous messaging and data relationship example of the web service of Figure 1;

Figure 4 is an example synchronous operation of the web service of Figure 3;

Figure 5 shows a mediator service correlating asynchronous to synchronous messaging of the examples of Figures 3 and 4;

Figure 6 shows an example configuration of the mediator service and runtime of Figures 1 and 5;

Figure 7 is further embodiment the system of Figure 5; and

Figure 8 is a block diagram of a component application program of Figure 9.

DESCRIPTION

Network System

Referring to Figure 1, a network system 20 comprises mobile communication devices 100 for interacting with one or more web services 106 provided via a coupled wireless network 102 and the Internet 104. The devices 100 transmit and receive requests/response messages 105, respectively, when in communication with the web services 106. The devices 100 can operate as web clients of the web services 106 by using the requests/response messages 105 in the form of message header information and associated data content, for example requesting and

BNSDOCID: <WO_____2005083934A1_I_>

receiving product pricing and availability from an on-line merchant. The web service 106 is an example of a system with which client application programs 302 (see Figure 2) on the communication devices 100 interact via the wireless network 102 and the Internet 104 in order to provide utility to users of the communication devices 100. The messages 105 sent between the communication devices 100 and the web service 106 could traverse a message-map service (not shown) which converts the messages 105 between the differing formats used by the devices 100 and the web service 106.

For satisfying the appropriate requests/response messages 105, the web service 106 could communicate with the devices 100 through various protocols (such as but not limited to HTTP and component API) for exposing relevant business logic (methods) to client application programs 302 (see Figure 2) once provisioned on the devices 100. The application programs 302 of the devices 100 can use the business logic of the web service 106 similarly to calling a method on an object (or a function). It is recognized that the client application program 302 can be downloaded/uploaded in relation to the web service 106, through the messages 105 via the network 102, 104, directly to the devices 100. It is further recognized that the devices 100 can communicate with one or more web services 106 via the networks 102, 104.

Server Environment

Referring to Figure 1, the web service 106 provides information messages 105 which are used by the client application programs 302 on the communication devices 100. Alternatively, or in addition, the web service 106 may receive and use the information messages 105 provided by the client application programs 302 executed on the communication devices 100, or perform tasks on behalf of client application programs 302 executed on the communication devices 100. The web service 106 can be defined as a software service, which can implement an interface expressed using Web Services Description Language (WSDL) registered in Universal Discovery Description and Integration (UDDI), for example,and can communicate through messages 105 with client devices 100 by being exposed over the Internet 104 through an appropriate protocol such as the Simple Object Access Protocol (SOAP), for example. In some implementations, SOAP is a specification that defines the XML format for the messages 105, including a well-formed XML fragment enclosed in SOAP elements. Other parts of SOAP specify how to

BNSDOCID: <WO____2005083934A1_I_>

represent program data as XML and how to use SOAP to do Remote Procedure Calls (RPC). These optional parts of SOAP are used to implement RPC-style applications where a SOAP request message 105 containing a callable function, and the parameters to pass to the function, is sent from the client device 100, and the service 106 returns the response message 105 with the results of the executed function. SOAP also supports document style applications where the SOAP message 105 is a wrapper around an XML document. A further optional part of SOAP defines the HTTP binding (e.g. header), whereas some SOAP implementations support MSMQ, MQ Series, SMTP, or TCP/IP transport protocols. Alternatively, the web service 106 may use other known communication protocols, message 105 formats, and the interface may be expressed in other web services 106 languages than described above. Accordingly, the services supplied by the web service 106 are utilized by the user of the devices 100 over the network 102, 104.

Client Environment

Referring to Figures 2 and 3, the applications 302 are software applications which can be written, for example, in eXtensible Markup Language (XML) and a subset of ECMAScript. An example application 302 is described in detail, for completeness purposes, with reference to Figure 10 in the Application Program 302 section found at the end of this Description Section. XML and ECMAScript are standards-based languages which allow software developers to develop the applications 302 in a portable and platform-independent way. The applications 302 can be transmitted over-the-air via the wireless network 102 and loaded into a memory module 210 of a device infrastructure 204. Alternatively, the applications 302 may be loaded via a serial connection, a USB connection, or a short-range wireless communication system such as IR, 802.11(x) and/or Bluetooth™ onto the device 100. Once loaded onto the mobile communication device 100, the applications 302 are executed by a framework 206 on the mobile communication device 100, which converts applications 302 into native code which is executed by the processor in the device infrastructure 204. Alternatively, the applications 302 may be executed as native code or interpreted by another software module or operating system on the mobile communication device 100, which provides the framework 206 as a native runtime environment, hereafter referred to generically by reference numeral 206.

BNSDOCID: <WO____2005083934A1_I_>

Referring again to Figure 3, the applications 302 are organised as multiple tier/layer 310 applications 302, such as but not limited to a messaging layer 404 and a data layer 400. It is recognised that the application 302 can contain other layers 310, such as but not limited to a presentation layer 402 and a workflow layer 406, as further explained below with reference to Figure 10. The application 302 is configured to have a set of data definitions 314 in the data layer 400, a set of asynchronous message definitions 316 in the message layer 404 and mappings 318 that specify how the message definitions 316 are related to the underlying data definitions 314. In general, it is recognised that the application definitions 314,316 (including definitions 320,322 – see Figure 10) of the respective layers 310 can be expressed in a structured definition language such as but not limited to XML.

Data Components 400 can be defined as application 302 data represented in native code or XML, or other structured definition language. Message Components 402 can be defined as messaging data represented in native code or XML, or other structured definition language. Message components 402 may define mapping relationships to Data Components 400 that specify their definition, or how underlying data is affected through transmission or reception of the messages 330,331a,331b. The Device Runtime or framework 206 can be defined as the software that hosts and evaluates the application 302. The Device Runtime 206 provides services to manage data associated to the application 302, provides capability for asynchronous incoming 331b and outgoing messages 330 generated by the application 302, and manages relationships between messages and data. Message Mapping can be defined as a relationship existing between data 400 and message 402 components that specifies partial or complete definition of the message based on a data mapping, and how messaging interactions affect the underlying data.

Generally the data definitions 314 are distinguished as having a set of sub-elements 323 (or fields), and define a key field or identifier 324 by which the mapping 318 (from the corresponding message definition 316) to the associated data element 323 may be resolved. Messages 105 derived from the message definitions 316 can define a set of fields but may not specify key fields, which is implemented through mappings 318. The messages 105 are typically short lived; are consumed and then discarded, whereas data elements 323 corresponding to the data definitions 314 are long lived and may be restored at any time from the persistent storage

BNSDOCID: <WO____2005083934A1_I_>

210 (see Figure 2) by providing the appropriate key field value 324 by the storage service (not shown) of the device runtime 206. The messages 105, either synchronous-based or asynchronous-based, represent interactions with entities (i.e. web-services 106) outside of the Device Runtime 206 and these messages 105 are typically not correlated by the web services 106 themselves. The messages 105 may be defined as originating (i.e. out message 105) from the device runtime 206 and targeted to the external web service 106, or may be transmitted (i.e. in message 105) to the device runtime 206.

Further, message definitions 316 may define relationships to data elements 323 called mappings 318 that determine how origination or reception of the related message 105 affects the related data element 323, as for example defined by the data definition 314 of the data layer 400. This mapping 318 relation is uniquely identified by the key field 324 mapping 318 that may be determined as follows, such as but not limited to:

the mapping 318 is made directly to the data definition 314: the message 105 takes its complete definition from the data definition 314 such that the data element key field 324 value is extracted from identical message definition 316 field element (generally referred to hereafter as message mapping 318 wherein all fields of the message 105 correspond to all fields of the data definition 314); and

the mapping 318 is from a field of the message definition 316 to a field of the data definition 314: the message 105 partially defines itself such that the data element key field 324 value is extracted from mapped message field (generally referred to hereafter as field mapping 318 wherein selected fields of the data definition 314 are mapped 318 to selected fields of the message definition 316).

As an example, referring to Figure 3, consider an asynchronous web service 106 (see Figure 1) that models a pizza parlour. This web service 106 exposes the capability to register the wireless device 100 as a PizzaClient application 302 (see Figure 2) and may aynchronously deliver the user an asynchronous response message 331, e.g. a Coupon message 326 or a Special message 328, to the wireless application 302 running on the runtime environment 206 of the device 100. The set of corresponding data elements 323 and asynchronous response messages 331 to interact with the web service 106 are depicted in Figure 3, which illustrates the

BNSDOCID: <WO____2005083934A1_I_>

PizzaClient data elements 323 and message field level mappings 318 to the outRegisterUser outgoing request message 330. The PizzaClient application 302 may contain none or more Coupon data elements 323 which are message mapped 318 directly to the inAddCoupon incoming message 326. Finally the Special data element 323 is message mapped 318 directly to the inAddSpecial incoming message 328. It is noted that the inAddCoupon 326 and inAddSpecial 328 are asynchronous messages 331, such that each arriving message 326,328 identifies its own key field (from mapping 318) that affects the underlying data element 323. For example, once the messages 326,328 are received by the application 302, the persistence service (e.g. data manager) of the device 100 may create a new data element or update an existing data element resident in the storage 210 (see Figure 2).

Further, referring to Figure 4, suppose that the Pizza Shop now wants to extend their web service 106 by allowing the user of the device 100 to order a pizza. The web service 106 can be enhanced to provide a synchronous message operation 332 that accepts some order criteria and returns order confirmation and delivery time. The order request is distinguished by an order id (this becomes the data key 324 preferably a unique identifier), and the order confirmation id 325 is associated with uncorrelated data from the web service 106 describing the success of the order. Correlation of the return data from the Web Service's 106 perspective is achieved by the synchronous request-response nature of the submission operation 332. However correlation of the returned data within the framework of the asynchronous messaging model (see Figure 3) of the device runtime environment 206 is not immediately apparent, due to the fact that the order confirmation data returned by the web service 106 is uncorrelated to the request by any key 324 information, which if included would tie the result to the original order data element. As depicted in Figure 4, two asynchronous message definitions 316 are used to generate corresponding messages 105 to handle the order placement (outPlaceOrder) and reception of order confirmation (orderConfirmation). The mediator 500 (see Figure 5) is used to help link the order confirmation information directly to the originating Order data element, as further described below.

Referring again to Figures 1 and 2, the client runtime environment 206 provided by the devices 100 can be configured to make the devices 100 operate as web clients of the web

BNSDOCID: <WO____2005083934A1_I_>

services 106. The client runtime environment 206 of the devices 100 is preferably capable of generating, hosting and executing the client application programs 302 (which are in the form of tiered/layered 310 applications – see Figure 3) on the device 100. Further, specific functions of the client runtime environment 206 can include such as but not limited to support for language, coordinating memory allocation, networking, management of data during I/O operations, coordinating graphics on an output device of the devices 100 and providing access to core object oriented classes and supporting files/libraries.

The terminal runtime environment 206 of the devices 100 preferably supports the following basic functions for the resident executable versions of the client application programs 302, such as but not limited to:

provide a communications capability to send the messages 105 to the Web Services 106 connected via the network 102, 104;

provide data input capabilities by the user on the input interface 202 (see Figure 2) of the devices 100 to supply data parts for Web Services' outgoing messages 105 (messages to the service 106);

provide data presentation or output capabilities for Web Services' response messages 105 (incoming messages) or uncorrelated notifications of the web service 106 on the output interface 202;

provide data storage services to maintain local client data in the memory module 210 (see Figure 9) of the device 100; and

provide an execution environment for a scripting language for coordinating operation of the application layers 400, 402, 404, 406 (see Figure 10) of the client application programs 302.

Therefore, the native client terminal runtime environment 206 provides an interface for the client application programs 302 and to the device 100 functionality of a processor 208 and associated operating system of a device infrastructure 204. The runtime environment 206 preferably supplies a controlled, secure and stable environment on the device 100, in which the component application programs 302 execute. The runtime environment 206 provisions the definitions of the layers 400, 402, 404, 406 to create the actual web client.

BNSDOCID: <WO____2005083934A1_I_>

Communication Device

Referring to Figures 1 and 2, the communication devices 100 are devices such as but not limited to mobile telephones, PDAs, two-way pagers and dual-mode communication devices (see Figure 9). The devices 100 include a network connection interface such as a wireless transceiver 200 coupled via connection 218 to the device infrastructure 204. The wireless transceiver 200 is connectable during operation of the devices 100 to the network 102, 104, such as to the wireless network 102 by RF links, which enable the devices 100 to communicate with each other and with external systems (such as the web service 106) via the network 102, 104. The wireless transceiver 200 also helps the device 100 to coordinate the requests/response messages 105 between the client application programs 302 and the service 106. The network 102, 104 supports the transmission of data in the requests/response messages 105 between devices 100 and external systems, which are connected to the network 102, 104. The network 102, 104 may also support voice communication for telephone calls between the communication devices 100 and devices which are external to the network 102, 104. A wireless data transmission protocol can be used by the wireless network 102, such as but not limited to DataTAC, GPRS or CDMA. The connection between the wireless network 102 and the Internet 104 includes an Internet Gateway (not shown), which provides for the messages 105 and associated data content to flow between the connected devices 100 and the web service 106.

Referring again to Figure 2, the devices 100 also have the user interface 202, coupled to the device infrastructure 204 by connection 222, to interact with a user (not shown). The user interface 202 can include one or more user input interface such as but not limited to a QWERTY keyboard, a keypad, a trackwheel, a stylus, a mouse, a microphone, and the user output interface such as an LCD screen display and/or a speaker. If the screen is touch sensitive, then the display can also be used as the user input device as controlled by the device infrastructure 204. The user interface 202 is employed by the user of the device 100 to coordinate the requests/response message messages 105 over the system20(see Figure 1) as employed by client application programs 302 executed in the runtime environment 206.

Referring again to Figure 2, operation of the communication device 100 is enabled by the device infrastructure 204. The device infrastructure 204 includes the computer processor 208

BNSDOCID: <WO____2005083934A1_I_>

and the associated memory module 210. The computer processor 208 manipulates the operation of the network interface 200, the user interface 202 and the runtime environment 206 of the communication device 100 by executing related instructions, which are provided by an operating system and client application programs 302 located in the memory module 210. Further, it is recognized that the device infrastructure 204 can include a computer readable storage medium 212 coupled to the processor 208 for providing instructions to the processor and/or to load/update client application programs 302 in the memory module 210. The computer readable medium 212 can include hardware and/or software such as, by way of example only, magnetic disks, magnetic tape, optically readable medium such as CD/DVD ROMS, and memory cards. In each case, the computer readable medium 212 may take the form of a small disk, floppy diskette, cassette, hard disk drive, solid state memory card, or RAM provided in the memory module 210. It should be noted that the above listed example computer readable mediums 212 can be used either alone or in combination.

Mediator Service 500

The desire to migrate towards an asynchronous messaging 105 paradigm in relation to the device 100 is further explained with reference to Figure 5, by example only, wherein a message set 600 (see figure 6) is used to facilitate asynchronous communication between the device 100 and the synchronous web service 106. For situations in which the web service 106 is an asynchronous web service 106, the message set 600 (see Figure 6) is also applicable, as further described below, wherein the device 100 may communicate directly with the asynchronous web service 106 preferably without the proxy function of the mediator 500. . It is recognized that the mediator service 500 could be hosted: on the device 100 as either part of the application 302 or as a separate service/program; on a third party server; and/or on the web service 106, as desired.

Application Synchronous Message Set 600

Referring to Figure 6, the message set 600 can be defined as a data to message set that provides for a synchronous relation of otherwise uncorrelated (asynchronous) messages 330,331. It is recognized that the message set 600 can be described in a structured definition language (e.g. markup language) such as but not limited to XML. An example of the message set is the data elements 324a,b,c and 325a,b of the data definition 314 of Figure 4. It is noted that the

BNSDOCID: <WO____2005083934A1_I_>

mediator service 500 can optionally proxy synchronous messaging 332 interaction with the web service 106 into the asynchronous exchange of messages 330,331 to the Device Runtime 206 of the device 100. The message Set 600 is a logical grouping of messages definitions 330,331 (see figure 4) of the message definition tier 404 and data elements 324a,b,c of the data tier 400 included for the outgoing asynchronous message 330 content and the data elements 325a,b included in the incoming asynchronous message 331 content. The data definition 314 of the data tier 400 states a correlation between otherwise unrelated asynchronous messages by defining the data 324a,b,c and 325a, as the message set 600. The message set 600 applies a restriction to the otherwise unrestricted asynchronous messaging 330;331 paradigm.

For example, the message set can be further defined as: a single data element definition 314 to which messages 330,331are correlated; one or more outgoing messages 330 that are derived from the data definition 314; and one or more incoming messages 331 that are applied to the data definition 314.

Referring to Figure 7 for example, the problem of correlating a Pizza Shop order could be addressed by defining the Message Set 600 in figure 6, where the outPlaceOrder message 330 and orderConfirmation message 31 are correlated to the Order data definition 314 and clearly define how outgoing and incoming asynchronous messages 330,331 affect the underlying data elements as defined by the definition 314. The outPlaceOrder message 330 complies to the agreement of outgoing messages in the message set 600 by linking to the key field 324a of Order definition 314, i.e. outgoing message 330 definitions may be constrained in that they provide a linkage 440 (see figure 4) to the key element 324a of the data definition 314. This may arise due to Message Mapping or Field Mapping, as described above. The orderConfirmation incoming message 331 conforms to the incoming message requirement of the message set 600 for example by not linking to any key field 324a of the Order data definition 314, rather containing an identifier field 325a that is also part of the message set 600, i.e. incoming message 331 definitions specify Field Mapping 442 directions to the Message Set 600 enclosed by the data element definition 314. Incoming message 331 definitions may be constrained in that they cannot employ Message Mapping 440, and for example no Field Mapping 442 may reference the key field element 324a of the data definition 314.

BNSDOCID: <WO____2005083934A1_I_>

It is further emphasized in relation to Figure 7 that the Mediator Service 500 may act as a proxy to the device runtime 206 asynchronous messaging 330,331 so as to assist the device 100 to interact asynchronously with a synchronous message 332 based web service 106. However, the Mediator Service may or may not be present between the device 100 and the web service 106 in cases where the web service is asynchronous based and has knowledge of the message set definitions 600. A further scenario is that the mediator service 500 is present between the device 100 and the web service 106 and has knowledge of the message set 600 definitions and can therefore either interact with the web service 106 in a synchronous fashion or asynchronously as dictated by the configuration of the web service 106. The Mediator Service 500, where used, is able to maintain correlation information of the message set 600 between the incoming device message 330 (i.e. in essence the outgoing request to the web service 106) and the outgoing device message 331 (in essence the response by the web service 106). It is further recognized that where used, the mediator service 500 can be part of the device 100, part of the web service 106, and/or configured as a third party proxy.

Message Set Components

Referring to Figure 6, in this system 20, the management of correlation of asynchronous messages 330,331 can be split between the intelligent Device Runtime 206 and the Mediator service 500 using the message set definitions 600. The larger part of this management burden can be borne by the device framework 206. The Device Runtime 206 is primarily responsible for managing the Message Set 600 and relationships, and correlating received messages 331 to prior originating messages 330. The Mediator Service 500, for example, splits the web service 106 request into the asynchronous exchange of messages 330,331 with the device 10, if needed, and associates the correlation information of the message set 600 between related messages 330,331.

Device Runtime Modules

The runtime environment 206 can have a Message Correlation Service 602 responsible for enforcing the rules of the Message Set 600, correlating outgoing asynchronous messages 330

BNSDOCID: <WO____2005083934A1_I_>

to incoming asynchronous messages 331 to a single mapped data instance as per the data definitions 314 of the message set 600. Subsystems of the service 602 can include a message Decoder 604 for converting Communication Service 608 message protocol (i.e. for incoming messages 331) into internal operable message format of the device 100 where needed, an Encoder 606 for converting internal message representation of the device 100 into format required to support protocol of the Communication Service 608 (i.e. for outgoing messages 330), and the Message Manager 610 for performing the correlation of messages 330,331 to a data instance as used by the application 302 and utilizes a message envelope of the messages 330,331 to carry the correlation Id 324a. The runtime environment 206 can also have a Data Persistence Manager 612 that persists and provides access to all instances of Data components 400 defined by the application 302. The Persistence Manager 612 permits resolution of a data instance by a key field data value 324a. It is recognised that the data instances mentioned are instantiated versions of the data definition 314 as utilised by the device 100 during operation of the application 302 as a result of direct or indirect interaction with the web service 106. A UI Service 614 provides interaction with the user of the device interface 202 (see Figure 2) via visualization of screen definitions 404 (of the application 302), knows when a user action corresponds to changes in underlying data, and knows when a particular user action results in interaction with the associated web service (e.g. sends the message 330). It is also recognised that the Communication Service 608 can provide an over the air (OTA) interface of the device 100.

For example, one scenario is for the Communication Service 608 to use a synchronous mechanism to transmit messages 330,331 to the Mediator Service 500 or the web service 106 directly (not shown), and can offer a synchronous listener interface for arriving messages from the mediator 500 or web service 106. As such the Communication Service 608 can provides a device facing asynchronous messaging mechanism to device applications 302, i.e. provide synchronous messaging 330,331 between the mediator 500 or web service 106 while providing asynchronous messaging internally of the device 100 with the message manager 610. a second scenario is for the communication service 608 to act as a simple messaging network 20 interface for the device 100 and therefore transfer asynchronous messages 330,331 outgoing and incoming with respect to the device 100.

BNSDOCID: <WO____2005083934A1_I_>

Mediator Service Modules

When utilized as a proxy between asynchronous and synchronous environments, the mediator service 500 can have a Synchronous Dispatcher module 614 for performing the messaging 332 interaction with the synchronous web service 106. The Synchronous Dispatcher 614 maintains the correlationId 324a between the arriving device message 330 and the departing device message 331. The Synchronous Dispatcher 614 is able to detect when the message 330 has arrived and is sitting at an Async Receiver 616, which receives and queues arriving device message 330 envelopes. On receipt of the message 330, the receiver 616 releases the connection (i.e. returns immediately to the device 100). As well, The Synchronous Dispatcher 615 is able to detect when the message 332 has arrived from the web service 106 and forwards the appropriate message 331 to an Async transmitter 618, which initiates the outgoing connection to the device 100, passes the outgoing message 331envelope with correlation Id 325a as received from the web service 106. Finally, an optional Decoder 620 for transforming the incoming device message 330 into an internal operable format that can be utilized by the Synchronous Dispatcher 615 for submission to the webservice 106, and an optional Encoder 622 for transforming the web service 106 result data (e.g. data element 325b) into the outgoing device message 331from an internal operable format.

Message Set and Mediator Service Operation

This section describes the interactions between the device runtime 206 and the web service 106 to satisfy asynchronous messaging in the context of a Pizza Shop order process example. Referring to Figure 6, the following steps can be performed such as but not limited to:

1. In response to user interaction with a screen of the user interface 202, the Screen Service 614 updates a data element associated to the screen, i.e. the device Runtime generates the Order data element based the interaction with the application 302 user;
2. The Screen Service 614 detects via application metadata of the message set 600 that a rule indicating that the message 330 is sent on update of this data item. The Screen Service 614 requests the Message Manager 610 to send the appropriate message 330, and supplies the data instance (e.g. data definition 314) required to allow message creation;

BNSDOCID: <WO_____2005083934A1_I_>

3. The Message Manager 610 examines the Message Set 600 definitions of the application 302, and determines that the message 330 requested in 1 is part of the Message Set 600. The key field 324a of mapped data is determined from the message set 600 definition (e.g. link 440 – see figure 4) and this value is reserved as the *correlationId* 324a;
4. The Message Manager 610 passes the data instance and outgoing message metadata definition 600 to the Encoder module 604. The Encoder module 604 takes the internal metadata representation of the message 330, and the provided values, and generates the message 330 supporting the protocol of the Communication Service 608, such that the device Runtime 206 generates the outPlaceOrder message330 from the Order data definitions 314 using mapping instructions in the Message Set 600. The outPlaceOrder message can contain the *id* 324a, *user*324b and *special* 324c fields derived from the Order *orderId*, *userId* and *specialName* fields of the data definition 314 as specified in the message set 600. The Device Runtime 206 detects that the orderId 324a represents the key field of the data element representing the data definition 314 and includes a token in the outPlaceOrder message 330 envelope that distinguishes this field as the correlation id 324a;
5. The Message Manager 610 adds the *correlationId* 324a to the envelope of the encoded message 330 request. The entire envelope is passed to the Communication Service 608 for delivery to the Mediator Service 500, if used, otherwise directly to the web service 106;

6. The Communication Service 608 initiates a connection to the Mediator Service Async Receiver 616 (or directly to the web service 106) and passes the message 330. The Async Receiver 616, if used, returns immediately to the Communication Service 608. Accordingly, the Device Runtime 206 transmits the outPlaceOrder message 330 to the Mediator Service 500, if used, which detects the correlation id 324a of the message 330;

Where Mediator synchronous request handling is used

7. The Mediator Service Synchronous Dispatcher 615 detects that the message 330 has arrived from the device 100. The message 330 is picked up from the Async Receiver 616;

BNSDOCID: <WO____2005083934A1_I_>

8. The Synchronous Dispatcher 615 obtains the *correlationId* 324a from the message 330 envelope and passes the message 330 data to the Decoder 620 to obtain the message content;
9. The Synchronous Dispatcher 615 initiates a synchronous request 332, for example, to the web service 106 with the data obtained in step 8. The Mediator Service 500 initiates the synchronous request 332 to the web service 106 using the outPlaceOrder parameters 324a,b,c, where the field 324b can identify the user and/or device 100 and/or application 302 originating the message 330. the field 324c can be a data value sent to the web service 106 as generated by the application 302. The web service 106 processes the information 324a,b,c of the message 330 and immediately returns a result 325a,b. The web service response 332 is returned in the same cycle as the request 332;
10. The Synchronous Dispatcher 615 passes the response data to the Encoder 622 to produce the required device response message 331. The Synchronous Dispatcher 615 adds the *correlationId* 325a to the envelope of the message 331 in response to the data received from the web service 106. The Mediator Service 500 therefore obtains the result 325a,b and generates the orderConfirmation message 331. The correlation id 325a is embedded in the envelope of the orderConfirmation message 330 as well as any data 325b (e.g. an update to the data element deliverytime of the data definition 314. The Mediator Service 500 transmits the message 331asynchronously/synchonously to the Device Runtime 206; and
11. The message 331 is passed to the Async Transmitter 618 which...
12. Calls the device 100 passing the message 331. The device 100 returns to the Mediator service 500 immediately.

It is recognised that in the above given mediator example that the web service could be substituted in the mediator's 500 stead, where the web service 106 would be responsible for placing the id 325a in the message 331 as per the expected shared definitions of the message set 600. At the device 100, further steps:

Device 100 asynchronous message reception and handling

BNSDOCID: <WO____2005083934A1_I_>

13. The device Communication Service 608 passes the received message 331 to the Message Manager 610. The Message Manager 610 obtains the *correlationId* 325a from the envelope of the message 331;
14. The Message Manager 610 passes the message 331 to the Decoder 606 which converts the message 331 into an internal operable representation if needed;
15. The Message Manager 610 queries the Message Set 600 definitions and determines that the received message 331 belongs to a particular set as per the id 325a. The Message Manager 610 determines the Data instance to which incoming messages apply. The Device Runtime 206 receives the orderConfirmation message 330 and detects that this message is part of the Pizza Order message set 600; and
16. The Message Manager 610 resolves the data instance using the *correlationId* 325a as the id value, and updates the data instance according to mapping rules described in the Message Set 600. It extracts the correlation id 325a, resolves the underlying data element (Order) in view of field element 325b and applies the orderConfirmation mappings to this instance.

Application Program 302

Referring to Figure 8, a block diagram of the component application program 302 comprises the data layer 400, the presentation layer 402 and the message layer 404, which are coordinated by workflow layer 406 through communications 214 with the client runtime environment 206. The structured definition language can be used to construct the definitions 314,316,320 of the layers 400, 402, 404 as a series of metadata records, which consist of a number of pre-defined elements representing specific attributes of a resource such that each element can have one or more values. Each metadata schema typically has defined characteristics such as but not limited to; a limited number of elements, a name of each element, and a meaning for each element. Example metadata schemas include such as but not limited to Dublin Core (DC), Anglo-American Cataloging Rules (AACR2), Government Information Locator Service (GILS), Encoded Archives Description (EAD), IMS Global Learning Consortium (IMS), and Australian Government Locator Service (AGLS). Encoding syntax allows the metadata of the layers 400, 402, 404 to be processed by the device infrastructure 204 (see Figure 2), and encoding schemes include such as but not limited to XML, HTML, XHTML,

BNSDOCID: <WO_____2005083934A1_I_>

XSML, RDF, Machine Readable Cataloging (MARC), and Multipurpose Internet Mail Extensions (MIME). The client runtime environment 206 can operate on the metadata descriptors of the layers 400, 402, 404 to provision an executable version of the application program 302. It is recognised that the layers 402 and 406 can be provided by other means for the application 302, such as but not limited to native code and other defined execution languages. The application 302 can make use of the data 400 and message 404 layers to implement mappings 318 (see Figure 3) between fields of the definitions 314,316,320 to help correlate asynchronous messaging 105 between the device 100 and the web service 106.

Referring again to Figure 8, the data layer 400 defines data entities (definitions 314) which are used by the application program 302. Examples of data entities which the data layer 400 may describe are orders, users, and financial transactions. The Data layer 400 defines what information is required to describe the data entities, and in what format the information is expressed. For example, the data layer 400 may define such as but not limited to an order which is comprised of a unique identifier for the order which is formatted as a number, a list of items which are formatted as strings, the time the order was created which has a date-time format, the status of the order which is formatted as a string, and a user who placed the order which is formatted according to the definitions 314 of the data layer 400.

Referring again to Figure 8, the message layer 404 defines the format of messages 105 used by the application program 302 to communicate with external systems such as the web service 106. For example, one of the message definitions 316 may describe such as but not limited to a message for placing an order which includes the unique identifier for the order, the status of the order, and notes associated with the order.

It is noted that the use of layers 402 and 406 may be optional for the application 302.

Referring again to Figure 8, the optional presentation layer 402 defines the appearance and behavior of the application program 302 as it displayed by the user interface 202. The presentation layer 402 can specify GUI screens and controls, and actions to be executed when the user interacts with the application 302 using the user interface 202. For example, the presentation

BNSDOCID: <WO_____2005083934A1_I_>

definitions 320 may define screens, labels, edit boxes, buttons and menus, and actions to be taken when the user types in an edit box or pushes a button. The majority of Web Service 106 consumers use a visual presentation of Web Service 106 operation results, and therefore provide the runtime environment 206 on their devices 100 capable of displaying user interface screens.

Referring to Figures 1 and 8, it is recognized that in the above described client application program 302 definitions hosting model, the presentation layer 402 may vary depending on the client platform and environment of the device 100. For example, in some cases Web Service consumers do not require a visual presentation. The application definitions 314,316,320,322 of the application program 302 can be hosted in a Web Service registry as a bundle of platform-neutral data 400, message 404, workflow 406 layer descriptors with a set of platform-specific presentation layer 402 descriptors for various predefined client runtimes 206 (see Figure 2). When the discovery or deployment request message 105 is issued the client type should be specified as a part of this request message 105. In order not to duplicate data, message, and workflow metadata while packaging application programs 302 for different client platforms of the communication devices 100, application definitions 314,316,320,322 can be hosted on the web service 106 (for example) as a bundle of platform-neutral component definitions 314,316,322 linked with different sets of presentation definitions 320. When a user makes a discovery or download request message 105, the client runtime type of the communication devices 100 is validated and the proper bundle is constructed for delivery by the web service 106 to the device 100 over the network 102, 104. For those Web Service 106 consumers, the client application programs 302 would contain the presentation layer 402 linked with the data 400 and message 404 layers through the workflow layer 406. It is recognized that the hosting model includes message 404 and data 400 layers with the remainder of the application functionality (presentation and workflow) expressed in a manner that cooperates with these defined layers 400, 404, such as but not limited to native code and other defined components as desired.

Referring again to Figure 8, the optional workflow layer 406 of the application program 302 defines processing that occurs when an action is to be performed, such as an action specified by a presentation layer 402 as described above, or an action to be performed when messages 105

BNSDOCID: <WO_____2005083934A1_I_>

(see Figure 1) arrive from the system 20. Presentation, workflow and message processing are defined by the workflow layer 406. The workflow layer 406 can be written as a series of instructions in a programming language or a scripting language, such as but not limited to ECMAScript, and can be compiled into native code and executed by the runtime environment 206, as described above. An example of the workflow layer 406 content may be to assign values to data, manipulate screens, or send the message 105. As with presentation layer 402, multiple workflow definitions 322 can be created to support capabilities and features that vary among devices 100. The appropriate workflow definition can be determined and sent at the time of downloading and provisioning of the application program 302.

ECMA (European Computer Manufacturers Association) Script is a standard script language, wherein scripts can be referred to as a sequence of instructions that is interpreted or carried out by another program rather than by the computer processor. Some other example of script languages are Perl, Rexx, VBScript, JavaScript, and Tcl/Tk. The scripting languages, in general, are instructional languages that are used to manipulate, customize, and automate the facilities of an existing system, such as the devices 100. In such systems, useful functionality is already available through the user interface 202 (see Figure 2), and the scripting language is a mechanism for exposing that functionality to program control. In this way, the device 100 is said to provide a host runtime environment of objects and facilities which completes the capabilities of the scripting language.

Specifically, EMCAScript is an object-oriented programming language for performing computations and manipulating computational objects within the host runtime environment. ECMAScript can be used as a Web scripting language, providing a mechanism to perform service 106 computation as part of the Web-based client-server architecture of the system20(see Figure 2). ECMAScript provides core scripting capabilities for a variety of host runtime environments, and therefore the core scripting language can be considered platform neutral for a number of particular host runtime environments. The runtime environment 206 (see Figure 2) can provide the ECMAScript host runtime environment for client-side computation of the communication devices 100, such as but not limited to; objects that represent windows, menus, pop-ups, dialog boxes, text areas, anchors, frames, history, cookies, and input/output. Further,

BNSDOCID: <WO____2005083934A1_I_>

the host runtime environment of the runtime environment 206 provides a means to attach scripting code to events such as but not limited to change of focus, page and image loading, unloading, error, and abort, selection, form submission, and mouse actions. In implementations using ECMA scripting, the code appears within the workflow layer 406, combines user interface elements and fixed and computed text and images, and is reactive to user interaction on the user interface 202. The web service 106 (see Figure 1) provides a different host environment for server-side computation including objects representing requests, clients, and files, and mechanisms to lock and share data. By using the client side and server side scripting together, it is possible to distribute computation between the client communication devices 100 and the service 106 while providing a customized user interface 202 for the Web-based application programs 302.

ECMAScript also defines a set of built-in operators which may not be, strictly speaking, functions or methods. ECMAScript operators include such as but not limited to various unary operations, multiplicative operators, additive operators, bitwise shift operators, relational operators, equality operators, binary bitwise operators, binary logical operators, assignment operators, and the comma operator. ECMAScript syntax resembles Java syntax, however, ECMAScript syntax is relaxed to enable it to serve as an easy-to-use scripting language for developers. For example, a variable in ECMAScript is not required to have its type declared nor are types associated with properties, and defined functions are not required to have their declarations appear textually before calls to them. It is recognized that in a class-based object-oriented programming language, in general, state is carried by instances, methods are carried by classes, and inheritance is only of structure and behavior. In ECMAScript, the state and methods are carried by objects, and structure, behavior, and state are all inherited.

Application Program 302 Example

Accordingly, referring to Figure 8, the client application programs 302 can be defined as a set of platform-neutral component definitions 314,316, namely for data 400 and message 404 layers, and the optional presentation layer 402 using XML (or any other suitable structured definition language). The optional workflow layer 406 can be defined using ECMAScript (or any other suitable platform-neutral scripting language). The client runtime environment 206 (see

BNSDOCID: <WO_____2005083934A1_I_>

Figure 2) can generate component templates based on meta-definitions when the definitions 314,316,320,322 of the application program 302 are provisioned on the communication device 100. With a large variety of terminal runtime environments 206, the cross-platform standards such as XML or ECMAScript can be used to define application component metadata instead of pre-building the application programs 302. This delayed binding can allow the generic application definitions of the component application programs 302 to be run on a wide variety of terminal system environments 206, represented by various different communication devices 100.

The following example shows how a Web Services client application program 302 could be expressed using a structured definition language, such as but not limited to XML, and a platform neutral scripting/programming language, such as but not limited to ECMAScript, with defined components conforming with the following Document Type Definition (DTD):

```
<!ELEMENT wcApp (desc?, iconUrl?, res*, wcData*, wcMsg*, style*, wcScr*, wcFlow)>
<!ATTLIST wcApp
        name CDATA #REQUIRED
        title CDATA #IMPLIED
        vendor CDATA #IMPLIED
        version CDATA #IMPLIED
        transportKey CDATA #IMPLIED
        installNotifURL CDATA #IMPLIED
        registerURL CDATA #IMPLIED
>
<!ELEMENT desc (#PCDATA)>
<!ELEMENT iconUrl (#PCDATA)>
<!ELEMENT res (#PCDATA)>
<!ATTLIST res
        name CDATA #REQUIRED
        url CDATA #REQUIRED
        type (xml | image | sound | any) #REQUIRED
        deferred (true | false) "false"
>
```

Example Data definitions 314

```
<!ELEMENT wcData (dfield+)>
<!ATTLIST wcData
        name CDATA #REQUIRED
        persisted (true | false) "true"
>
<!ELEMENT dfield (#PCDATA)>
<!ATTLIST dfield
        name CDATA #REQUIRED
        type (String | Number | Boolean | Date | Any) "Any"
        array (true | false) "false"
```


BNSDOCID: <WO____2005083934A1_I_>

```
        cmp (true | false) "false"
        cmpName CDATA #IMPLIED
        key (0 | 1 | 2) "0"
    >
    Example Message definitions 316
    <!ELEMENT wcMsg (mfield*)>
    <!ATTLIST wcMsg
        name CDATA #REQUIRED
        mapping CDATA #IMPLIED
    >

    <!ATTLIST wcMsg
        pblock CDATA #IMPLIED
    >
    <!ELEMENT mfield (#PCDATA)>
    <!ATTLIST mfield
        name CDATA #REQUIRED
        type (String | Number | Boolean | Date | Array | XML) #IMPLIED
        mapping CDATA #IMPLIED
    >

    Example Presentation definitions 320
    <!ELEMENT wcScr (layout?, menu?, refresh?, event?)>
    <!ATTLIST wcScr
        name CDATA #REQUIRED
        title CDATA #IMPLIED
        main (true | false) "false"
        dialog (true | false) "false"
        param CDATA #IMPLIED
    >
    <!ELEMENT style (font?)>
    <!ATTLIST style
        name CDATA #REQUIRED
        bgColor CDATA #IMPLIED
    >
    <!ELEMENT font EMPTY>
    <!ATTLIST font
        name CDATA #REQUIRED
        color CDATA #IMPLIED
        size CDATA #IMPLIED
        bold (true | false) "false"
        italic (true | false) "false"
        underline (true | false) "false"
    >
    <!ELEMENT refresh (msg+)>
    <!ELEMENT msg (#PCDATA)>
    <!ELEMENT layout (layout*, label*, separator*, edit*, image*, choice*, button*, textarea*)>
    <!ATTLIST layout
        type (grid | flow | border | vertical) #REQUIRED
        param CDATA #IMPLIED
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
    >
    <!ELEMENT menu (item*)>
    <!ELEMENT item (action, condition?)>
    <!ATTLIST item
```


BNSDOCID: <WO_____2005083934A1_I_>

```
        name CDATA #REQUIRED
        label CDATA #REQUIRED
        shortcut CDATA #IMPLIED
>
<!ELEMENT action EMPTY>
<!ATTLIST action
        screen CDATA #IMPLIED
        pblock CDATA #IMPLIED
        param CDATA #IMPLIED
        acceptChanges (true | false) "true"
>
<!ELEMENT condition EMPTY>
<!ATTLIST condition
        pblock CDATA #REQUIRED
        param CDATA #IMPLIED
        result (true | false) "true"
>
<!ELEMENT event EMPTY>
<!ATTLIST event
        type (onInit | onClick | onChange | onFocusOut) "onInit"
        pblock CDATA #IMPLIED
        screen CDATA #IMPLIED
        param CDATA #IMPLIED
>
<!ELEMENT separator EMPTY>
<!ELEMENT label (condition?, event?)>
<!ATTLIST label
        name CDATA #REQUIRED
        value CDATA #REQUIRED
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT edit (condition?, event?)>
<!ATTLIST edit
        name CDATA #REQUIRED
        value CDATA #IMPLIED
        mapping CDATA #IMPLIED
        type (char | number | date | pwd | phone | email) "char"
        readOnly (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT textarea (condition?, event?)>
<!ATTLIST textarea
        name CDATA #REQUIRED
        value CDATA #IMPLIED
        mapping CDATA #IMPLIED
        readOnly (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT image (condition?, event?)>
<!ATTLIST image
        name CDATA #REQUIRED
        resName CDATA #REQUIRED
        placement CDATA #IMPLIED
```


BNSDOCID: <WO____2005083934A1_I_>

```
>
<!ELEMENT choice (condition?, event?, entry*)>
<!ATTLIST choice
        name CDATA #REQUIRED
        value CDATA #IMPLIED
        mapping CDATA #IMPLIED
        type (singleList | multiList | dropdown | checkbox | radio) "singleList"
        readOnly (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT entry (#PCDATA)>
<!ELEMENT button (condition?, event?)>
<!ATTLIST button
        name CDATA #REQUIRED
        label CDATA #REQUIRED
        image (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
```

Example Workflow definitions 322

```
<!ELEMENT wcFlow (pblock+)>
<!ELEMENT pblock (#PCDATA)>
<!ATTLIST pblock
        id CDATA #REQUIRED
        param CDATA #IMPLIED
>
```

As given above, the XML elements define the example component application 302 including a wcApp element, a wcData element, a wcMsg element, a wcSrc element, and a wcFlow element. Referring to Figure 8, the wcApp element is a top-level element which defines the application program 302. The wcData element defines the example data layer 400, which is comprised of a group of named, typed fields. The wcMsg element defines the example message layer 404, which similarly defines a group of named, typed fields. The wcSrc element defines the example presentation layer 402. The example presentation layer 402 is a label, a separator, an image, a button, an edit field, a text area, a single-selection list, a multi-selection list, a drop-list, a checkbox, a radio button, or a screen containing a group of other presentation definitions 320.

Referring to the above example component application program 302 and Figure 8, the wcFlow element defines the example workflow layer 406. The pblock attributes of the XML elements specify a pblock element nested in the wcFlow element. Each pblock element comprises script which defines part of the workflow of the application program 302. The script is

BNSDOCID: <WO_____2005083934A1_I_>

written in ECMAScript. In order to define the behavior of the application 302, the optional workflow layer 406 uses ECMAScript to reference and manipulate the data layer 400, the presentation layer 402, and the message layer 404. The workflow layer 406 can also reference external object types, which allow actions to be performed on the components defined in the application 302. For example, a wcMsg type allows a message defined by a message definition 316 to be evaluated to determine whether mandatory fields have been supplied, and to be sent to an external system such as the web service 106. A wcData type allows the size of collections of data entities defined by data definition 314 to be determined, and allows data entities to be deleted. A wcScr type allows a presentation definition 320 to be displayed to the user. Similarly, a special dialog external object allows a message to be displayed to the user on the user interface 202 (see Figure 2).

BNSDOCID: <WO____2005083934A1_I_>

WE CLAIM:

1. A system for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the system comprising:

a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier;

a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

2. The system of claim 1, wherein the first identifier is configured for insertion in the request message by the mobile device and the second identifier is configured for insertion in the response message by the data source.

3. The system of claim 1 further comprising a communication service for providing a communication interface between the message manager and the network.

4. The system of claim 3, wherein the communication manager is configured to provide communication of the messages between the communication manager and the message manager asynchronously.

BNSDOCID: <WO_____2005083934A1_I_>

5. The system of claim 4, wherein the communication manager is configured to provide communication of the messages between the communication manager and the network asynchronously.

6. The system of claim 2 further comprising a screen service for initiating the message request based on a user data event from a user interface of the device.

7. The system of claim 6, wherein the message manager is configured for querying the message correlation set to determine if the data corresponding to the user event is defined by the message correlation set as the first data parameter.

8. The system of claim 7, wherein the message manager is configured to select the first correlation identifier of the message correlation set corresponding to the identified first data parameter as part of the message correlation set.

9. The system of claim 6 further comprising a persistence manager for resolving the persistence of the first data parameter value according to the first correlation identifier.

10. They system of claim 2, wherein the message correlation set is described in a structured definition language.

11. A method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the method comprising the steps of:

sending an asynchronous request message of the communication messages;

receiving an asynchronous response message of the communication messages;

linking the asynchronous request message with the corresponding asynchronous response message by employing a message correlation set including a set of correlation definitions, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the

BNSDOCID: <WO_____2005083934A1_I_>

asynchronous response message when received, the first identifier different from the second identifier;

associating a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

12. The method of claim 11, wherein the first identifier is configured for insertion in the request message by the mobile device and the second identifier is configured for insertion in the response message by the data source.

13. The system of claim 11 further comprising the step of providing a communication interface between a message manager and the network.

14. The system of claim 13, wherein the communication interface is configured to provide communication of the messages between the communication interface and the message manager asynchronously.

15. The system of claim 14, wherein the communication interface is configured to provide communication of the messages between the communication interface and the network asynchronously.

16. The system of claim 12 further comprising the step of initiating the message request based on a user data event from a user interface of the device.

17. The system of claim 16 further comprising the step of querying the message correlation set to determine if the data corresponding to the user event is defined by the message correlation set as the first data parameter.

BNSDOCID: <WO____2005083934A1_I_>

18. The system of claim 17 further comprising the step of selecting the first correlation identifier of the message correlation set corresponding to the identified first data parameter as part of the message correlation set.

19. The system of claim 16 further comprising the step of resolving the persistence of the first data parameter value according to the first correlation identifier.

20. They system of claim 12, wherein the message correlation set is described in a structured definition language.

21. A computer program product for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the computer program product comprising:

a computer readable medium;

a message correlation set module stored on the medium and configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier;

a message manager module for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set module, the first and second data parameters also part of the message correlation set as data definitions.

BNSDOCID: <WO_____2005083934A1_I_>

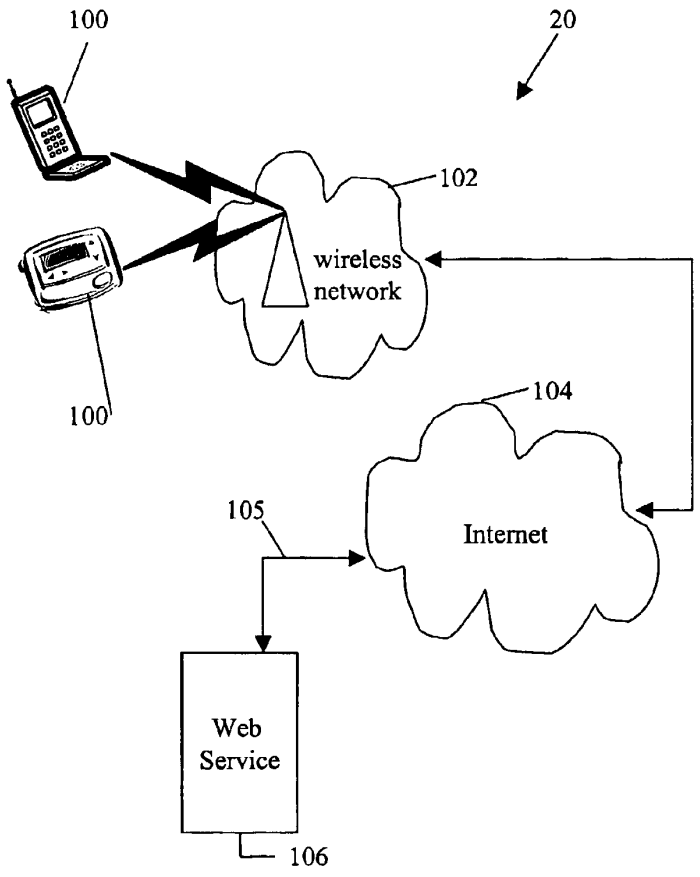


Figure 1

BNSDOCID: <WO_____2005083934A1_I_>

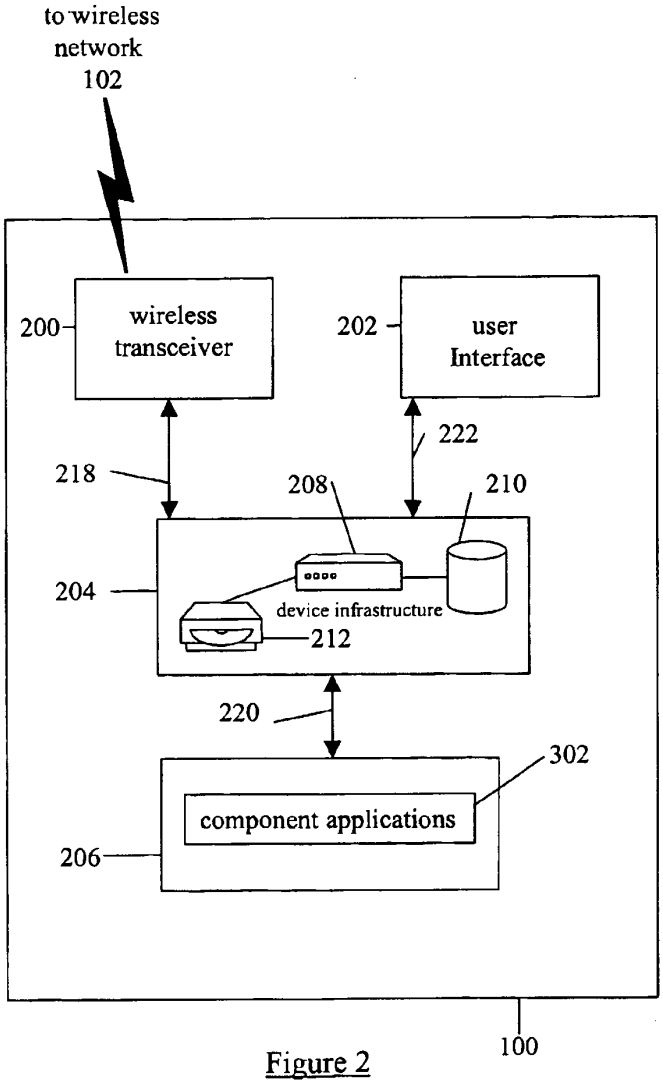


Figure 2

BNSDOCID: <WO____2005083934A1_I_>

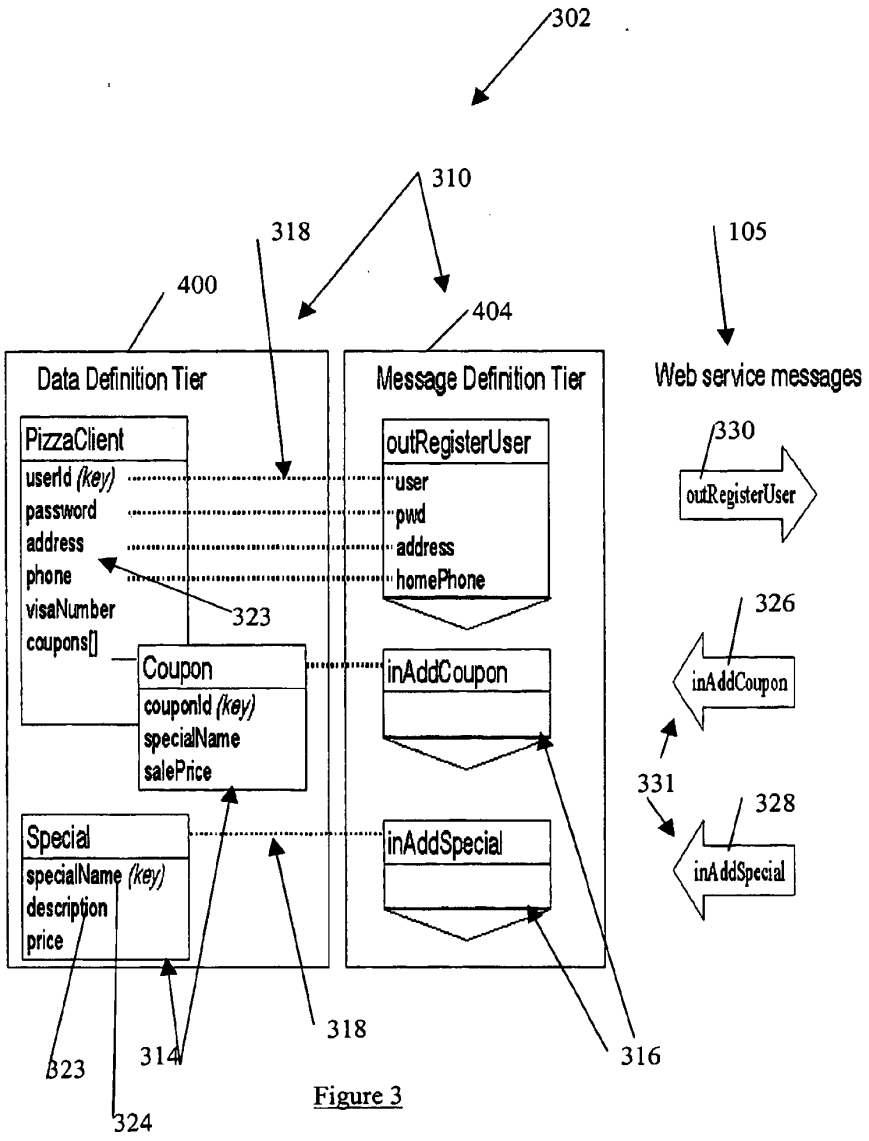


Figure 3

BNSDOCID: <WO_____2005083934A1_I_>

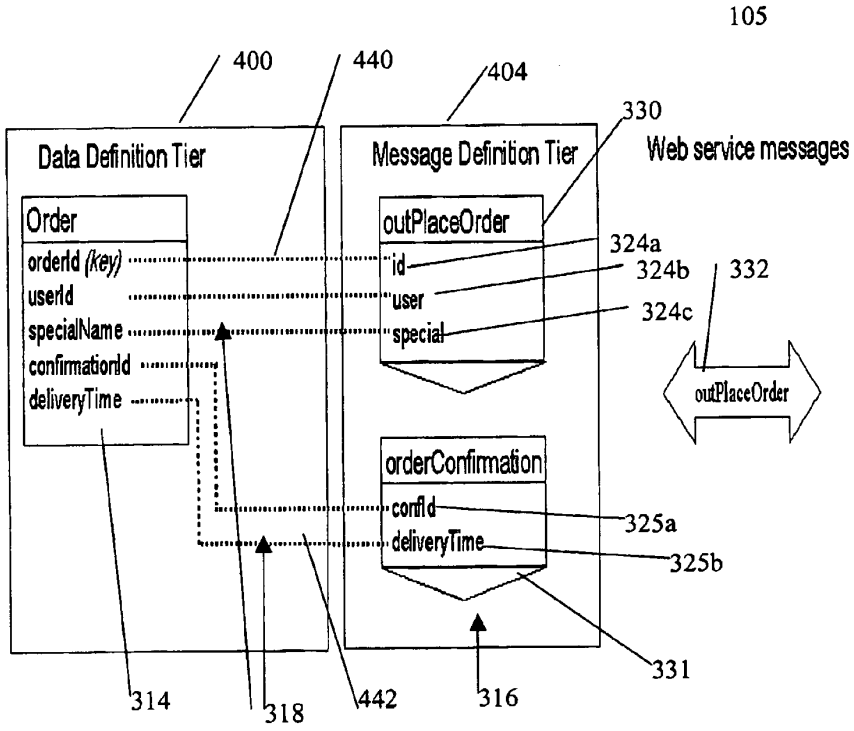


Figure 4

BNSDOCID: <WO_____2005083934A1_I_>

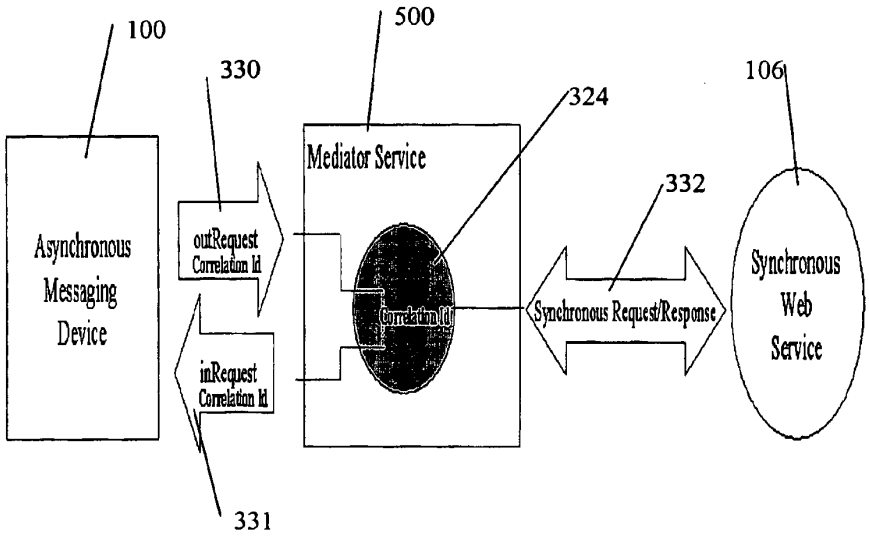


Figure 5

BNSDOCID: <WO_____2005083934A1_I_>

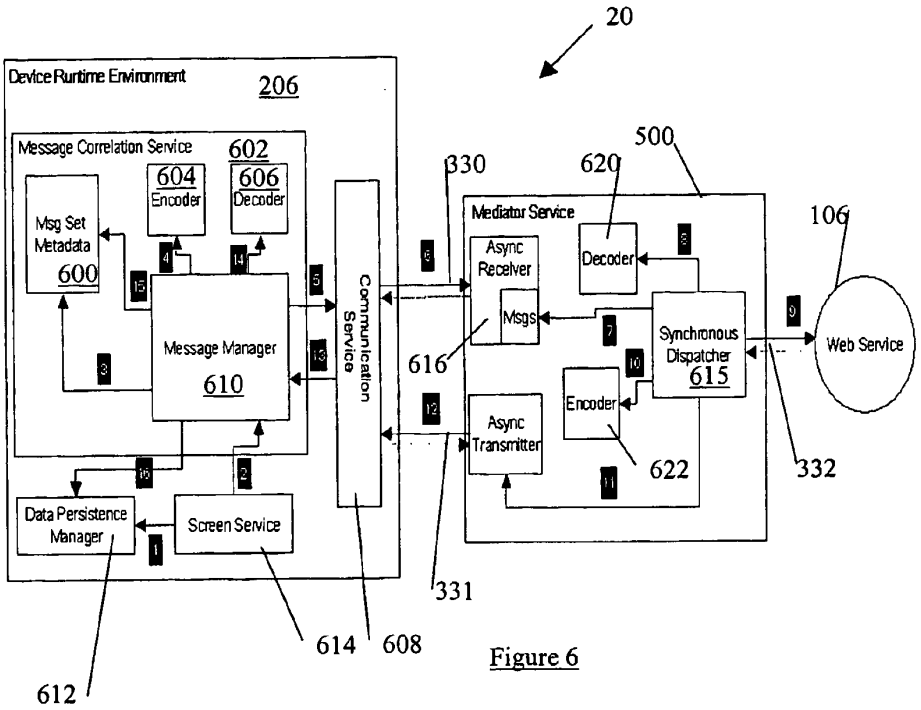


Figure 6

BNSDOCID: <WO_____2005083934A1_I_>

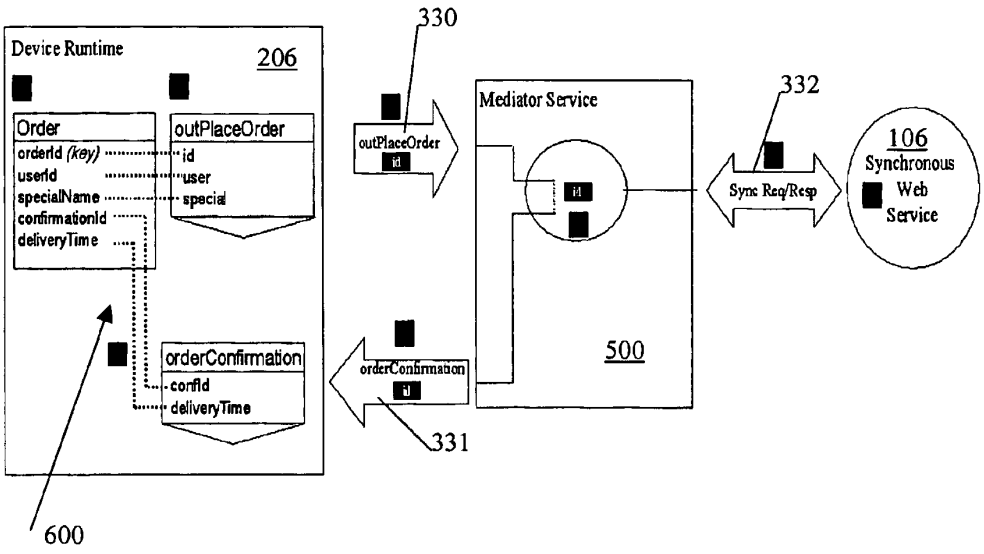


Figure 7

BNSDOCID: <WO_____2005083934A1_I_>

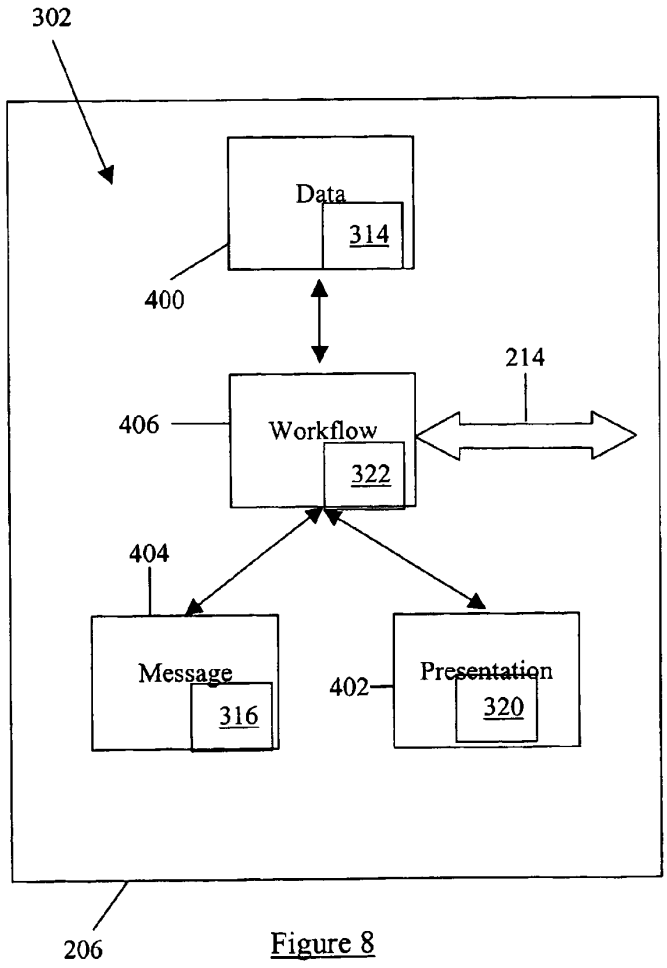


Figure 8

BNSDOCID: <WO_____2005083934A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000286

A. CLASSIFICATION OF SUBJECT MATTER
IPC7 H04L 12/16, H04Q 7/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC7 H04L 12/16, H04Q 7/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database - Search Terms used: web, service, asynchronous, mobile, device,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/0023127 (SABETI) 21.02.2002	1-21
A	US 2003/0206192 (CHEN et al.) 06.11.2003	1-21
A, P	US 2004/0255046 (RINGSETH et al.) 16.12.2004	1-21
A	US 6,035,324 (CHANG et al.) 07.03.2000	1-21
A, P	WO 2004/066081 (CHEENATH) 05.08.2004	1-21

[ ] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 June 2005 (08-06-2005)	5 July 2005 (05-07-2005)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Donald Lefebvre (819) 997-2822

BNSDOCID: <WO_____2005083934A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CA2005/000286

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US6035324	07-03-2000	GB2330502 A	21-04-1999
		JP11134277 A	21-05-1999
		SG71145 A1	21-03-2000
		SG97884 A1	20-08-2003
		TW463112 B	11-11-2001
		US6035324 A	07-03-2000
US2002023137	21-02-2002	DE10030521 A1	17-01-2002
		EP1168761 A2	02-01-2002
		US2002023137 A1	21-02-2002
US2003206192	06-11-2003	AU2002367759 A1	22-09-2003
		EP1430412 A1	23-06-2004
		US2003206192 A1	06-11-2003
		WO03077139 A1	18-09-2003
US2004255046	16-12-2004	US2004255046 A1	16-12-2004
WO04066081	05-08-2004	WO04066081 A3	07-04-2005
		US20040143645 A1	22-07-2004

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2007 (25.10.2007)

PCT

(10) International Publication Number
WO 2007/120310 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/061532

(22) International Filing Date:
1 December 2006 (01.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/742,155 1 December 2005 (01.12.2005) US
11/394,782 31 March 2006 (31.03.2006) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LIOY, Marcello** [CA/US]; 11629 Miro Circle, San Diego, California 92131 (US). **DYCK, Jeffrey** [CA/US]; 4816 Mt. Harris Drive, San Diego, California 92117 (US).

(74) Agents: **WADSWORTH, Philip R.** et al.; 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

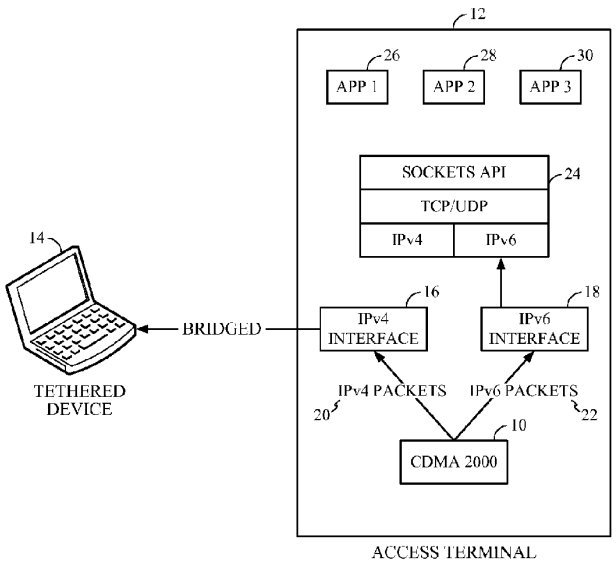
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: CONCURRENT INTERNET PROTOCOL CONNECTIVITY TO AN ACCESS TERMINAL AND A TETHERED DEVICE



(57) Abstract: Using split interfaces for Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4), and bridging the IPv4 interface, makes it possible to support a Tethered Device (TD) and an Access Terminal (AT) having concurrent IP connectivity. This configuration enables the support of IP Multimedia Subsystem (IMS) applications in the AT using IPv6 while concurrently supporting general Internet usage on a TD. It is also possible to bridge an IPv6 interface to the TD.

WO 2007/120310 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONCURRENT INTERNET PROTOCOL CONNECTIVITY TO AN ACCESS TERMINAL AND A TETHERED DEVICE

Claim of Priority under 35 U.S.C. §119

[0001] The present Application for Patent claims priority to Provisional Application No. 60/742,155 entitled "Method For Supporting Concurrent IP Connectivity To An Access Terminal And Tethered Device Each Using Different IP Protocols In CDMA 2000 Networks," Filed December 1, 2005, and assigned to the assignee hereof and hereby expressly incorporated by reference herein.

BACKGROUND

Field

[0002] The present disclosed embodiments relates generally to cellular communications, and more specifically to concurrent Internet Protocol (IP) connectivity to an Access Terminal (AT) and a Tethered Device (TD).

Background

[0003] It is desirable to support one Internet Protocol (IP) protocol to an Access Terminal (AT) and another to a Tethered Device (TD). An example of where this is desirable is with the launch of the new IP Multimedia Subsystem (IMS) services, which will provide a rich set of new Multimedia services in the mobile environment. One of these services will the Voice over IP (VoIP), which will replace traditional circuit switched voice, which is how voice services are supported today. In order to support these IMS services, an AT must be continuously connected to the IP Network, which is also known as "always-on." Typically in the case for Code Division Multiple Access (CDMA) 2000 networks this implies that it is not possible to support a TD as the AT is already in a data session.

[0004] There is therefore a need in the art for concurrent IP connectivity to an AT and a TD.

SUMMARY

[0005] Using split interfaces for Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4), and bridging the IPv4 interface, makes it possible to support a TD and

an AT having concurrent IP connectivity. This configuration enables the support of IMS applications in the AT using IPv6 while concurrently supporting general Internet usage on a TD. It is also possible to bridge the IPv6 interface to the TD.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is an illustration of a concurrently connected Access Terminal and Tethered Device.

DETAILED DESCRIPTION

[0007] The embodiments described herein make it possible to provide service concurrently to the AT and TD. Different IP protocol versions can be used by the AT and TD. In the case of IMS, it is desirable to use IP version 6 (IPv6) for the AT in order to be always on an assigned IP for as long as the AT is powered on. In order to support a wide scale deployment of these services, it would require as many IP addresses as there are ATs. In the case of IPv4 there is a dearth of addresses, so IPv6 is preferred for the AT.

[0008] For most general Internet services, such as web browsing and email, still use IP version 4 (IPv4). Thus for the TD it is desirable to have IPv4 connectivity.

[0009] The embodiments described below with reference to FIG. 1 describe how to provide IPv6 in the AT while concurrently supporting IPv4 to a TD. However, the same technique could be used to provide IPv4 to the AT and IPv6 to the TD.

[0010] IP packets arriving over an air interface 10 and based on an IP version are received by an AT 12 and are either forwarded up an AT stack 24 (for example, IPv6 packets 22) or forwarded to a TD 14 (for example, IPv4 packets 20).

[0011] There are a variety of ways this could be done:

[0012] 1. Examine the incoming packets and apply the forwarding as described in the paragraph above.

[0013] 2. Use the notion of Network Interfaces, which provide an abstraction layer, between the physical layer (in this case the CDMA2000 air interface data protocols, such as Radio Link Protocol (RLP) and Point-to-Point Protocol (PPP)) and the generic IP stack above (commonly referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite). This is described in more detail below.

[0014] The use of the Network Interface can provide a variety of processing options with respect to IP packets passing through them, such as filtering and routing/bridging information.

[0015] It is possible in the interface itself to identify whether or not packets should be forwarded directly to another interface without processing them further. This further processing is typically done at the IP layer, and consists of routing. Routing is the act of examining the IP addresses in the header and determining if the packet is destined for the local host, which is the device doing the routing, or another host. Typically if it is intended for another host, a determination may need to be made over which link to transmit it – if there are multiple links. If the interface is configured to directly forward the packets to another interface (or link), this is referred to as bridging the two interfaces together. This is typically used when it is known that all of the packets arriving in one interface must be transmitted over another interface, regardless of the addressing information they contain. An example of this is a Wireless LAN bridge. Any packets arriving on the Ethernet interface must be forwarded over the WLAN interface without exception.

[0016] In an AT it is desirable to have separate network interfaces for IPv4 and IPv6 as there is much information for each protocol that is independent, but needs to be duplicated, such as the state of the interface (disabled, available, configuring, etc.), IP address(es), and so forth.

[0017] Using the properties of bridging and the separation of the IPv6 and IPv4 interfaces allows an IPv4 interface 16 to be set up in bridging mode such that it forwards all IPv4 packets 20 to the TD, while leaving an IPv6 interface 18 in non-bridged mode, which results in the IPv6 packets 22 being delivered to the IP stack 24, and the payload ultimately being delivered to the IMS application. This allows IPv6 IMS applications 26, 28, and 30 on the AT 12 to work concurrently with generic IPv4 Internet applications on the TD 14.

[0018] Using this split interface/bridging solution, it is also possible to run IPv6 addresses on the TD 14 while supporting IPv4 applications on the AT 12.

[0019] When it becomes desirable to support IPv6 applications on the TD 14 as well, because the IPv6 packets are going to the IP layer 24 they could be routed to the TD as well if they are not destined for the AT 12, but rather for the TD. This would allow

both IPv4 and IPv6 applications on the TD running concurrently with IPv6 applications running on the AT.

WHAT IS CLAIMED IS:

CLAIMS

1. An Access Terminal for having concurrent Internet Protocol Activity with a Tethered Device, the Access Terminal comprising:

an Internet Protocol stack;

a first Internet Protocol version interface adapted in a non-bridged mode for delivering first Internet Protocol version packets to the Internet Protocol stack; and

a second Internet Protocol version interface adapted in a bridged mode for delivering second Internet Protocol version packets to the Tethered Device.

2. The Access Terminal of claim 1 wherein the first Internet Protocol version interface is an Internet Protocol version 6.

3. The Access Terminal of claim 2 wherein the second Internet Protocol version interface is an Internet Protocol version 4.

4. The Access Terminal of claim 1 wherein the first Internet Protocol version interface is an Internet Protocol version 4.

5. The Access Terminal of claim 4 wherein the second Internet Protocol version interface is an Internet Protocol version 6.

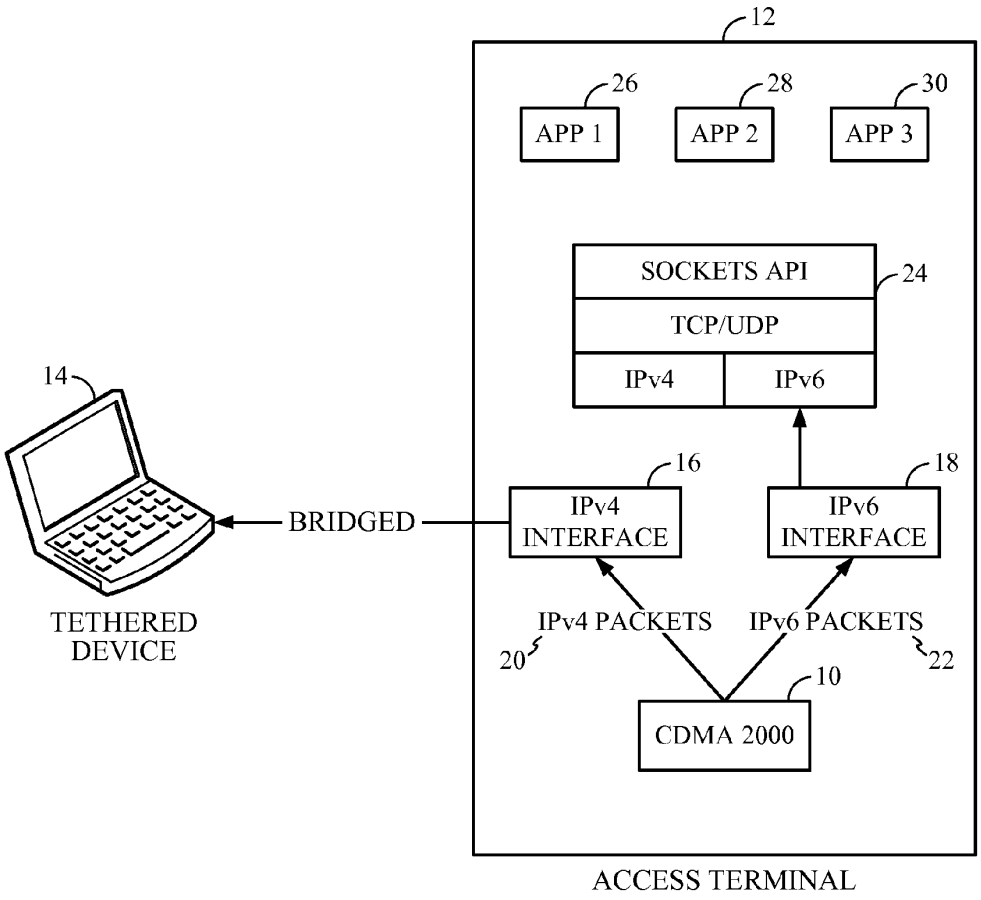

12
26
28
30
APP 1
APP 2
APP 3
SOCKETS API
24
TCP/UDP
IPv4
IPv6
14
16
18
IPv4
INTERFACE
IPv6
INTERFACE
BRIDGED
TETHERED
DEVICE
IPv4 PACKETS
IPv6 PACKETS
20
22
10
CDMA 2000
ACCESS TERMINAL

FIG. 1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017063 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/26556

(22) International Filing Date: 21 August 2002 (21.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/313,968 21 August 2001 (21.08.2001) US

(71) Applicant *(for all designated States except US)*: **APOGEE NETWORKS** [US/US]; 1455 Broad Street, 4th Floor, Bloomfield, NJ 07003 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LEUNG, Yiu, Kau** [US/US]; 5 Knob Hill Road, Morganville, NJ 07751 (US). **PRICE, John, Davis** [US/US]; 5 Ashland Court, Colts Neck, NJ 07722 (US). **FEINBERG, Brion** [US/US]; 51 Amagansett Drive, Morganville, NJ 07751 (US).

(74) Agents: **DUNNAM, Michael, P.** et al.; Woodcock Washburn LLP, One Liberty Place, 46th Floor, Philadelphia, PA 19103 (US).

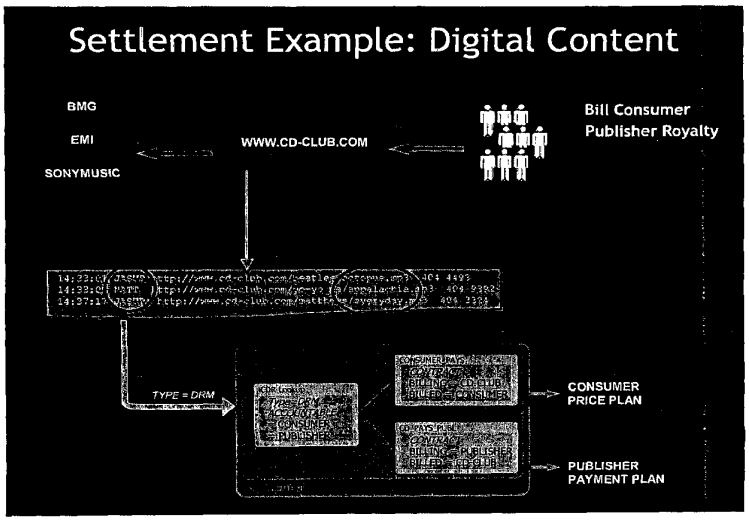
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SETTLEMENT OF TRANSACTIONS SUBJECT TO MULTIPLE PRICING PLANS____



(57) Abstract: The invention includes a method, system, and computer-readable medium having computer-executable instructions for rating a transaction. The inventive method includes processing a transaction, where the transaction is processed when a service is provided from a service provider to a service consumer, accessing via a computer network multiple pricing plans related to the transaction, and rating the transaction in accordance with the multiple pricing plans. The method further may include receiving output states from at least one pricing plan. The rating may be accomplished within one pricing plan, or within a group of pricing plans.

WO 03/017063 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SETTLEMENT OF TRANSACTIONS SUBJECT TO MULTIPLE PRICING PLANS

Cross Reference to Related Applications

This application claims priority under 35 U.S.C. § 119 (e) from provisional application no. 60/313,968 filed August 21, 2001. The provisional application 60/313,968 is incorporated by reference herein, in its entirety, for all purposes.

Technical Field

The invention relates generally to the processing of data, and more particularly to efficiently and generically aggregating data available on a communication network and billing/paying multiple parties for access to the content of the aggregated data.

Background of the Invention

Recently, the collection and processing of data transmitted over communication networks, like the Internet, has moved to the forefront of business objectives. In fact, with the advent of the Internet, new revenue generating business models have been created to account for the consumption of content received from a data network (*i.e.*, content-based billing). For example, content distributors, application service providers (ASPs), Internet service providers (ISPs), and wireless Internet providers have realized new opportunities based on the value of the content that they deliver. As a result of this content-billing initiative, it has become increasingly important to resolve intelligently and flexibly the corresponding transactions according to the business needs of the customer.

Often, even in traditional commerce streams, there are many different participants between the maker and the consumer of the good. Some of these so-called "middlemen" simply may facilitate access to the good, while others may add useful characteristics to the good. This is especially true in a distributed network environment, like the Internet, that impose additional burdens on capturing the

transaction process because of the unlimited number of data sources and the correspondingly unlimited number of data types. As a result, adequately describing the transacting of the goods and services in such an environment, or even across any of the traditional environments requires a technique that is capable of understanding and processing the participants and the various types of data.

To date, resolving the characteristics of a transaction has been accomplished over data-specific environments using certain application-specific (*i.e.*, "non-generic") methods. For example, a typical telephone bill captures the characteristics of a voice-based telecommunications transaction. In particular, the participants may be identified as the party initiating the call (*i.e.*, the "calling party" telephone number), the party receiving the call (*i.e.*, the "called party" telephone number), and one or more parties connecting the communication (*i.e.*, the "local" or "long distance carrier"). This simple example adequately captures all of the necessary aspects of the telephone call to properly account for the transaction by requiring payment from certain parties (*e.g.*, the calling and/or the called party) to certain other parties (*e.g.*, the local and/or long distance carrier). While these "hard-coded" transaction resolution techniques are sufficient to accommodate only specific environments involving well-defined participants, they are correspondingly too rigid to efficiently satisfy the ever-changing face of a communication network like the Internet. Also, these "hard-coded" techniques are too specific to operate across the many and varied transaction environments that exist throughout the business world.

Therefore, there exists a need to provide a flexible technique that can capture and resolve transactions of any type and involving any participants without requiring modification of the technique for each type. Such a technique would serve to accommodate multi-faceted network environments like the Internet, as well as to provide a single solution that would apply to any business environment.

Summary of the Invention

The invention includes a method, system, and computer-readable medium having computer-executable instructions for rating a transaction. The inventive

method includes processing a transaction, where the transaction is processed when a service is provided from a service provider to a service consumer, accessing via a computer network multiple pricing plans related to the transaction, and rating the transaction in accordance with the multiple pricing plans. The method further may include receiving output states from at least one pricing plan. The rating may be accomplished within one pricing plan, or within a group of pricing plans. Also, accessing the multiple pricing plans may be accomplished via interconnected building blocks located within each of the pricing plans. The method also may include a revenue fold that summarizes the output of multiple pricing plans, including child and parent accounts. Selection of the appropriate child accounts may be a function of end dates that are within a parent account's time period. The method further may pool revenue/usage data as a function of billing cycles, and update the pooled revenue/usage data by summing the values of data from selected account plan periods. Values of the pooled revenue/usage data may be obtained via a building block. The inventive method also may determine a commission, wherein the commission is a credit given to an account.

Brief Description of the Drawings

Other features of the invention are further apparent from the following detailed description of the embodiments of the invention taken in conjunction with the accompanying drawings, of which:

Figure 1 is a block diagram of a system for analyzing content transmitted over a communication network, according to the invention;

Figure 2 is a block diagram further describing the components of the system described in Figure 1;

Figures 3A and 3B provide a flow diagram further detailing the operation the system described in Figure 1;

Figure 4 provides a block diagram of the system described in Figure 1, providing greater detail of a configuration and operation of a transaction layer;

Figures 5A and 5B provide a flow diagram of a method for identifying the characteristics of a transaction, according to the invention;

Figure 6 is a block diagram further detailing the operation and configuration of the transaction layer, according to the invention;

Figure 7 is a flow diagram that details the operation and configuration of the transaction layer of transaction layer, according to the invention;

Figure 8 illustrates a sample settlement scenario for settling the fees associated with the download of certain content;

Figure 9 illustrates a general system description of settlement technologies useful in accordance with the invention to accommodate multiple aggregation of usage, multiple ownership of content, and multiple settlement options;

Figure 10 illustrates a settlement example for digital music downloaded by a consumer from an on-line music club that implements a pricing plan to the consumer and a publisher payment plan using the settlement techniques of the invention;

Figure 11 illustrates a transaction pricing usage based settlement model for use in settling low volume, high value transactions;

Figure 12 illustrates a billing cycle pricing, usage based settlement model for use in settling high volume, low value transactions;

Figure 13 illustrates a revenue sharing settlement using folds in accordance with a first embodiment of the invention;

Figure 14 illustrates a revenue sharing settlement using revenue/usage pools in accordance with a second embodiment of the invention;

Figure 15 illustrates a revenue pool contribution example for the embodiment of Figure 14;

Figure 16 illustrates a revenue pool accessor example for the embodiment of Figure 14;

Figure 17 illustrates a revenue sharing settlement using commissions in accordance with a third embodiment of the invention;

Figure 18 provides an example of computing revenue fold;

Figure 19 illustrates how accounts and pools with different billing cycles contribute to and access from pool instances; and

Figure 20 provides an example of how an account with billing period ending will get one commission from account.

Detailed Description of the Invention

System Overview

Figure 1 is a block diagram of a system 100 for analyzing content transmitted over a communication network. Although the following description will be discussed in the context of collecting, processing and billing for data transmitted over the Internet, it should be appreciated that the invention is no so limited. In fact, the invention may be applied to any type of network, including a private local area network, for example. Also, the invention may be used for purposes other than billing for the usage of content. For example, the invention may be used to analyze the type of data transmitted over a particular network, or to determine the routing patterns of data on a network. Furthermore, the invention may be used to facilitate the intelligent collection and aggregation of data relevant to a particular industry. In addition, the invention may be used to track specific Internet protocol (IP) network resources and to detect fraud, for example.

In addition, it should be appreciated that the term "content" may be defined as data that is transmitted over the network. In the context of the Internet, content may include .mp3 files, hypertext markup language (html) pages, videoconferencing data, and streaming audio, for example. The terms "content provider" and "customer" will be used throughout the description as well. Content provider may refer to the primary creator or provider of the content, while customer is the primary recipient of the content. Both the producer and customer may be a human or a computer-based system.

As shown in Figure 1, an instrumentation layer 101 provides raw data to a content collection layer 102. Instrumentation layer 101 may consist of various data sources, for example, network routers. The network routers may provide information

regarding the various types of routed data, including for example, data format, originating Internet protocol (IP) address, and destination IP address. One example of such information is Cisco System's NetFlow™.

Content collection layer 102 collects information about the delivery of the content, as well as the substance of the content itself. Content collection layer 102 also may sort, filter, aggregate, and store the content according to the particular needs of the end user. In effect, content collection layer is responsible for extracting meaningful information about IP traffic, and so it is provided with an understanding of the data sources in instrumentation layer 101. Content collection layer 102 also may transform the data from the plurality of sources in instrumentation layer 101 into standard formats for use in a transaction layer 103.

Content collection layer 102 is in communication with transaction layer 103. Generally, content collection layer 102 reports to transaction layer 103 that a relevant communication event has occurred and should be considered by the remainder of system 100. A communication event may be defined as any transfer of data between systems. Transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 is in communication with a settlement layer 104. Settlement layer 104 captures the operations that are necessary to understand the significance of the transaction defined by transaction layer 103. For example, settlement layer 104 may rate a particular transaction by assigning a monetary value to the transaction. Settlement layer 104 also may divide the burdens and benefits of the monetary value among the relevant parties. In this way, settlement layer 104 ensures that certain parties receive a particular portion of the payment made by the other parties. Settlement layer 104 also may be responsible for delivering this burden and benefit information to the appropriate parties with the appropriate identifiers (*e.g.*,

account numbers). As will be explained in more detail below, the present invention is directed to operations of the settlement layer 104.

Figure 2 is a block diagram further describing the components of system 100. As shown in Figure 2, instrumentation layer 101 includes data sources 201-203 that each provide raw data 204-206, respectively, to collection layer 102. As discussed, data sources 201-203 may include various internetworking devices like routers, bridges, and network switches. Data sources 201-203 provide raw data to an input data adapter 207. Accordingly, input data adapter 207 understands the operation of and the data provided by data sources 201-203. Although one input data adapter is shown in Figure 2, it should be appreciated that more than one input data adaptermay be used in system 100. For example, each data source may have a dedicated input data adapter.

Input data adapter 207 understands the incoming data and extracts the data into the appropriate fields. This field-delimited data, called flow objects 208, are sets of attributes. The attributes may be any characteristics that are provided by, or can be derived from, raw data 204-206 provided by data sources 201-203, respectively. For example, flow objects 208 may include a set of attributes describing the source and destination, including source IP address, destination IP address, source interface, and destination interface. Because input data adapter 207 is charged with understanding raw data 204-206 from data sources 201-203, as well as the required flow objects 208 of system 100, it is capable of transforming the raw data to the flow objects, where the flow objects may all be of a standard format.

Input data adapter 207 provides flow objects 208 to a content data language 209. Content data language 209 may transform the attributes in flow objects 208 into other attributes that are desired by a particular customer. For example, content data language 209 may derive a network identifier attribute that is not readily available from a data source, from a source address attribute and a destination address attribute that are provided by flow object 208 attributes from input data adapter 207. This derivation may be based on a customer's desire to determine which network conveyed the transaction between the source and the destination. Therefore, following this

example, content data language 209 will know to extract the source address attribute and the destination address attribute from flow objects 208.

Content data language 209 may perform other functions as well. For example, content data language 209 may perform a generic lookup function 219 that is built into content data language 209. Generally, generic lookup 219 describes a technique for mapping any number of attributes to any number of other derived attributes. For example, generic lookup 219 may be used to map a unique resource locator (URL) attribute to a particular content-type attribute.

Content data language 209 also is in communication with a correlator 211. Generally, correlator 211 connects the many daily network content events from various network devices, like routers for example. Often, the connected data may come from distinctly different data sources at distinctly unrelated times. Correlator 211 allows this data to be intelligently connected to each other, regardless of how different the sources or of how disparate the time received. For example, a Netflow™ enabled router and a Radius™ enabled network access switch may each provide certain data that is relevant to one particular transaction. However, because portions of the data come from different devices, the data may arrive at system 100 at different times, and in different formats. Also, because each provides data that is necessary to complete one transaction, the data from each cannot be considered separately. Correlator 211 allows this data to be intelligently grouped regardless of the format of the data or of the time the data pieces are received.

Furthermore, correlator 209 may rearrange the order of the received flow objects 208 to suit the needs of the remainder of system 100. By performing such correlation without having to first store all of the data on a disk (*e.g.*, a database), significantly faster processing is achieved. Correlator 209 may perform this correlation in real-time, for example.

Although system 100 has been described using content data language 209 and correlator 211, it should be appreciated that flow objects 208 may proceed directly to a filter 212, if no correlation is required and if no attribute derivation is required, for example. Filter 212 analyzes flow objects 208 to ensure that the provided attributes

are desired by system 100. If flow objects 208 are not needed (*i.e.*, a mismatch), filter 212 may prevent flow objects 208 from passing to an aggregator 213. Also, although filter 212 has been shown as a separate device in system 100, it should be appreciated that the functionality of filter 212 may be incorporated into aggregator 213.

Filter 212 passes the matching flow objects to aggregator 213. Aggregator 213 may provide additional filtering and classification of the multitude of daily network content transactions, based on user criteria. Aggregator 213 may perform such filtering and classification in real-time. Aggregator 213 provides the filtered and classified information to an output data adapter 214. Output data adapter 214 may convert the data from aggregator 213 into one or more content detail records for storage in CDR database 215. Therefore, CDR database 215 stores a complete description of a content event.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 passes the CDR onto ownership resolution component 216. A proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. These tasks are accomplished by ownership resolution component 216 and transaction resolution component 221.

Ownership resolution component 216 serves to define the participants of the communication event. In particular, because raw data 204-206 may not provide sufficient "ownership" data relating to the parties involved in the content transaction, such "ownership" data must be provided by system 100 to properly account for the entire transaction. Ownership resolution component 216 operates to provide such ownership-based data to system 100.

Ownership resolution component 216 is in communication with transaction resolution component 221. Transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content.

Such predetermined relationships may be previously agreed upon by the participants, or may be created and agreed upon with the implementation of system 100. Therefore, transaction component 103 understands the nature of the parties, the actions that one or more parties perform, and the influence of such action on the respective parties.

Transaction component 216 provides the transaction information to a rating component 217. Rating component 217 provides a weight or significance (*e.g.*, a price) to the transaction, so as to provide a tangible value to the transaction. Rating component 217 may make this determination based on various metrics including the type of the content, the quantity of content consumed, the place and time delivered, or the quality of the content, for example. Therefore, rating component 217 allows system 100 to provide some contextual value, indicting the significance or relevance that certain content or information has to the individual customer.

Rating component 217 provides the rated transaction to a presentment component 218. Presentment component 218 may provide the capability for a customer 220 to view their real-time billing information, for example, over the network. Presentment component 218 also may attach relevant identifiers to the bill (*e.g.*, account numbers, etc.).

Figures 3A and 3B provide a flow diagram further detailing the operation 300 of system 100. As shown in Figure 3A, in step 301, raw data 204-206 is received from data sources 201-203. In step 302, input data adapter 207 converts raw data 204-206 to flow objects 208, where flow objects 208 are sets of attributes, determined from raw data 204-206. In step 303, it is determined whether there is a need to derive new attributes from the existing attributes found in flow objects 208. If there is such a need, in step 304, CDL 209 is used to derive new attributes from existing attributes. Also, as discussed above, attributes may be correlated by correlator 211.

In step 305, flow objects 208 are filtered by filter 212. In step 306, the matching flow objects (*i.e.*, those passed by filter 212) are further filtered and classified by aggregator 213. In step 307, output data adapter 214 converts the data aggregated by aggregator 213 to a format compatible with transaction layer 103.

As shown in Figure 3B, in step 308, output adapter 214 may format the aggregated data into one or more content data records for storage in CDR database 215. In step 309, ownership resolution component 216 identifies the parties involved in the transaction. In step 310, transaction resolution component 221 captures the predetermined agreements among the parties, as well as the value added by each of the individual parties. In step 311, the CDR is rated based on predetermined metrics (*e.g.*, time of transmission, quality of content). In step 312, a bill is presented to the customer.

Content Transaction Layer

A transaction, including a business transaction for example, may be any activity between two or more participants that affects certain parties. The affected parties may be considered the participants to the transaction, although parties and participants may be mutually exclusive entities. It should be appreciated that the terms "parties" and "owners" may be used interchangeably throughout. Also, a transaction may include one or more events, where an event may be some action (*e.g.*, the transfer of a service or good) that the participants conduct with each other. Such events may be the exchange of data over a communication network, for example. Also, it should be appreciated that the same event or action may take place in any direction (*e.g.*, from party A to party B or from party B to party A). The "subject" of the action is the party who performs the activity, while the "object" of the action is the party who is affected or influenced in any way by the action.

Transaction layer 103 is responsible for capturing the characteristics of the transaction, including the parties, participants, subject, object, event/action type, direction of the action, for example. The scope of the characteristics captured by transaction layer 103 will vary with the nature of instrumentation layer 101, the capability of content collection layer 102, and the requirements of settlement layer 104. Generally, transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of

the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 is a data store that holds each CDR for further processing by ownership resolution component 216 and transaction resolution component 221. In the context of a billable electronic business transaction, a proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. As discussed, ownership resolution component 216 serves to define the participants of the communication event, while transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216.

Transaction layer 103 is generic in that it operates without requiring an understanding of instrumentation layer 101 and content collection layer 102. Instead, transaction layer 103 takes the relevant characteristics of the transaction provided by instrumentation layer 101 and content collection layer 102, and selects and generates those characteristics required by settlement layer 104.

Although the operation of transaction layer 103 will be described in the context of an electronic event over a communication network for the purposes of billing for the event, it should be appreciated that the invention is not so limited, but is so described the purpose of clarity. For example, it should be appreciated that the invention may include functions other than billing, including security, network capacity planning, and content monitoring, for example. Also, the generic techniques described may be applied beyond the context of an electronic event over a communication network.

Figure 4 provides a block diagram of system 100 providing greater detail of the configuration and operation of transaction layer 103. As shown in Figure 4, content collection layer 102 provides a usage record 401 to transaction layer 103. A series of fields 403-408 comprise usage record 401. Although fields 403-408 will be

identified by certain labels for the purpose of clarity, it should be appreciated that fields 403-408 may identify any of the many possible characteristics of the transaction.

In the example provided by Figure 4, fields 407 and 408 identify the parties or participants to the transaction. In particular, field 407 identifies "User A" and field 408 identifies "User B." User A may be the subject party and User B may be the object party. For example, in the context of a telecommunication event, User A may be the "calling" party and User B may be the "called" party. Field 405 and field 406 identify a measurable quantity of the event. In particular, following the example of the telecommunications event, field 405 identifies a duration (in minutes) of the event and field 406 identifies the quantity of data exchanged during the event (in megabytes). Field 403 and field 404 may identify a "start time" and an "end time," respectively, of the communication event.

Although fields 403-408 provide just one example, in any case, it should be appreciated that user record 401 will include certain characteristics provided by instrumentation layer 101 and/or derived by content collection layer 102. These characteristics typically are provided to transaction layer 103 because they have some particular significance to identifying the characteristics necessary to allow settlement layer 104 to provide some accounting of the transaction. Therefore, usage record 401 may not necessarily include all of the characteristics provide by instrumentation layer 101 and/or derived by content collection layer 102, because certain characteristics may not relevant to the settlement of the transaction (*e.g.*, network type). Yet, usage record 401 will include those available characteristics that pertain to permitting settlement layer 104 to properly account for the transaction.

Once usage record 401 passes through transaction layer 103, a modified usage record 402 may be provided to settlement layer 104. Modified usage record 402 may be modified by transaction layer 103 to include additional details of the transaction event required by settlement layer 104 and/or required by the customer's system to which the usage record applies (*e.g.*, a usage billing system). As shown for modified usage record 402, an account A field 409 and an account B field 410 may be added to

further identify the transaction. In one example, account A field 409 may include an alphanumeric designator that identifies the account number that has been assigned by the customer's billing system for User A. In the context of the telecommunications system, account A field 409 may hold User A's ten-digit home telephone number, for example.

In any case, the components of transaction layer 103 operate to identify these additional fields, based on the requirements of the customer's system and of settlement layer 104. In particular, ownership resolution component 216 operates to ensure that the necessary participants or parties to the transaction are identified, while transaction resolution component 221 operates to ensure that the relationships among the parties or participants are identified.

Identification of the relevant entities and their relationships may be accomplished using "lookups" in data stores located within ownership resolution component 216 and transaction resolution component 221, for example. For example, a data table may have a "User" data field and an associated "Account" data field. When User A is received by ownership resolution component 216, it will conduct a lookup in the data table and identify Account A as the appropriate account associated with User A. Also, transaction resolution component 221 may have a data table that permits a lookup of the relationship between User A and User B, identified in usage record 401. For example, upon receiving field 407 designating User A and field 408 designating User B, transaction resolution component 221 may conduct a lookup of an algorithm that identifies the appropriate burdens and benefits (*e.g.*, debit and credit of money) assigned to each of the users with respect to each other.

It also should be appreciated that transaction layer 103 may not provide additional characteristics to usage record 401, as described but may select the relevant characteristics (*i.e.*, those characteristics needed by settlement layer 104) from the characteristics made available by instrumentation layer 101 and/or derived by content collection layer 102. In fact, usage record 401 may include all of the necessary characteristics to properly account for the transaction. In this case, ownership resolution component 216 and transaction resolution component 221 select the

relevant characteristics from the available characteristics. As will be explained in more detail below, the information added to the usage record 402 may also constitute pricing plans and the settlement layer may be configured to handle more sophisticated settlement strategies involving multiple parties and multiple pricing plans over a multiplicity of noncontiguous time periods.

Figures 5A and 5B provide a flow diagram of a method 500 for identifying the characteristics of a transaction using system 100. As shown in Figure 5A, in step 501, raw data 204-206 is received into system 100. Raw data 204-206 includes certain characteristics provided by data sources 201-203, respectively, in instrumentation layer 101. In step 502, content collection layer 102 processes (*e.g.*, aggregates, correlates and filters) raw data 204-206. In step 503, content collection layer 102 provides the processed data to CDR database 215 in transaction layer 103. CDR database 215 stores the data for further processing by transaction layer 103.

In step 505, it is determined whether the contents of the data provided to transaction layer 103 already include the needed ownership data. If the data includes the needed ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507. If, on the other hand, the data provided to transaction layer 103 does not already include the needed ownership data, the required data is identified (*e.g.*, using database lookups) by ownership resolution component 216, in step 506. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507.

As shown in Figure 5B, in step 508 it is determined whether the contents of the data provided to transaction layer 103 already include the needed relationship data (*i.e.*, data defining the burdens and benefits encountered by the parties/participants to the transaction). If the data includes the needed relationship data, the relevant data is selected by transaction resolution component 221 and provided to settlement layer 104, in step 510. If, on the other hand, the data provided to transaction layer 103 does not already include the needed relationship data, the required data is identified (*e.g.*,

using database lookups) by transaction resolution component 221, in step 509. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 510.

Ownership and Transaction Resolution

Figure 6 is a block diagram further detailing the operation and configuration of transaction layer 103. It should be appreciated that elements described for transaction layer 103 are not exclusive, but provide just one example of a configuration for transaction layer 103. In particular, the functionality of the previously described ownership resolution component 216 and transaction resolution component 221 will be described in greater detail in the various components described with reference to Figure 6. In practice, however, it should be appreciated that transaction layer 103 may comprise of any number of components that ensure that the necessary parties to a transaction are identified generically.

As shown in Figure 6, transaction layer 103 includes a configuration repository 601, a configuration database 610, a configuration manager 603, and a fail over detector 604. In addition, transaction layer 103 includes a transaction layer engine 608 in communication with configuration repository 601, configuration manager 603, and fail over detector 604.

Transaction layer engine 608 includes a rules processor 605, a CDR reader 606, and a transaction writer 607. Transaction layer engine 608 processes raw data 204-206 in usage record 401 and creates a modified usage record 402, based upon the requirements of settlement layer 104. It should be appreciated that there may be more than one transaction layer engine 608 for each transaction layer 103. However, a single transaction layer engine 608 is shown for the purpose of clarity and brevity.

CDR reader 106 understands the nature of the transaction and operates to read a particular usage record 401 stored in CDR database 215. CDR reader 106 then submits usage record 401 to rules processor 605. Rules processor 605 applies rules (*e.g.*, written in XML) to usage record 401 so as to determine ownership and the relationships among the ownership, for each individual usage record 401. Rules

processor 605 may then generate one or more modified usage records 402, based on the application of the rules to usage record 401. Once rules processor 605 generates the modified usage record 402, transaction writer 607 operates to write a transaction (based on the modified usage record 402) to CDR database 215. Modified usage record 402 is then used by settlement layer 104 to further process the transaction (*e.g.*, rate the transactions monetarily).

Fail over detector 604 operates to provide fault tolerance and initiate a fail over engine (not shown) for a failed transaction layer engine, in accordance with one or more mathematical algorithms, the discussion of which is beyond the scope of the invention. Configuration manager 603 provides an external interface to transaction layer 103 using a business editor 609. Business editor 609 may be manipulated by a user or customer using a graphics user interface (GUI). In particular, the GUI of business editor 609 receives commands from a user and translates them into actions to be performed on usage record 401, for example, by rules processor 605. Configuration repository 601 operates to provide an abstraction to configuration database 610. Configuration database 610 may be a relational database or a set of extensible markup language (XML) computer-readable files, for example.

Figure 7 is a flow diagram that details the operation of transaction layer 103, as shown in Figure 6. As discussed, it should be appreciated that multiple transaction engines may be used to implement a process. Where the invention is instituted using computer-readable instruction, transaction layer engine 608 may be implemented as a computer-executable instruction or thread. Therefore, multiple transaction layer engines may be implemented by having multiple computer-readable instructions.

In step 701, transaction layer engine 608 reads usage record 401 using CDR reader 606. In step 702, rules processor 605 applies one or more rules to usage record 401 read by CDR reader 606, so as to determine one or more "accountables." Accountables are labels that are used to facilitate identifying the parties or owners to a transaction. Accountables may be defined and/or modified by an external user (*e.g.*, a customer) using the graphical user interface provided by business editor 609. Also, it should be appreciated that accountables may be defined for a new usage types for

which no rules in rules processor 605 are provided. The identification of accountables is the function of ownership resolution component 216, as described with reference to Figure 4.

In step 703, "contracts" are identified that define the relationships or agreements between one or more accountables. In the context of a billing system, a contract identifies which parties pays (*i.e.*, the billed party) and which party receives payment (*i.e.*, the billing party). A particular contract may be identified and executed when one or more "conditions" are satisfied. The identification of contracts is conducted by transaction resolution component 221, as described with reference to Figures 2 and 4. A condition is an expression of a logical assertion that can be evaluated as true or false. In transaction layer 103, for example, a condition may be true if a certain data element is present and false if the data element is not present. The following is an example of a condition in XML:

```
<condition name="condition1" function="IsPresent" outcome="true"
type="Accountable" id="ColoProvider"/>
```

In step 704, once the contracts are determined, they are executed. In step 705, usage record 401 is changed to modified usage record 402 based upon the execution of the contract and the identification of the accountables. In step 706, modified usage record 402 may be written to a data table using transaction writer 607, so that settlement layer 104 can rate it, in step 707. Therefore, a transaction may be represented as modified usage record 402, where modified usage record may include the elements of usage record 401 in addition to the accountable and contract elements (*e.g.*, fields 409-410 as discussed with reference to Figure 4).

Although the discussion provided an example of a single contract and two accountables for a single usage record, it should be appreciated that many contracts and many accountables (*i.e.*, and therefore many "transactions") may be derived from a single usage record, because there may be multiple transactions implicated from a single usage record 401. For example, usage record 401 may involve three parties

each having a contract with the other respective parties. In this example, therefore, there may be three separate contracts for a single usage record 401, and three individual accountables for each party or owner. Moreover, as will be explained below, the contracts may operate according to pricing plans that vary over time and from party to party.

In addition to requiring a certain accountable, it may be necessary to determine a value of the accountable. For example, transaction layer 103 may determine not only that the "called party" accountable be a part of the transaction, but also that a value for the called party (*e.g.*, "856-555-1212" or "John Doe") be identified. Also, it may be necessary to transform one accountable into another accountable to satisfy the requirement of settlement layer 104. For example, settlement layer 104 may require the called party accountable (either determined by transaction layer 103 or provided in usage record 401) be transformed into a network identifier accountable.

In either case, the value or transformation of accountables or contracts may be determined using certain predetermined functions or "primitives." A primitive defines a transformation or a valuation of an accountable or contract. As discussed, transformations may allow a value of an accountable to be determined using another accountable, for example. Primitives define and direct such transformations. The input to a primitive can be one of fields 403-408 from usage record 401 or a previously determined accountable, for example.

Primitives may be described and distinguished based on their prescribed functionality. For example, one type of primitive may be a database lookup. A database lookup is a primitive that operates to transform one accountable or contract to another accountable or contract. Also, a database lookup primitive may function to assign a value to an accountable or contract, as a result of conducting a lookup of the accountable or contract in a database. It should be appreciated that the database lookup primitive also allows flexibility in that any database that has Java Database Connectivity (JDBC) drivers (*e.g.*, Oracle, Microsoft SQL Server, Sybase, Database 2) can be used to perform complex lookups. In this way, therefore, previous

accountable or contact transformations can be linked to find new accountables or contracts, respectively.

Other types of primitives may include direct value assignment, and a function primitive that looks up data in an external database. Other primitives may include a function primitive that it allows a third party based library (*e.g.*, Java-based) to be used. Another primitive may be a "regular expression" based primitive that allows parsing of complex text-based fields with a full feature (*e.g.*, PERL5 compliant) pattern specification. Common used techniques would include parsing URLs, filenames and paths, calling/called telephone numbers, email address, for example. In addition, a CDR database 215 lookup primitive allows holding on to an ownership entity if no further processing is required. This primitive is used where usage record 401 provides the information needed by settlement layer 104 without any need for more data correlation and/or manipulation by transaction layer 103.

A default primitive may be a hard-coded primitive that is used where the value is known and/or is not dependent on usage record 401. For example, such a primitive may be used where a party is always present in a consumption event, regardless of the other relevant parties. A network address primitive allows determination of a network entity given an arbitrary string. An area code primitive may be used to determine an area code of a telephone number given the complete telephone number. This primitive may be relevant for a Voice-over-IP application. These examples primitives are not exclusive, but are meant to provide a few examples of the manipulation and correlation that may be achieved by the primitives on the accountables and contracts.

The following is an example of an accountable primitive in XML:

```
<accountable>
<name> ColoProvider </name>
<role> ServiceProvider </role>
<usageType> RMONHost </usageType>
<valid from="past" to="present" />
<primitive type="default">
<value> Exodus </value>
</primitive>
</accountable>
```

Each accountable that is involved in a contract will have an assigned "role." It follows, therefore, that an accountable that is not involved in a contract may not need to have an assigned role. The role associates the particular accountable for integration with settlement layer 104.

Similar to the accountable, a contract is implemented using a set of primitives. The following is an example of a contract primitive in XML. In the example, a Web hosting scenario is present where a content provider (*e.g.*, CNN) places content on one or more Web servers and pays a Web Hoster for doing so based on some predefined pricing plan.

In order to define the accountables, certain elements of usage record 401 may be assumed as follows: Web Hit Time, Web Server Name/IP address, Client IP address, bytes, Mime type, and URL. In this example, if a rule in the business world requires the "Content Provider" of the Web Server (*e.g.*, CNN) to pay to the Web Hoster, there are two accountables: Web Hoster and Content Provider. The XML definition of a contract that captures this business rule may be as follows:

```
01  <contract>
02  <name> ContentProvider-Pays-WebHoster </name>
03  <usageType> WebHosting </usageType>
04  <valid from="past" to="present" />
05  <condition function="IsPresent" type="Accountable"
    name="condition1"  id=" ContentProvider " />
06  <condition function="IsPresent" type="Accountable"
    name="condition2" id="WebHoster" />
07  <billedFunction>
08  <status> enabled </status>
09  <primitive type="internal-account-lookup">
10  <database name="GlobalDB"/>
11  <argument order="1" type="Accountable"
    name="ContentProvider"/>
12  </primitive>
13  </billedFunction>
14  <billingFunction>
15  <status> disabled </status>
16  <primitive type="internal-account-lookup">
17  <database name="GlobalDB"/>
```

```
18      <argument order="1" type="Accountable"
name="WebHoster"/>
19      </primitive>
20      </billingFunction>
21      </contract>
```

In this example, a contract has a name defined in line 02 as "ContentProvider-Pays-WebHoster." The contract also defines an element or usage type called "WebHosting" in line 03. The contract also has two sets of conditions in lines 05 and 06, called "IsPresent," which consider whether "ContentProvider" and "WebHoster" elements are present, respectively. Therefore, this particular contract will be selected and executed by transaction layer 103 if these elements are present.

Also, in this contract example, there are two primitives that are specified. There is a first primitive for finding the account number of the billed entity "ContentProvider," which begins on line 07 and ends on line 13, and there is a primitive for determining the account of the billing entity "WebHoster" beginning on line 14 and ending on line 20. Therefore, the example contract contemplates the "who pays to whom" logic, and results in the execution of a contract that creates a modified usage record 402, which captures the transaction. Notably, in lines 09 and 16, both primitives are defined as database lookups.

As noted above, to settle a transaction, the system must determine who should compensate whom and by how much. Many processes contribute to such "settlement." Accordingly, the settlement layer 104 is not necessarily a particular logical component but may be spread throughout the system. In operation, a typical "settlement" might occur as described below with respect to Figure 8.

Figure 8 illustrates a sample content event as received by transaction layer 103 pursuant to the processes described above. In this example, "content.com" is identified as the billed party for a caching service, and IP address "128.33.2.41" is identified as the billed party for consuming content type "audio video interleave" (.avi). This IP address may be mapped to a customer account that may vary over time. The system also may identify the log provider (*e.g.*, web host service) and may identify the content property owner (*e.g.*, "Disney") as the party to receive a royalty,

or some other form of compensation, for the download. This ownership may create rules based on the unique resource locator (URL) substring and other event information. Also, links may be provided from the event to the multiple accounts related to that event. The use of pricing plans and pools, as described below, allow business rules to be captured regarding compensation for events, for example, in ways that greatly increase system flexibility. In this example, a fee may be charged to "content.com," while revenue may be paid back to the log provider.

Settlement of Transactions Subject to Multiple Pricing Plans

In many transactions, the accounts include one or more pricing plans that are customized to particular customers. As shown in Figure 9, the settlement technologies used to settle such transactions may allow for multiple ownership of content, multiple aggregation of usage, and provide a variety of revenue sharing models. Several of such models will be described below including folds with parent account plans, revenue pooling, and commission relationships between plans.

Figure 10 illustrates a settlement example for the case of digital content, such as digital music content downloadable off of the Internet. In this example, an on-line music club (*e.g.,* BMG, EMI, Sony) has a contractual relationship with the consumers as well as the music publishers (*e.g.,* "www.cd-club.com") and, at settlement, allocates payment according to the price plan(s) with the consumer and the payment plan(s) with the publishers. These payment plans recognize that each song may have a different price and that the revenue paid to the publisher, author, etc. may vary over time depending upon the frequency of download, for example. The price to the consumer also may vary with use. Figures 11 and 12 illustrate settlement models that take into account transaction pricing and billing cycle pricing for such usage based settlements. As those skilled in the art will appreciate, the per transaction usage based model may be best utilized for low volume, high value transactions, while the billing cycle pricing usage based model may be better for high volume, low value transactions.

The present invention allows for the networking of a multiplicity of pricing plans during rating process 217 in settlement layer 104. Thus, the system described

below is implemented primarily in ratings 217 described above with respect to Figure 2.

Pricing Plan Overview

In accordance with the invention, pricing plans may be created by interconnecting rating building blocks with customizable properties. Each rating building block may be specialized in one well-defined function that falls roughly into five classes: usage selection and filtering, usage computation, accumulation, rate computation, and bill presentation. By interconnecting these rating building blocks, together with the ability to add new rating building blocks to the system, very flexible and extensible pricing plans can be created. The computation may be desirably constrained within one pricing plan.

A new class of rating building blocks also may be defined to extend the usefulness of pricing plans. This new class of rating building blocks allows a plan to access the states of another pricing plan or a group of pricing plans. These states can be usages and/or charges associated with line items and/or intermediate computations. With this new capability, computation is not constrained within one pricing plan but within a network of pricing plans working together. This new computation offers, but is not limited to, many settlement features.

A revenue fold summarizes revenue, which is the output of a pricing plan, from child accounts and presents the folded revenue to their corresponding parent accounts as input to their pricing plans. This process may start from the lowest level and continue on up to the root level. The value of revenue fold may be available to a parent account in a pricing plan through a building block (*e.g.*, "RevenueToDate"). As illustrated in Figure 13, the revenue fold settlement model of the invention may provide for pricing plans at each level in the hierarchy and allow for the use of resellers.

Revenue/usage pools are similar to global variables except that they include the concept of billing cycles. Different periods of a pool imply different instances and therefore different values. A pool value may be updated during invoice processing by summing the values of invoice line items associated with the pool from appropriate

account plan periods. An account plan period is considered appropriate if the end date is within the period of the particular pool instance. Note that it is possible to have zero or more than one account plan periods from the same account to be included in the same pool instance. The computation of a pool value may not be cumulative between updates. When a pool value needs to be updated, the computation may start over with the previous value of a pool having no consequence. For example, the value of a pool may be accessible from a pricing plan through a building block (*e.g.*, "PoolAccessor") with the pool name as its property. The output of the "PoolAccessor" is the sum of the pool instances having the same pool name and billing period end dates within the start and end dates of the account plan period. As shown in Figure 14, this settlement feature is useful in revenue sharing scenarios where total revenue and resources are pooled together and total revenue is shared among the contributing accounts based on contributed resources. The pools may be hierarchy independent and defined by the pricing plans. A revenue pool contribution example is given in Figure 15, and a revenue pool accessor example is given in Figure 16.

A commission is a credit given to an account. The credit amount is computed based on the revenue, or states of another account. The two accounts involved in the transaction are commission source account and commission destination account. As shown in Figure 17, the commission source account (commission generator plan) generates the commission contribution iCDR using a building block (*e.g.*, "CommissionGenerator") with "AccountNumber" and "CommissionDescription" as its properties. The amount, not necessarily revenue, going into the CommissionGenerator (commission plan) is the commission amount. When used in conjunction with existing rating building blocks, commission features such as the following can be supported: commission going to multiple accounts, commission based on total revenue or a subset of the revenue (*e.g.*, only monthly and usage charges, but not setup charges), commission for the first "n" billing period only (or different rate after first "n" periods), and step rate.

The commission destination account may receive the commission data through a building block (*e.g.*, "CommissionAccumulator"). Additional commission features such as the following can be supported on the destination account: a recurring base commission, promotional commission rate, and step commission rate. The commission settlement model also may be hierarchy independent and permit variable settlement arrangements.

When computation involves a network of pricing plans, the correct output of a particular pricing plan may be dependent on the processing of another pricing plan. The output of the other pricing plan may in turn dependent on yet another pricing plan. A cyclic dependence can even exist. In order to have the correct computation for the network of pricing plans as a whole, the system detects and continues processing until all pricing plans reach their final values. Accordingly, the settlement processing software in accordance with the invention has a built-in mechanism to repeat processing of the pricing plans until their values are final. The algorithm will stop after a configurable loop count to prevent infinite processing in case there is a cyclic dependence.

Billing Cycle Considerations

Because more than one account may be involved in settlement, it is possible that they have different billing periods. The following section details how each settlement feature is processed for the settlement models of the invention when accounts with different billing periods are involved.

Revenue fold summarizes revenue from child accounts and presents the folded revenue to their parent accounts. This process starts from the lowest level and continues up to the root level. In actual settlement processing, revenue fold is a post order traversal of a tree whose nodes are account plan periods, where a post order tree traversal traverses each sub tree of the root in post order followed by the root. The child account plan periods are selected if the end dates are within the parent's account plan period. It is possible to have zero or more than one account plan period from the same account included in one revenue fold. The root account's account plan period is defined by the invoice processing start and end dates.

An iCDR is generated for each revenue fold. The iCDR is rated by the pricing plan for the account plan period receiving the revenue fold. Therefore, pricing plans for non-leaf accounts take revenue fold into consideration. The value of revenue fold is available in a pricing plan through a building block (*e.g.*, "RevenueToDate").

Figure 18 provides an example of computing revenue fold. To compute the revenue fold for account 1001, the revenue from all child accounts of 1001 with account plan period end dates between 3/1 and 4/1 are summed. In this example, the revenue for account 2001 for the billing period 2/7 to 3/7, account 2002 for the billing period 2/15 to 3/15, account 2003 for the billing period 2/22 to 3/22 are summed. Before the summing of the revenue of these accounts can occur, their own revenues are determined. In order to determine the revenue of these child accounts, their child accounts with account plan period end dates between their account plan period start and end dates are selected and summed. The following example shows that to determine the revenue for account 2003 for the billing period 2/22 to 3/22, revenue for account 3001 for the billing period 2/1 to 3/1 and account 3002 for the billing period 2/15 to 3/15 are summed. This process repeats until the leaf level account is reached.

The value of a pool is accessible from a pricing plan through a rating building block (*e.g.*, "PoolAccessor"). The output of "PoolAccessor" is the sum of the pool instances having billing period end dates within the start and end dates of the account plan period. It is possible to have zero or more than one instance selected given a particular account plan period depending on the billing period of the pool and the account. Therefore, given the same plan, "PoolAccessor" output may vary according to the account plan period. This technique ensures that each invoice line item associated with a pool will be included a pool instance and that each pool instance will be accessed once by an account which accesses the pool.

Figure 19 illustrates how accounts and pools with different billing cycles contribute to and access from pool instances. For example, line items associated with pool A for account 1001 with billing period from 4/1 to 6/1 and account 1002 with billing periods from 3/22 to 4/22 and 4/22 to 5/22 will contribute to the pool A's

instance with period from 4/1 to 6/1. The output of the PoolAccessor will be zero for account 2001 during the period 4/1 to 5/1. For billing period from 5/1 to 6/1, account 2001 will get the value of pool A's instance with period from 4/1 to 6/1. Account 2002 with billing period from 4/1 to 6/1 will also get pool A's 4/1 to 6/1 instance. The account plan period from 4/1 to 8/1 for account 2003 will get the sum of the two pool A's instances, 4/1 to 6/1 and 6/1 to 8/1.

During invoice processing, one or more iCDRs will be generated for each commission producing account plan periods. The generated record will have the destination account number, amount, and a timestamp. The timestamp is the end date of the account plan period that generated the record. The record will then be rated by the destination account in the appropriate account plan period.

Figure 20 provides an example of how an account 2001 with billing period ending 6/1 will get one commission from account 1001 for the period 4/1 to 6/1 and two commissions from account 1002 for the periods 3/22 to 4/22 and 4/22 to 5/22.

An invoice output may be dependent on the processing of settlement features. In turn, processing of settlement features may be dependent on correct invoice output. For example, if the pricing plan associated with an invoice accesses one or more pools, revenue/usage pool processing should be completed successfully before a correct invoice can be produced. To process a revenue/usage pool correctly, account plan periods associated with a pool have to produce a correct invoice that in turn may be dependent on revenue fold. There may not be a single, correct pre-defined order of processing for these settlement features. In some cases, the same settlement features may have to be processed more than once (*e.g.*, revenue fold, generate commission and then revenue fold again).

The settlement processing has a built-in mechanism to repeat processing of the settlement features in a fixed sequence until the values are final. To prevent the algorithm from looping forever, there is a configurable maximum loop count. If the result is not final after the maximum loop count, a warning will be given, and the user may remove the circular dependency (if one exists) and/or increases the maximum loop count.

The invention described above is directed to a system and method for handling the networking of pricing plans in the settlement of transactions. The invention often was described in the context of the Internet, but is not so limited to the Internet, regardless of any specific description in the drawing or examples set forth herein. For example, the invention may be applied to wireless networks, as well as non-traditional networks like Voice-over-IP-based networks and/or private networks. It will be understood that the invention is not limited to the use of any of the particular components or devices herein. Indeed, this invention can be used in any application that requires aggregating data. Further, the system disclosed in the invention can be used with the method of the invention or a variety of other applications.

While the invention has been particularly shown and described with reference to the embodiments thereof, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art will appreciate that various changes and adaptations of the invention may be made in the form and details of these embodiments without departing from the true spirit and scope of the invention as defined by the following claims.

What is claimed is:

1. A method of rating a transaction, comprising:

processing a transaction, wherein the transaction is processed when a service is provided from a service provider to a service consumer;

accessing via a computer network multiple pricing plans related to the transaction; and

rating the transaction in accordance with the multiple pricing plans.

2. The method of claim 1, wherein at least one of the pricing plans includes at least one of the following: revenue folds, revenue/usage pools, and commissions.

3. The method of claim 1, further comprising receiving output states from at least one pricing plan.

4. The method of claim 1, wherein the rating is accomplished within one pricing plan.

5. The method of claim 1, wherein the rating is accomplished within a group of pricing plans.

6. The method of claim 1, wherein the accessing is accomplished via interconnected building blocks located within each of the pricing plans.

7. The method of claim 1, wherein the building blocks perform at least one of the following functions: data usage selection and filtering, data usage computation, data accumulation, rate computation, and presentation of required payment.

8. The method of claim 6, wherein the building blocks have customizable properties.

9. The method of claim 6, wherein the building blocks allow a first pricing plan to access states of another pricing plan.

10. The method of claim 9, wherein the states are usages and charges associated with one or more pricing plans.

11. The method of claim 6, wherein the building blocks allow a first pricing plan to access the states of a group of pricing plans.

12. The method of claim 11, wherein the states are usages and charges associated with one or more pricing plans.

13. The method of claim 1, further comprising a revenue fold, wherein the revenue fold summarizes the output of multiple pricing plans.

14. The method of claim 13, wherein the revenue fold summarizes child accounts and inputs the summary information to pricing plans of corresponding parent accounts.

15. The method of claim 13, wherein the value of the revenue fold is available to the pricing plan via a building block.

16. The method of claim 13, wherein the revenue fold is available to child and parent accounts.

17. The method of claim 13, further comprising selecting child accounts with end dates that are within a parent account's time period.

18. The method of claim 1, further comprising pooling revenue/usage data as a function of billing cycles.

19. The method of claim 18, further comprising updating the pooled revenue/usage data by summing the values of data from selected account plan periods.

20. The method of claim 18, further comprising selecting the account plan period as a function of the end date of the account plan with respect to the pooled revenue/usage data.

21. The method of claim 18, further comprising accessing a value of the pooled revenue/usage data via a building block.

22. The method of claim 1, further comprising determining the value of a pricing plan as a function of another pricing plan.

23. The method of claim 22, further comprising providing a configurable loop count.

24. A computer-readable medium having computer-executable instructions, comprising:

processing a transaction, wherein the transaction is processed when a service is provided from a service provider to a service consumer;

accessing via a computer network multiple pricing plans related to the transaction; and

rating the transaction in accordance with the multiple pricing plans.

25. The computer-readable medium of claim 24, having computer-executable instructions further comprising receiving output states from at least one pricing plan.

26. The computer-readable medium of claim 24, having computer-executable instructions further comprising a revenue fold, wherein the revenue fold summarizes the output of multiple pricing plans.

27. The computer-readable medium of claim 24, having computer-executable instructions further comprising selecting child accounts with end dates that are within a parent account's time period.

28. The computer-readable medium of claim 24, having computer-executable instructions further comprising pooling revenue/usage data as a function of billing cycles.

29. The computer-readable medium of claim 24, having computer-executable instructions further comprising determining a commission, wherein the commission is a credit given to an account.

30. The computer-readable medium of claim 24, having computer-executable instructions further comprising determining the value of a pricing plan as a function of another pricing plan.

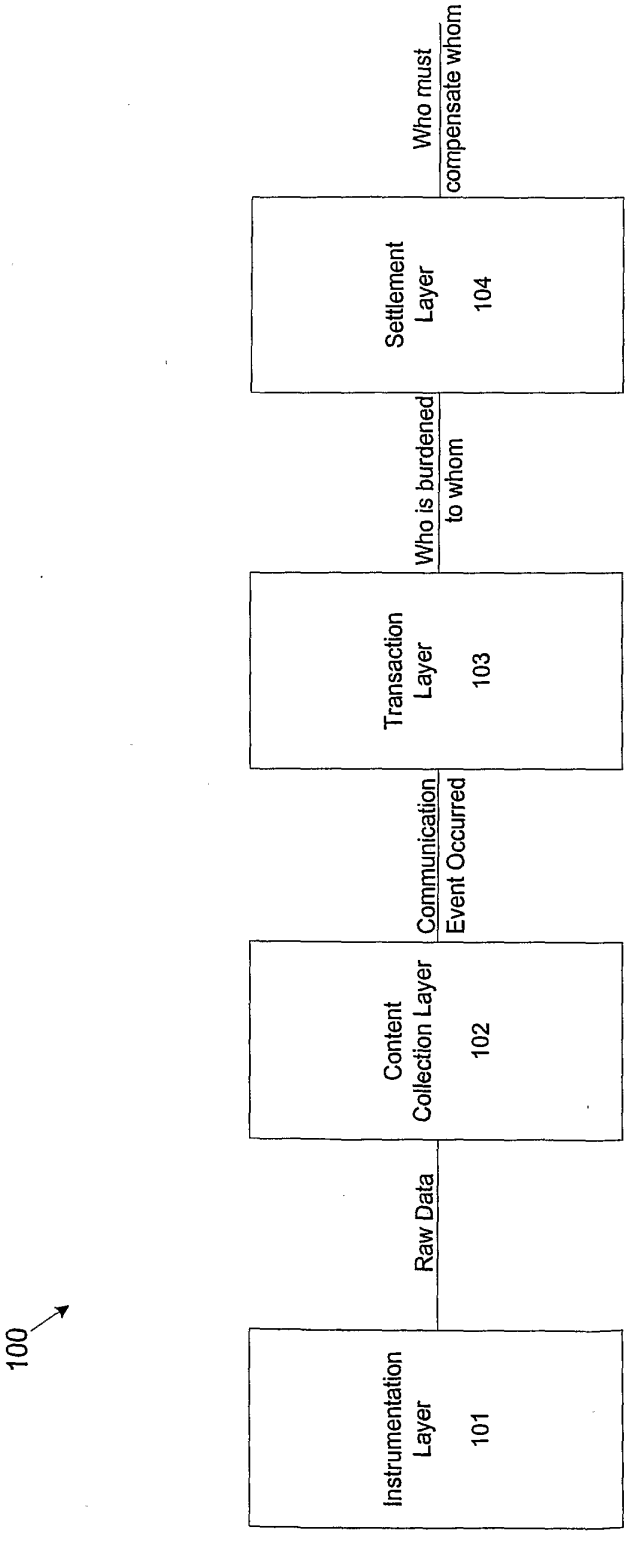

100
Instrumentation Layer 101
Raw Data
Content Collection Layer 102
Communication Event Occurred
Transaction Layer 103
Who is burdened to whom
Settlement Layer 104
Who must compensate whom

Figure 1

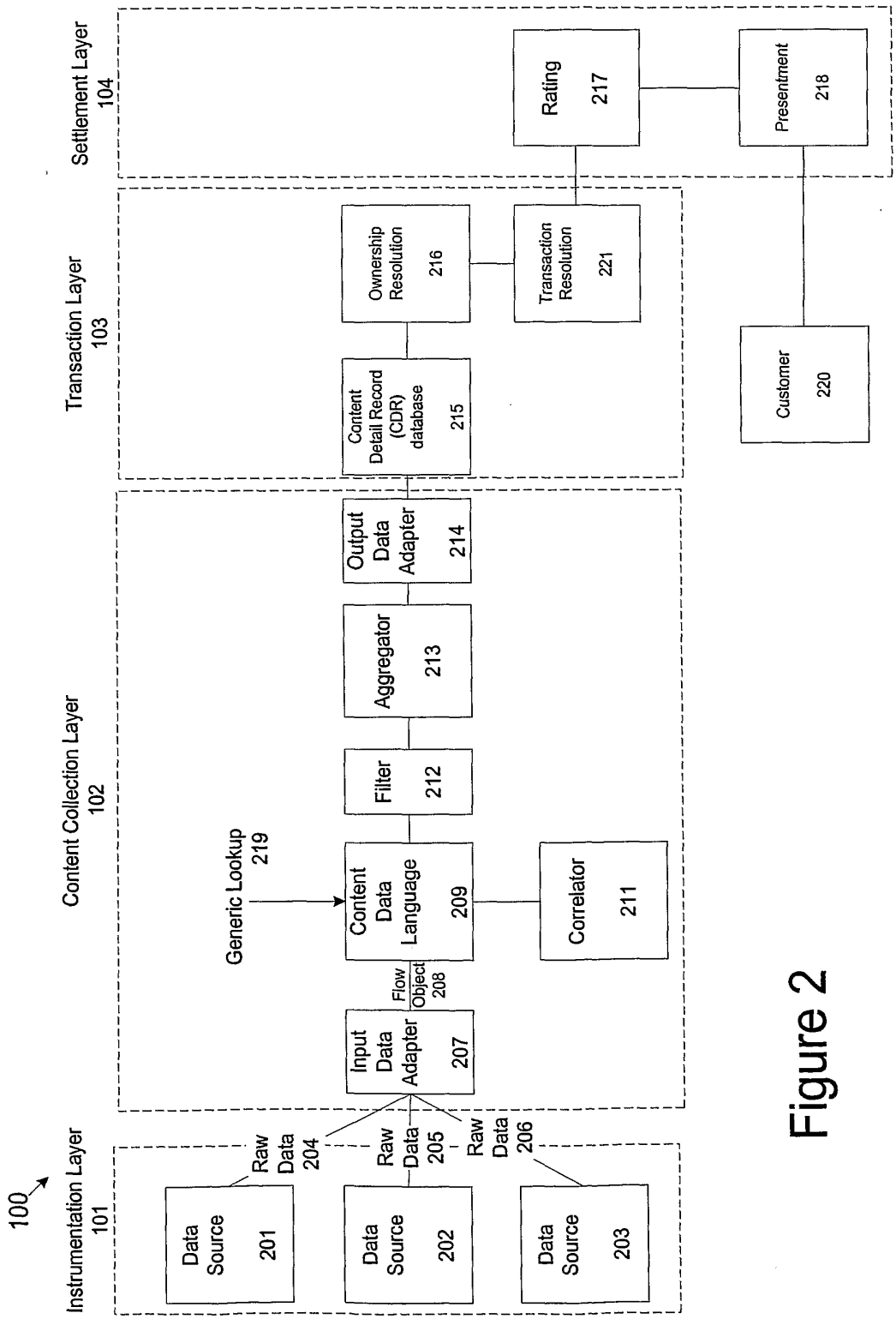

100
Instrumentation Layer
101
Data Source
201
Data Source
202
Data Source
203
Raw Data
204
Raw Data
205
Raw Data
206
Content Collection Layer
102
Input Data Adapter
207
Flow Object
208
Content Data Language
209
Generic Lookup
219
Filter
212
Aggregator
213
Output Data Adapter
214
Correlator
211
Transaction Layer
103
Content Detail Record (CDR) database
215
Ownership Resolution
216
Transaction Resolution
221
Settlement Layer
104
Rating
217
Presentment
218
Customer
220

Figure 2

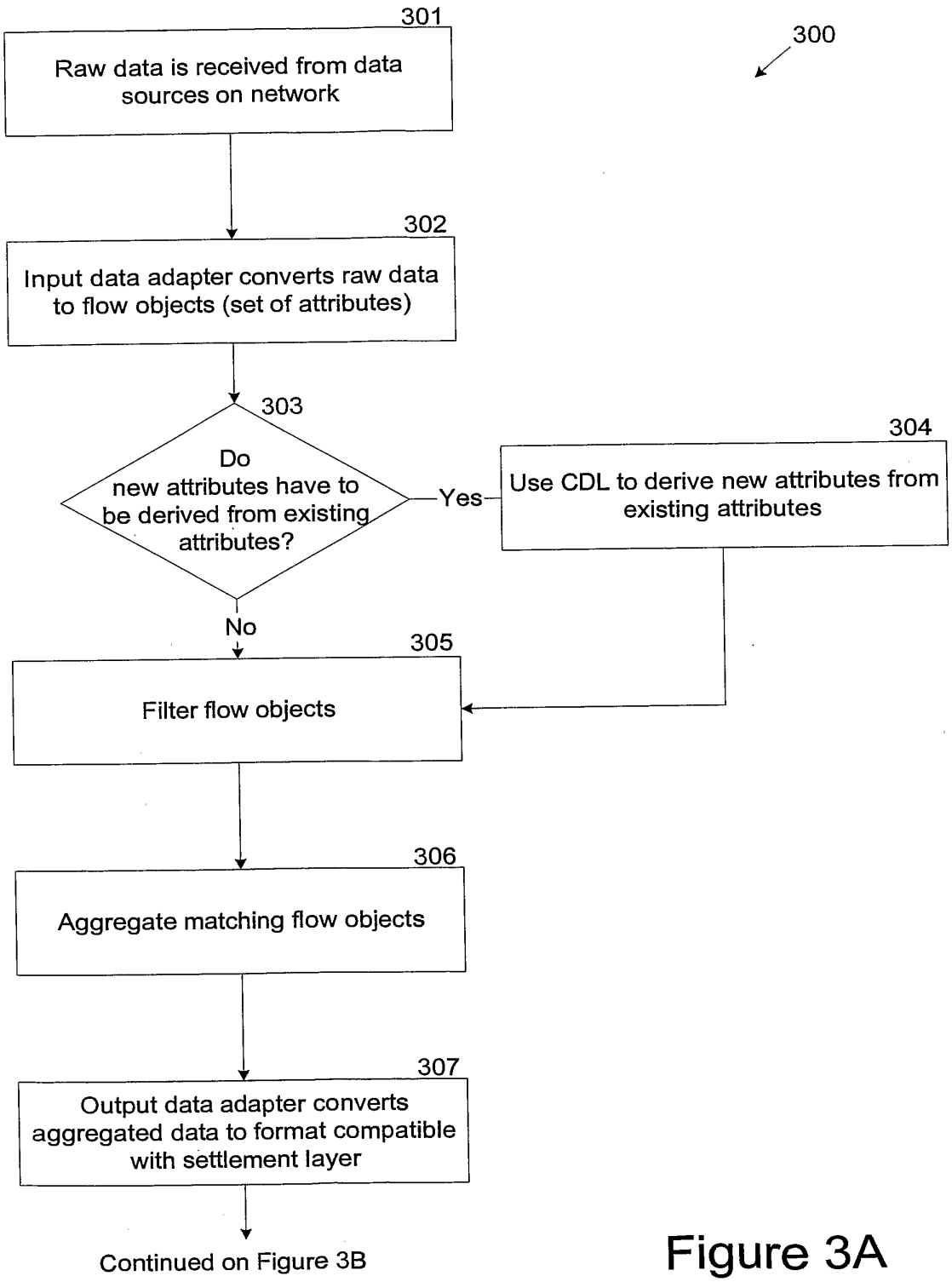

301
Raw data is received from data sources on network
300
302
Input data adapter converts raw data to flow objects (set of attributes)
303
Do new attributes have to be derived from existing attributes?
Yes
304
Use CDL to derive new attributes from existing attributes
No
305
Filter flow objects
306
Aggregate matching flow objects
307
Output data adapter converts aggregated data to format compatible with settlement layer
Continued on Figure 3B

Figure 3A

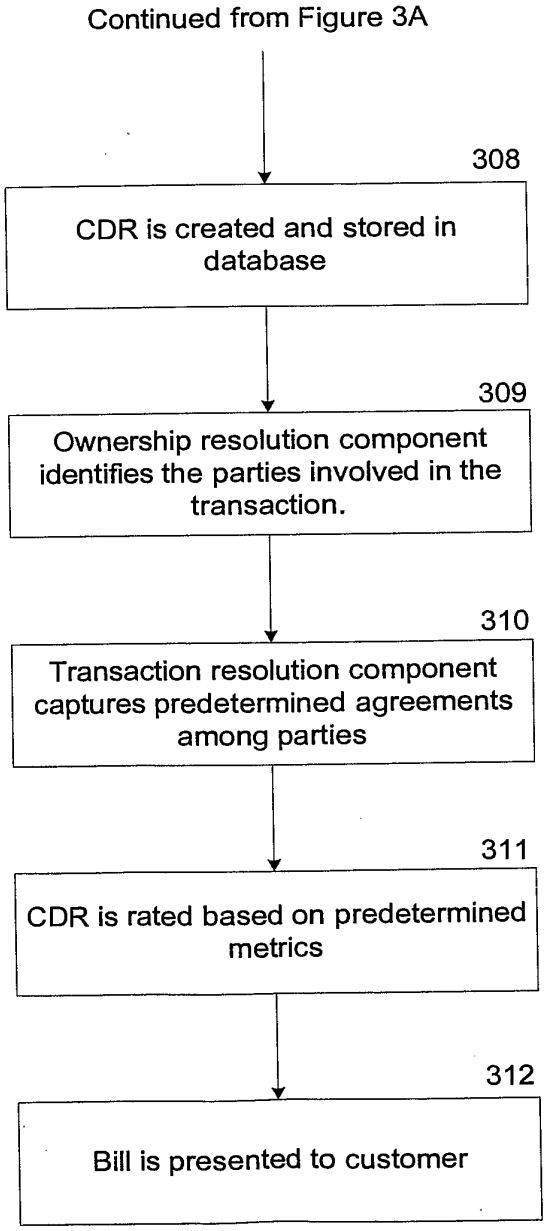

Continued from Figure 3A
308
CDR is created and stored in database
309
Ownership resolution component identifies the parties involved in the transaction.
310
Transaction resolution component captures predetermined agreements among parties
311
CDR is rated based on predetermined metrics
312
Bill is presented to customer

Figure 3B

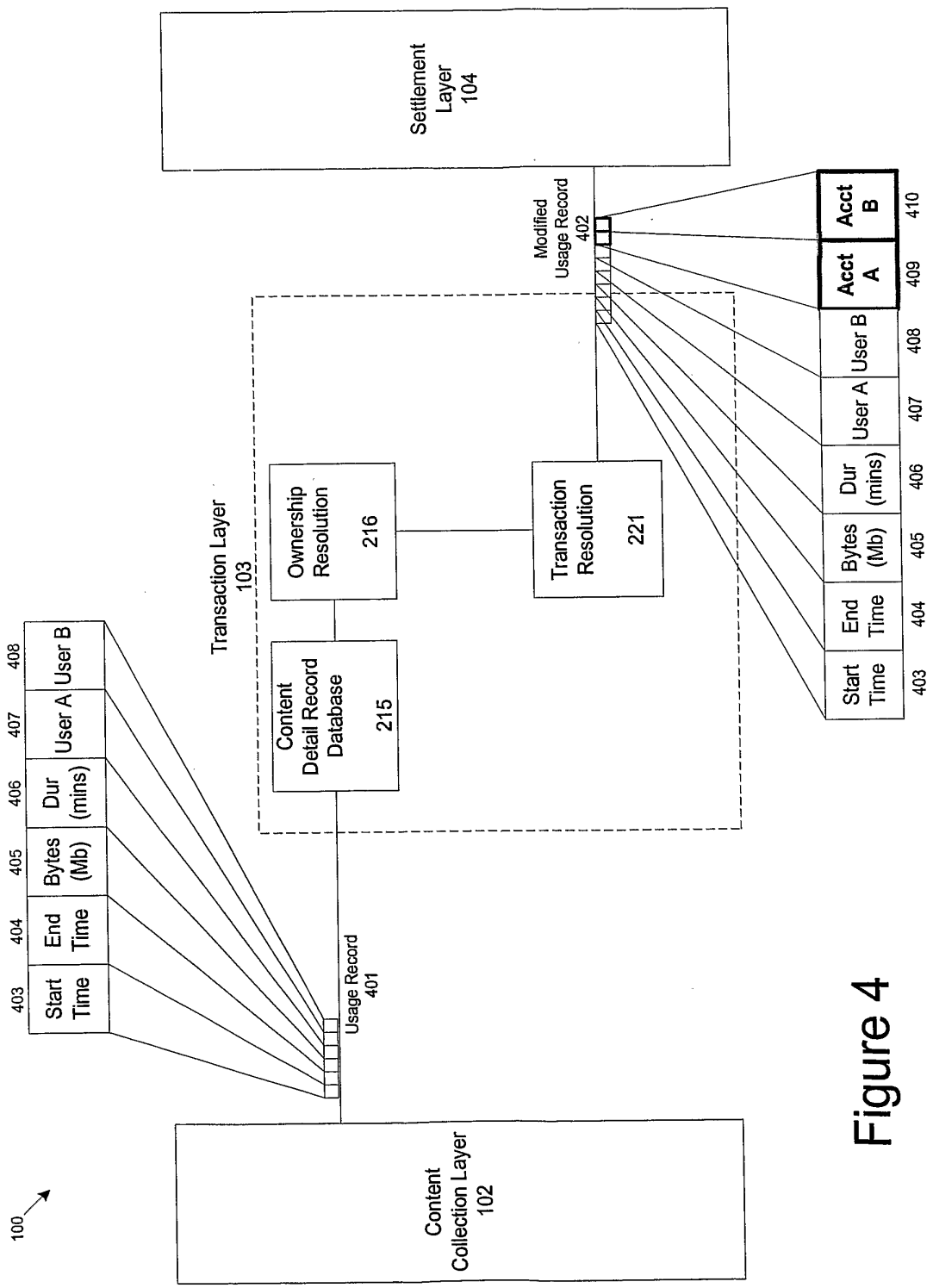

100
Content Collection Layer 102
Usage Record 401
Start Time 403
End Time 404
Bytes (Mb) 405
Dur (mins) 406
User A 407
User B 408
Transaction Layer 103
Content Detail Record Database 215
Ownership Resolution 216
Transaction Resolution 221
Modified Usage Record 402
Settlement Layer 104
Start Time 403
End Time 404
Bytes (Mb) 405
Dur (mins) 406
User A 407
User B 408
Acct A 409
Acct B 410

Figure 4

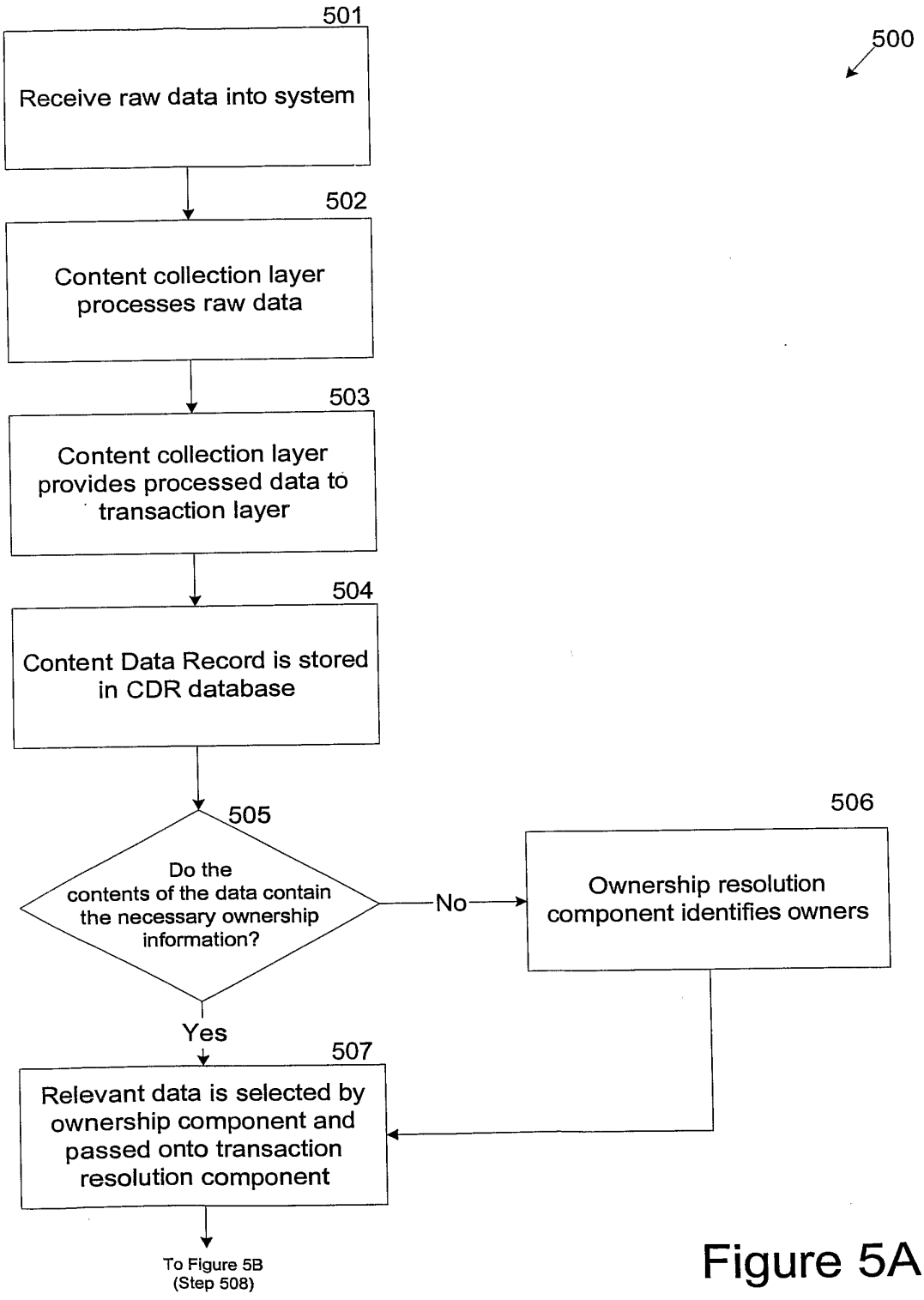

500
501
Receive raw data into system
502
Content collection layer processes raw data
503
Content collection layer provides processed data to transaction layer
504
Content Data Record is stored in CDR database
505
Do the contents of the data contain the necessary ownership information?
No
506
Ownership resolution component identifies owners
Yes
507
Relevant data is selected by ownership component and passed onto transaction resolution component
To Figure 5B (Step 508)

Figure 5A

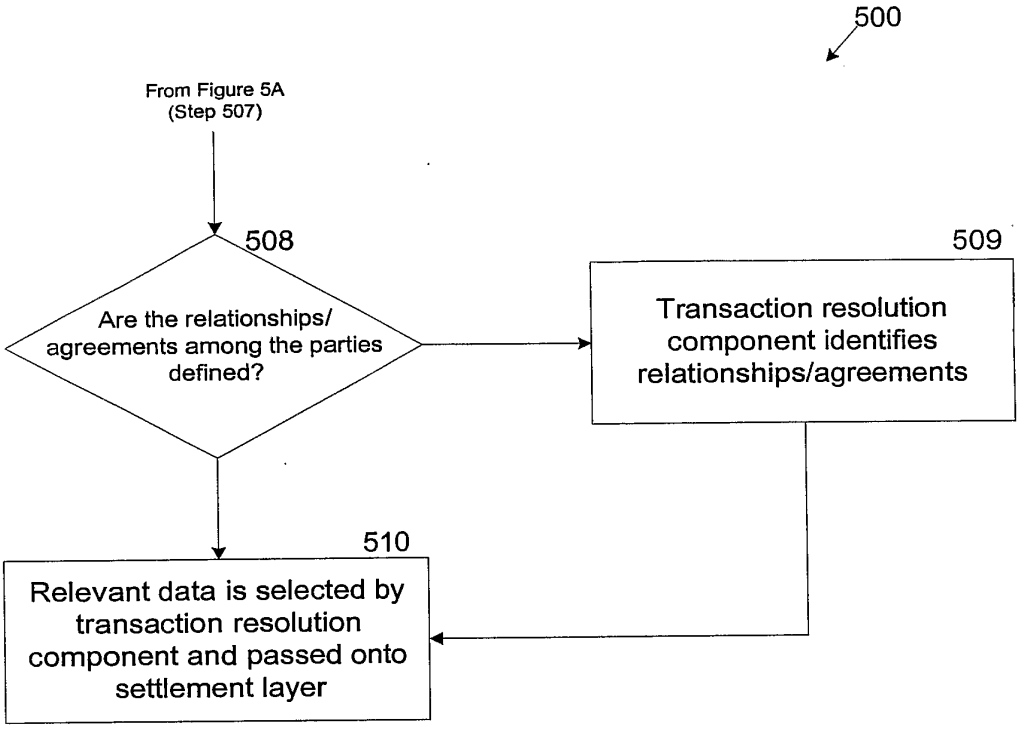

500
From Figure 5A
(Step 507)
508
Are the relationships/ agreements among the parties defined?
509
Transaction resolution component identifies relationships/agreements
510
Relevant data is selected by transaction resolution component and passed onto settlement layer

Figure 5B

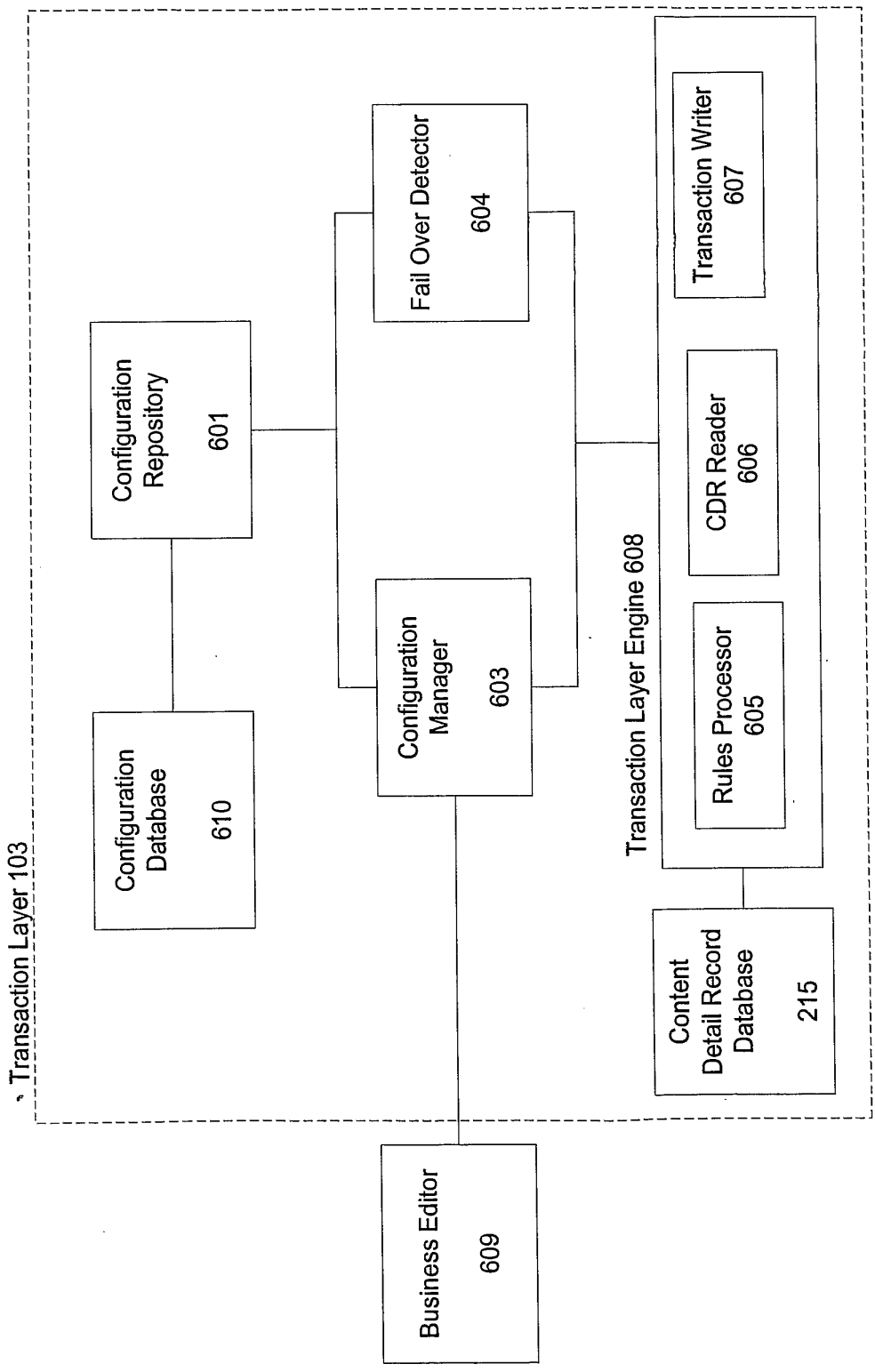

Transaction Layer 103
Configuration Repository 601
Configuration Database 610
Fail Over Detector 604
Configuration Manager 603
Business Editor 609
Transaction Layer Engine 608
Transaction Writer 607
CDR Reader 606
Rules Processor 605
Content Detail Record Database 215

Figure 6

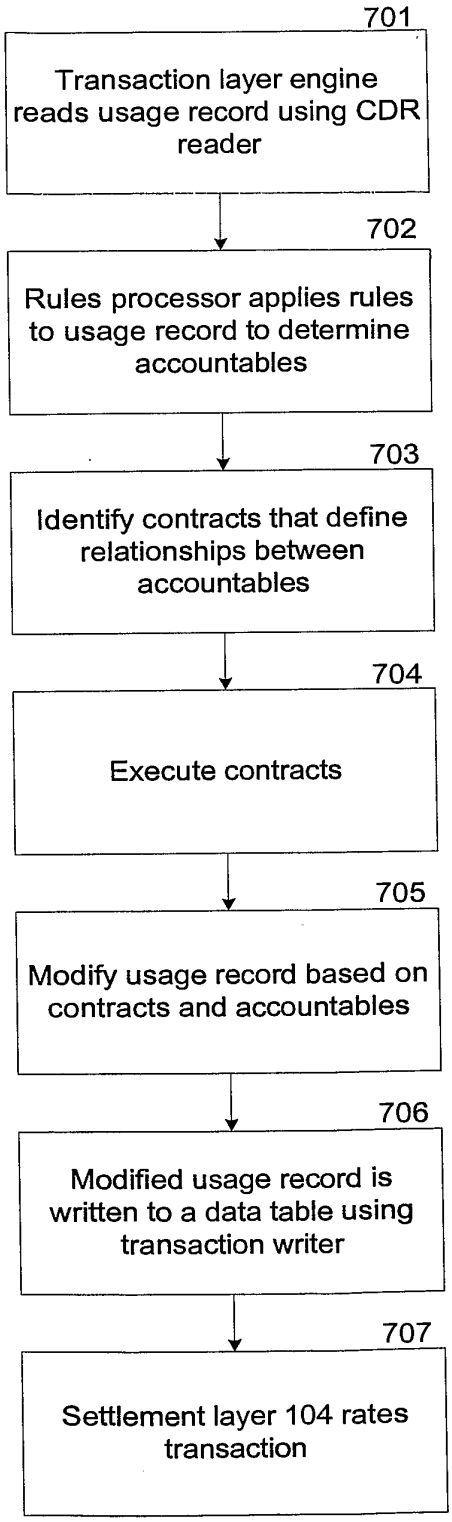

701
Transaction layer engine reads usage record using CDR reader
702
Rules processor applies rules to usage record to determine accountables
703
Identify contracts that define relationships between accountables
704
Execute contracts
705
Modify usage record based on contracts and accountables
706
Modified usage record is written to a data table using transaction writer
707
Settlement layer 104 rates transaction
700

Figure 7

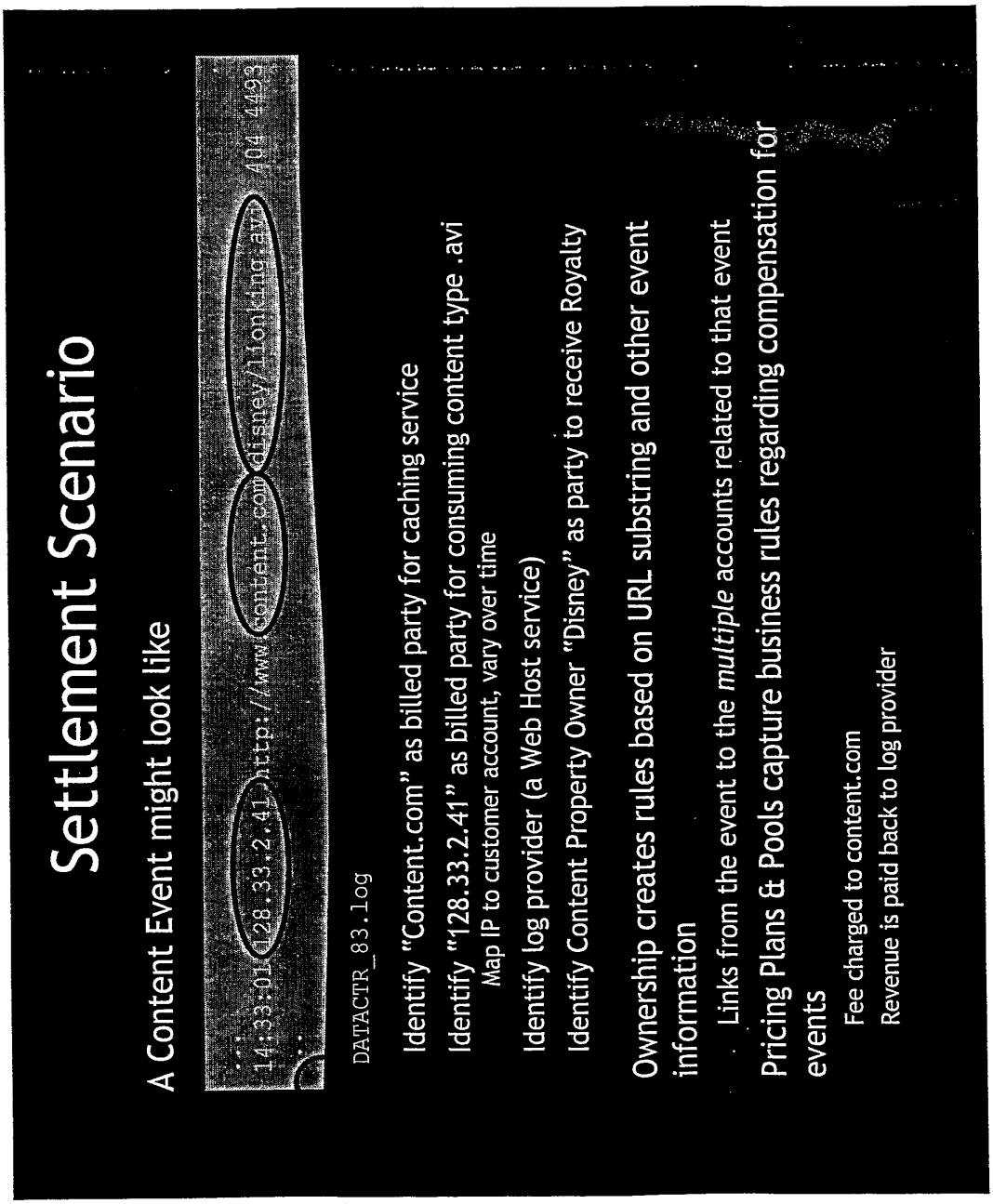

Settlement Scenario
A Content Event might look like
14:33:01 128.33.2.41 http://www.content.com/disney/lionking.avi 404 4493
DATACTR_83.log
Identify "Content.com" as billed party for caching service
Identify "128.33.2.41" as billed party for consuming content type .avi
Map IP to customer account, vary over time
Identify log provider (a Web Host service)
Identify Content Property Owner "Disney" as party to receive Royalty
Ownership creates rules based on URL substring and other event information
Links from the event to the multiple accounts related to that event
Pricing Plans & Pools capture business rules regarding compensation for events
Fee charged to content.com
Revenue is paid back to log provider

Figure 8

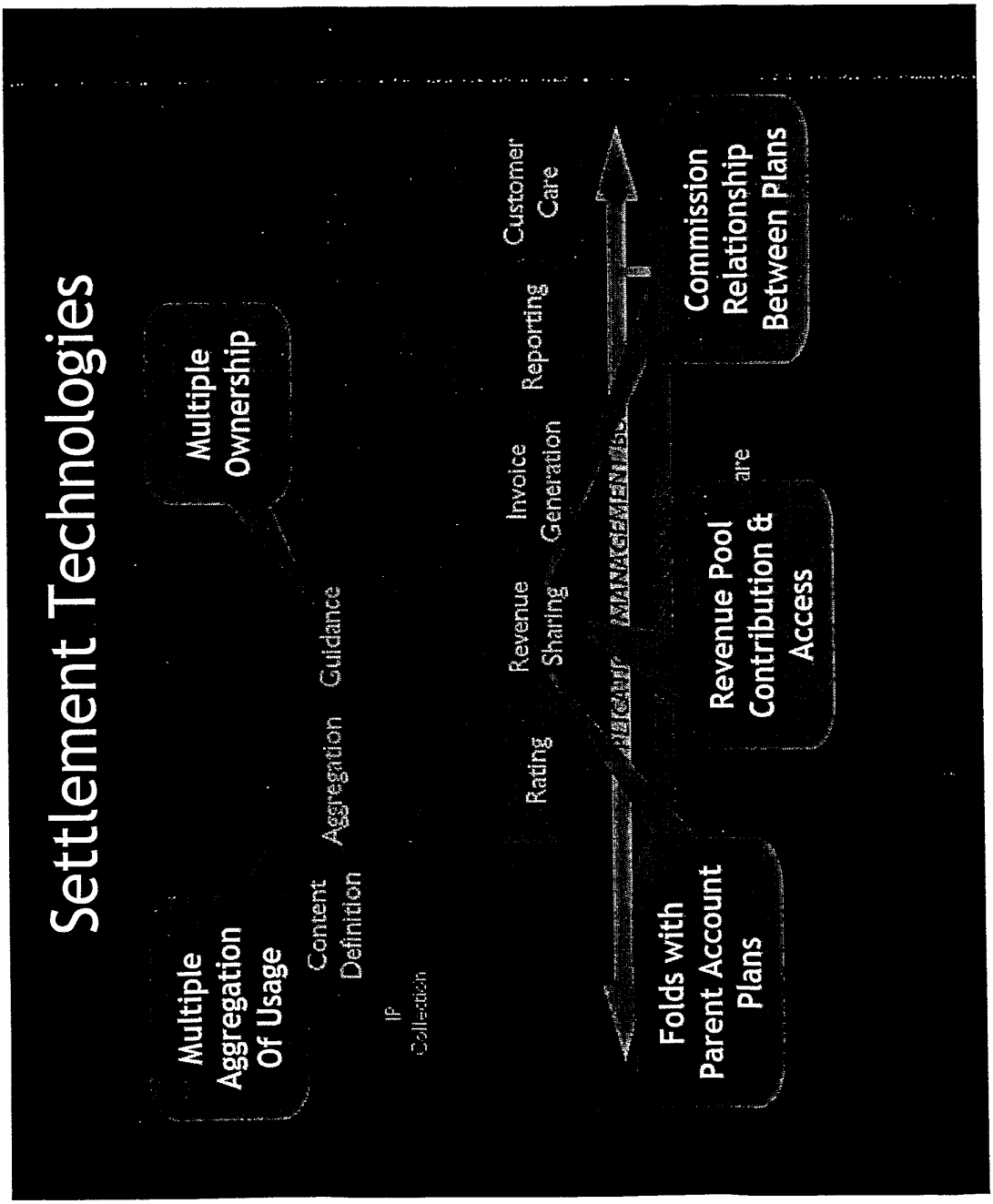

Settlement Technologies
Multiple Aggregation Of Usage
Content Definition
Aggregation
Guidance
IP Collection
Multiple Ownership
Rating
Revenue Sharing
Invoice Generation
Reporting
Customer Care
Folds with Parent Account Plans
Revenue Pool Contribution & Access
Commission Relationship Between Plans

Figure 9

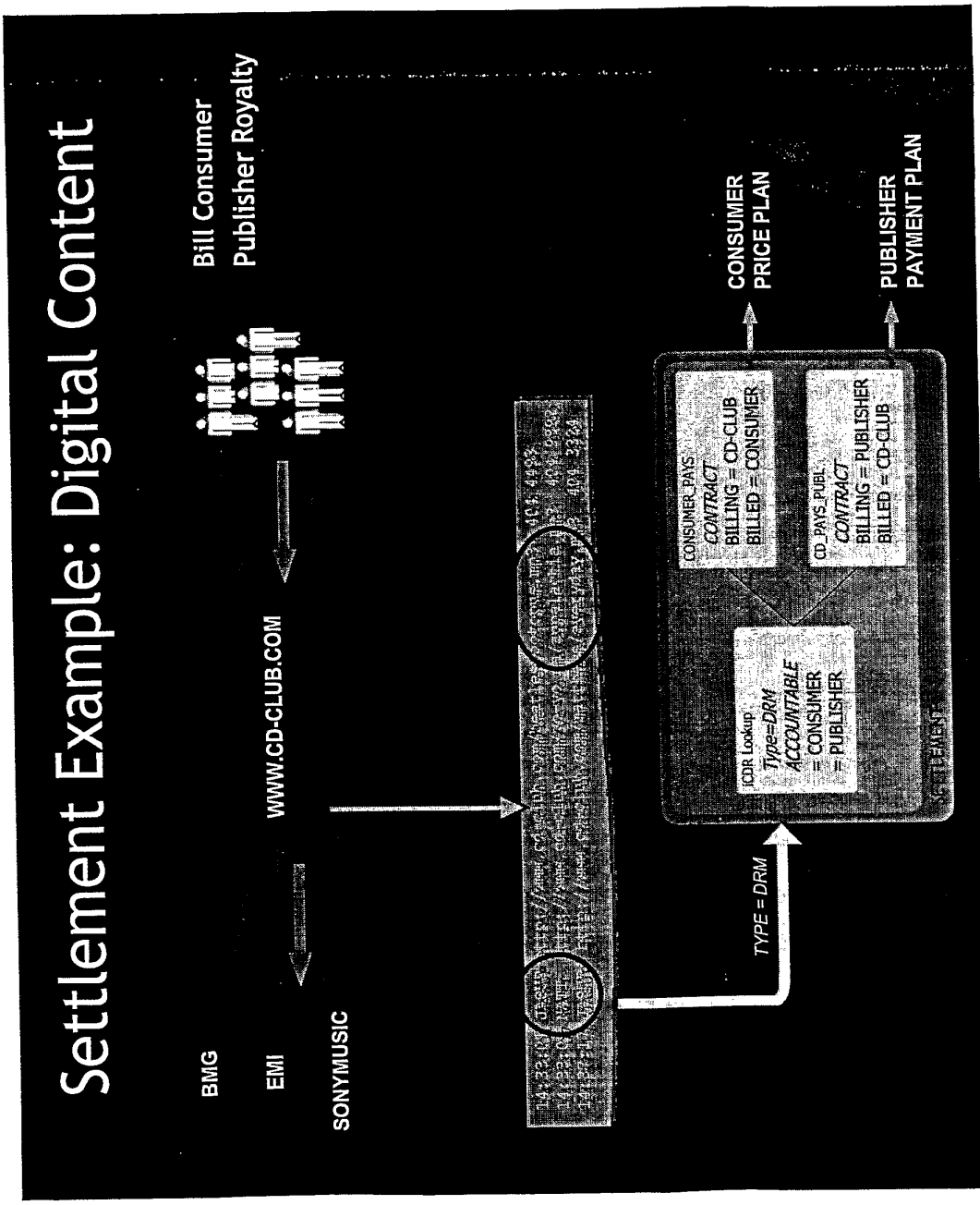

Settlement Example: Digital Content
BMG
EMI
SONYMUSIC
WWW.CD-CLUB.COM
Bill Consumer
Publisher Royalty
CONSUMER
PRICE PLAN
PUBLISHER
PAYMENT PLAN
CONSUMER_PAYS:
CONTRACT
BILLING = CD-CLUB
BILLED = CONSUMER
CD_PAYS_PUBL:
CONTRACT
BILLING = PUBLISHER
BILLED = CD-CLUB
IDR Lookup:
Type=DRM
ACCOUNTABLE
= CONSUMER
= PUBLISHER
TYPE = DRM

Figure 10

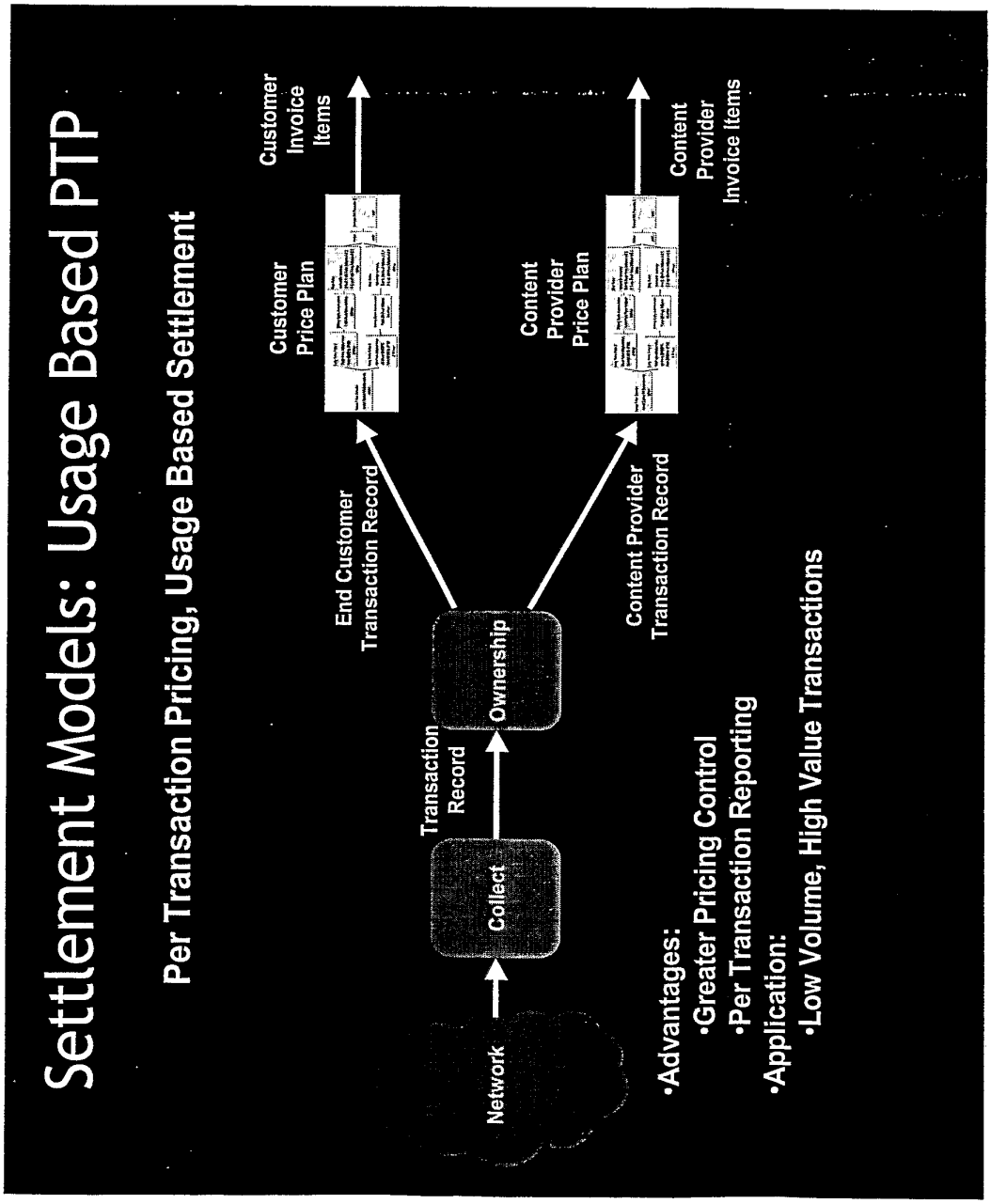

Settlement Models: Usage Based PTP
Per Transaction Pricing, Usage Based Settlement
Customer Invoice Items
Customer Price Plan
End Customer Transaction Record
Content Provider Price Plan
Content Provider Invoice Items
Content Provider Transaction Record
Transaction Record
Ownership
Collect
Network
•Advantages:
•Greater Pricing Control
•Per Transaction Reporting
•Application:
•Low Volume, High Value Transactions

Figure 11

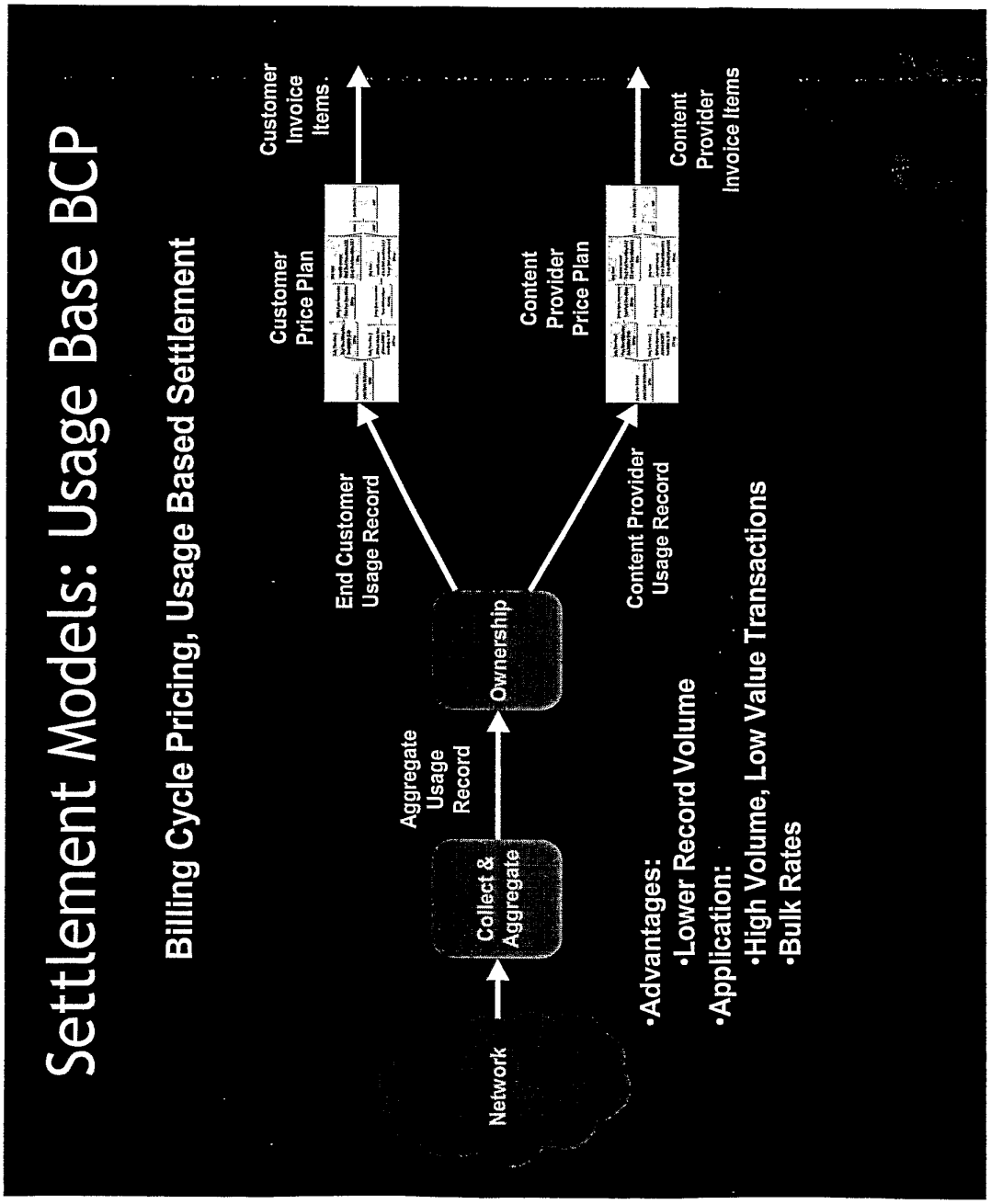

Settlement Models: Usage Base BCP
Billing Cycle Pricing, Usage Based Settlement
Customer Invoice Items.
Customer Price Plan
End Customer Usage Record
Content Provider Price Plan
Content Provider Usage Record
Content Provider Invoice Items
Aggregate Usage Record
Ownership
Collect & Aggregate
Network
•Advantages:
•Lower Record Volume
•Application:
•High Volume, Low Value Transactions
•Bulk Rates

Figure 12

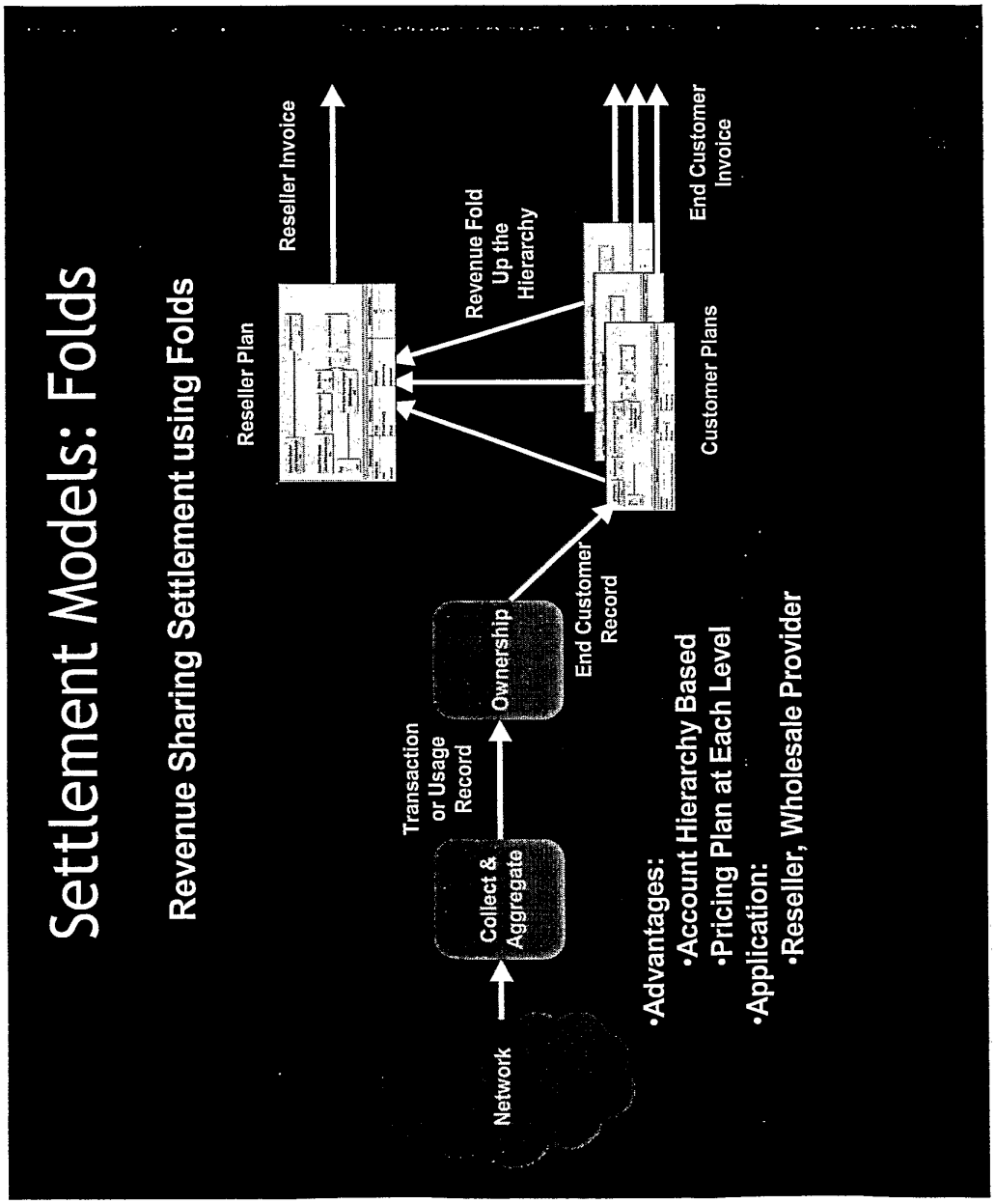

Settlement Models: Folds
Revenue Sharing Settlement using Folds
Reseller Plan
Reseller Invoice
Revenue Fold Up the Hierarchy
End Customer Invoice
Customer Plans
Transaction or Usage Record
Collect & Aggregate
Ownership
End Customer Record
Network
•Advantages:
•Account Hierarchy Based
•Pricing Plan at Each Level
•Application:
•Reseller, Wholesale Provider

Figure 13

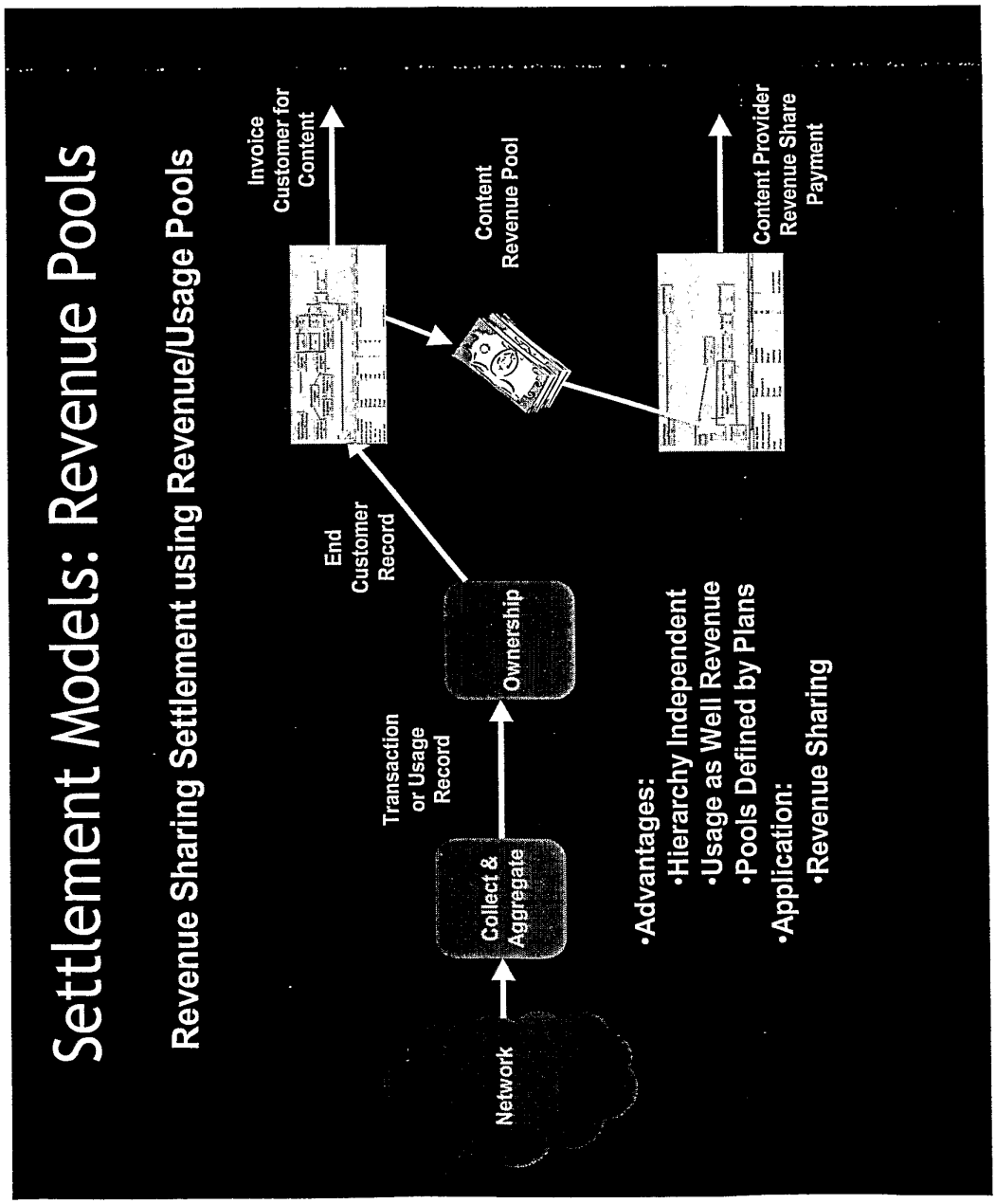

Settlement Models: Revenue Pools
Revenue Sharing Settlement using Revenue/Usage Pools
Invoice Customer for Content
Content Revenue Pool
Content Provider Revenue Share Payment
End Customer Record
Transaction or Usage Record
Ownership
Collect & Aggregate
Network
•Advantages:
•Hierarchy Independent
•Usage as Well Revenue
•Pools Defined by Plans
•Application:
•Revenue Sharing

Figure 14

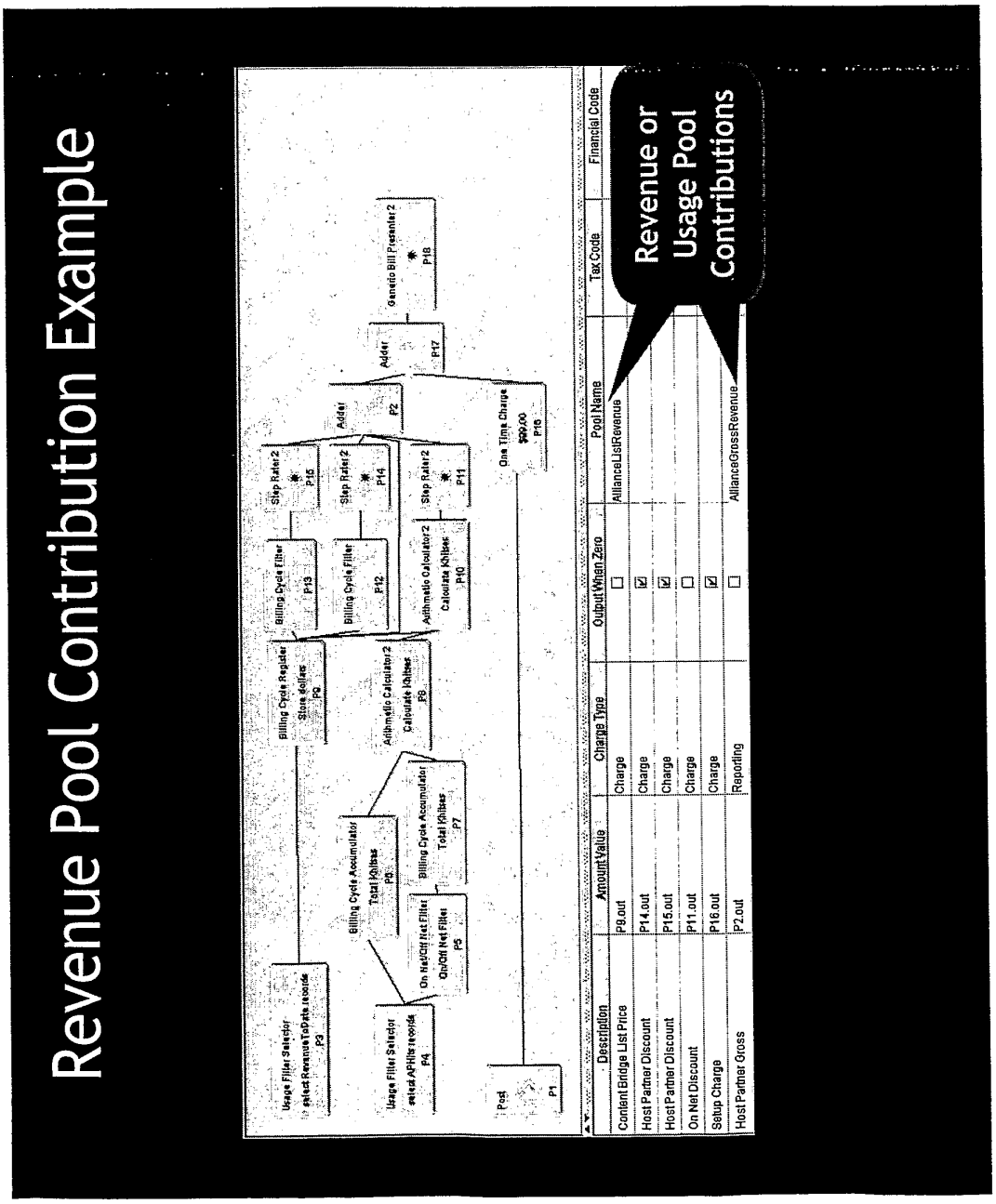

Revenue Pool Contribution Example
Revenue or Usage Pool Contributions
Post
P1
Usage Filter Selector
select APhits records
P4
Usage Filter Selector
select RevenueToPute records
P3
On Net/Off Net Filter
On/Off Net Filter
P5
Billing Cycle Accumulator
Total Kbites
P6
Billing Cycle Accumulator
Total Kbites
P7
Arithmetic Calculator2
Calculate Kbites
P8
Billing Cycle Register
Store dollars
P9
Arithmetic Calculator2
Calculate Kbites
P10
Step Rater2
P11
Billing Cycle Filter
P12
Step Rater2
P14
Billing Cycle Filter
P13
Step Rater2
P15
One Time Charge
$99.00
P16
Adder
P2
Adder
P17
Generic Bill Presenter2
P18
Description
Amount Value
Charge Type
Output When Zero
Pool Name
Tax Code
Financial Code
Content Bridge List Price
P8.out
Charge
AllianceListRevenue
Host Partner Discount
P14.out
Charge
Host Partner Discount
P15.out
Charge
On Net Discount
P11.out
Charge
Setup Charge
P16.out
Charge
Host Partner Gross
P2.out
Reporting
AllianceGrossRevenue

Figure 15

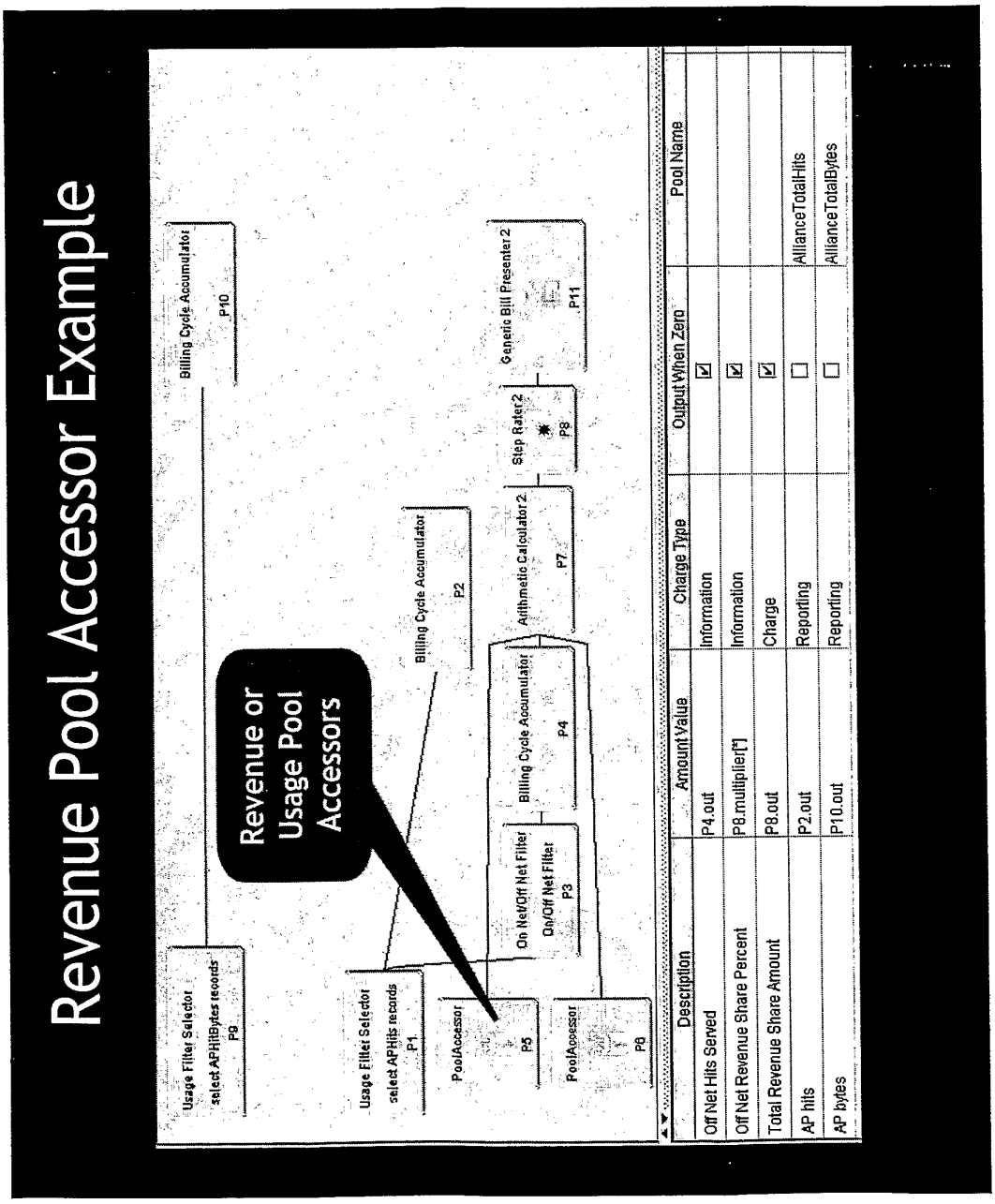

Revenue Pool Accessor Example
Revenue or Usage Pool Accessors
Usage Filter Selector
select APHitBytes records
P9
Billing Cycle Accumulator
P10
Usage Filter Selector
select APHits records
P1
Billing Cycle Accumulator
P2
PoolAccessor
P5
On Net/Off Net Filter
Billing Cycle Accumulator
P4
Arithmetic Calculator 2
P7
Step Rater 2
P8
Generic Bill Presenter 2
P11
PoolAccessor
P6
On/Off Net Filter
P3
Description
Amount Value
Charge Type
Output When Zero
Pool Name
Off Net Hits Served
P4.out
Information
Off Net Revenue Share Percent
P8.multiplier[1]
Information
Total Revenue Share Amount
P8.out
Charge
AP hits
P2.out
Reporting
AllianceTotalHits
AP bytes
P10.out
Reporting
AllianceTotalBytes

Figure 16

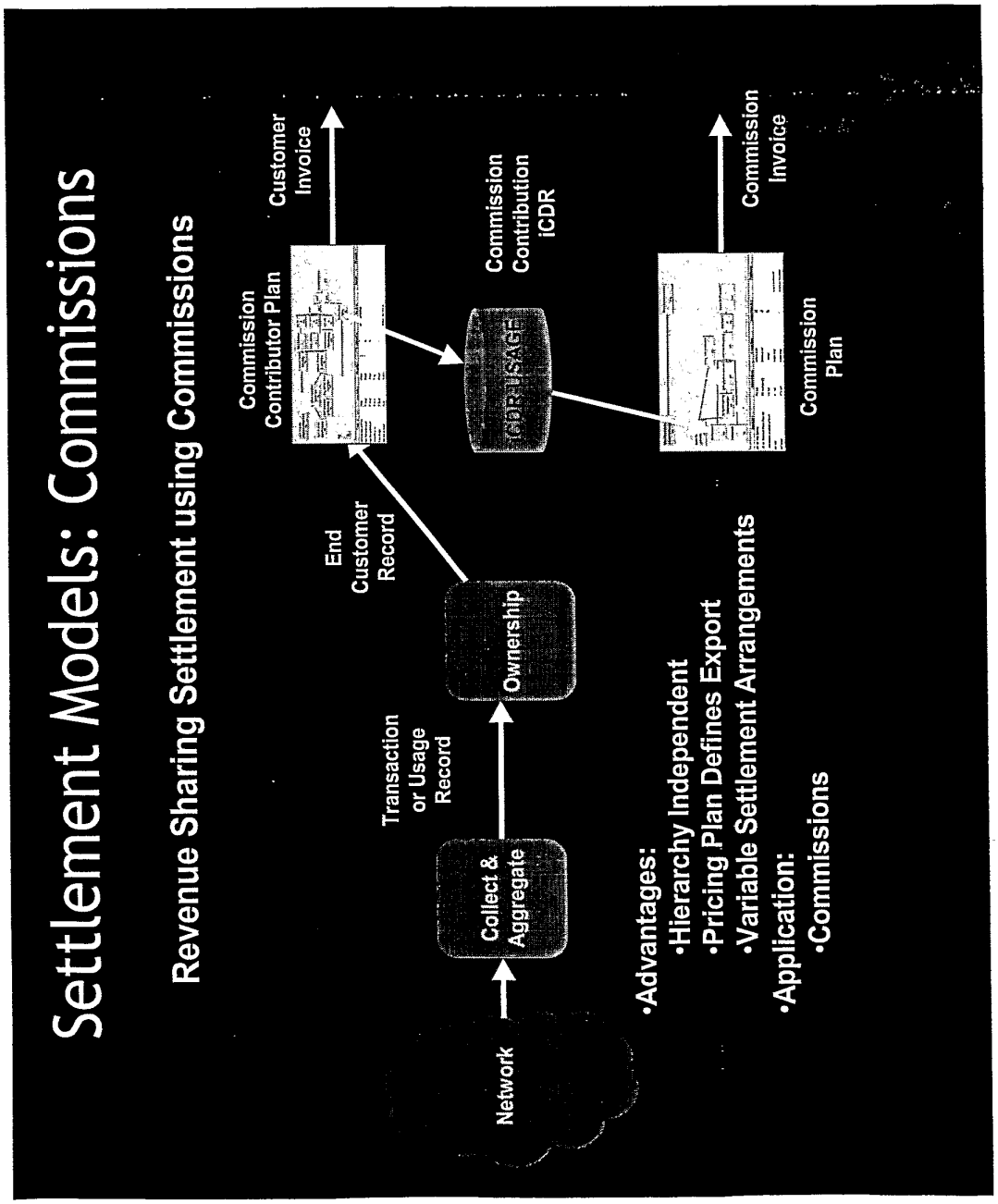

Settlement Models: Commissions
Revenue Sharing Settlement using Commissions
Network
Collect & Aggregate
Transaction or Usage Record
Ownership
End Customer Record
Commission Contributor Plan
Customer Invoice
Commission Contribution iCDR
Commission Plan
Commission Invoice
•Advantages:
•Hierarchy Independent
•Pricing Plan Defines Export
•Variable Settlement Arrangements
•Application:
•Commissions

Figure 17

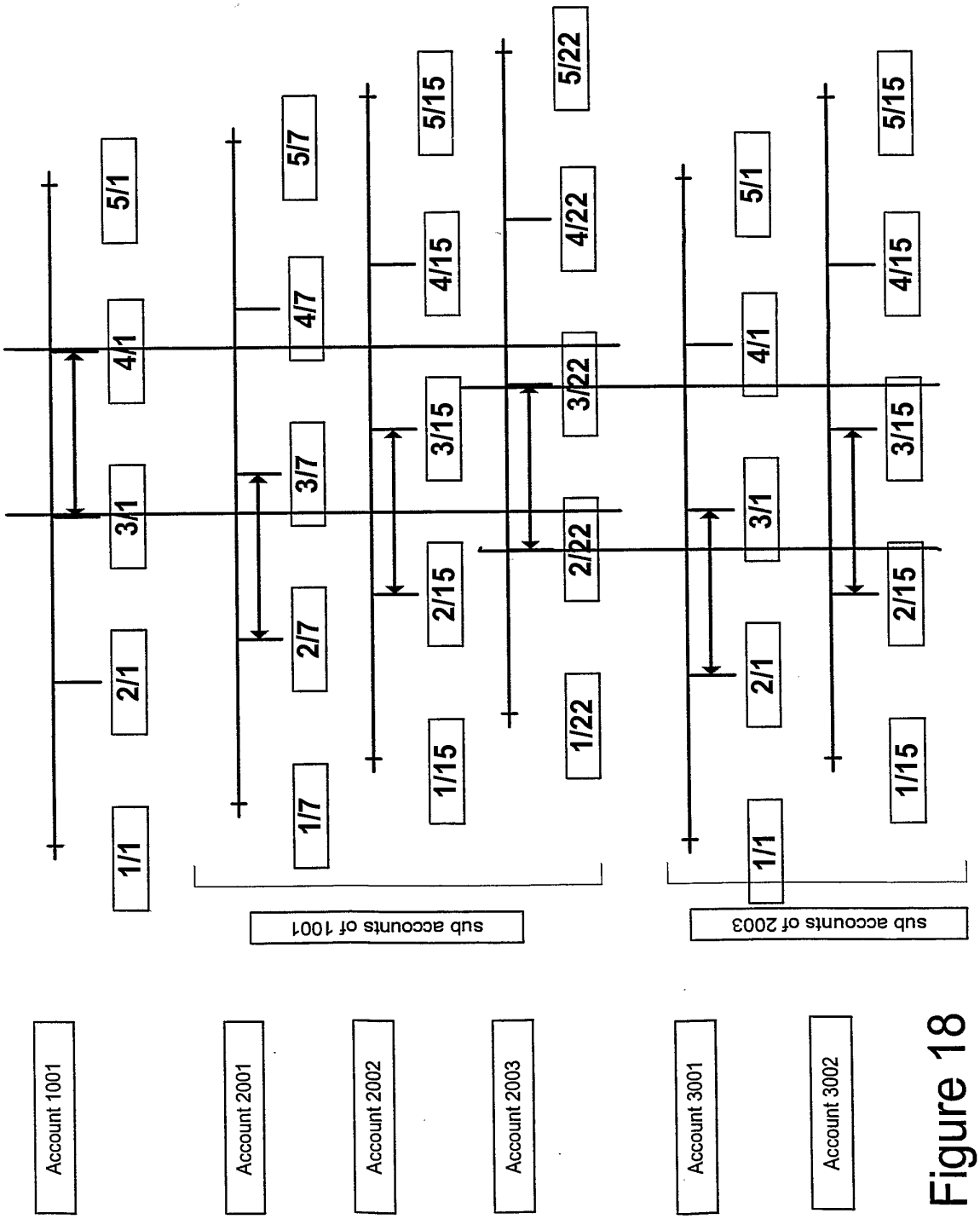

Account 1001
Account 2001
Account 2002
Account 2003
Account 3001
Account 3002
sub accounts of 1001
sub accounts of 2003
1/1
2/1
3/1
4/1
5/1
1/7
2/7
3/7
4/7
5/7
1/15
2/15
3/15
4/15
5/15
1/22
2/22
3/22
4/22
5/22

Figure 18

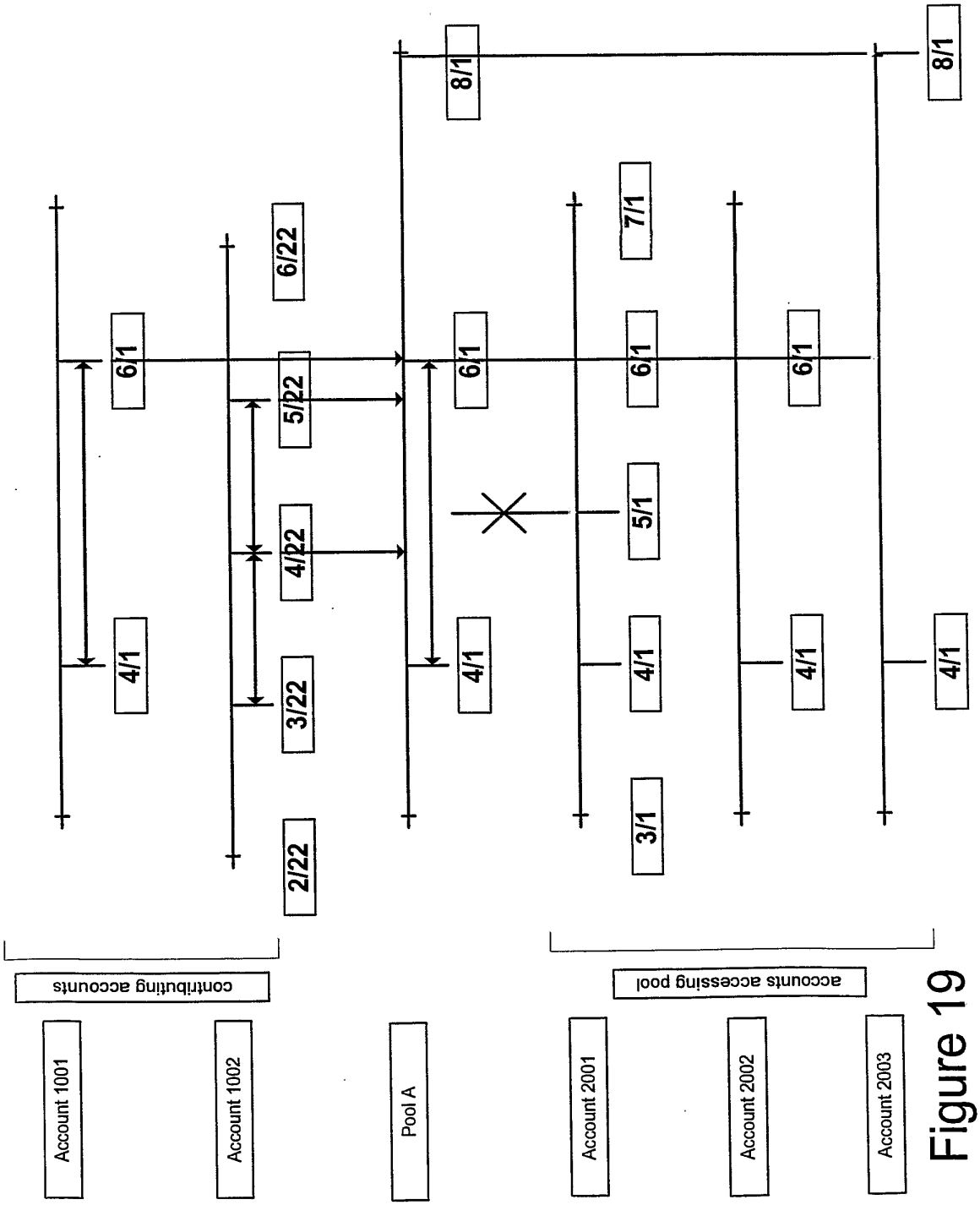

Account 1001
Account 1002
Pool A
Account 2001
Account 2002
Account 2003
contributing accounts
accounts accessing pool
2/22
3/22
4/22
5/22
6/22
7/1
8/1
6/1
4/1
5/1
3/1

Figure 19

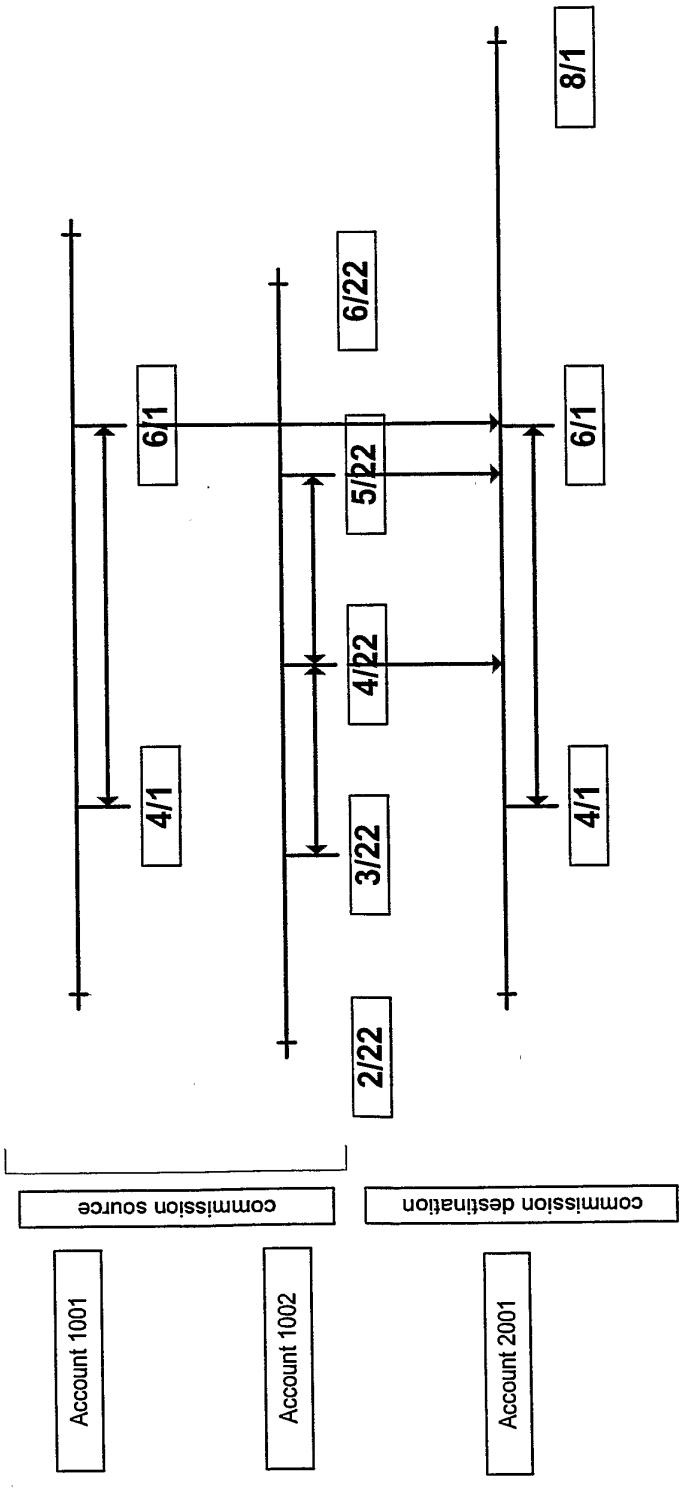

8/1
6/22
6/1
6/1
5/22
4/22
4/1
4/1
3/22
2/22
commission source
commission destination
Account 1001
Account 1002
Account 2001

Figure 20

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067616 A1

(51) International Patent Classification[7]: H04Q 7/38, H04M 15/00

(21) International Application Number: PCT/FI02/00128

(22) International Filing Date: 15 February 2002 (15.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20010302 16 February 2001 (16.02.2001) FI

(71) Applicant *(for all designated States except US)*: **SONERA OYJ** [FI/FI]; Teollisuuskatu 15, FIN-00510 Helsinki (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **YLI-KORHONEN, Jukka** [FI/FI]; Tarkka-ampujankatu 17 D 56, FIN-90120 Oulu (FI). **JUNTUNEN, Ari** [FI/FI]; Sihtikuja 1 D 51, FIN-90520 Oulu (FI). **KEINÄNEN, Kimmo** [FI/FI]; Talvikkitie 18 A 3, FIN-90580 Oulu (FI).

(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O.Box 148, FIN-00121 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), DE (utility model), DK (utility model), DM, DZ, EC, EE (utility model), ES, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM, METHOD AND NETWORK NODE FOR PROVIDING SERVICE-SPECIFIC BILLING IN A TELECOMMUNICATIONS SYSTEM

P	ID	N	S1	V	S2	SV	BV
Elvis	PT	price_today	:	number	&	0	500
Elvis	EC	extra_cutback	=	number	&	0	250
Iiris	SP	single_payment	-	number	*	250	250

(57) Abstract: In a multi-provider environment, where a network operator provides bearer services and a service provider provides the actual service, customizing billing for services requires accurate contracts concerning the content and structure of billing data transmitted by the service provider. In order to eliminate this problem, a billing content is determined for a service in such a manner that the content is available to the network operator and it determines parameters (N) provided in service billing data and indicates how to find the parameters from the billing data (ID, S1, S2). For determining billing data, definition rules are defined in advance to indicate at least the type of data that should be specified for each parameter.

WO 02/067616 A1

System, method and network node for providing service-specific billing in a telecommunications system

FIELD OF THE INVENTION

The invention relates to billing for a service transmitted in a telecommunications system, and particularly to providing service-specific billing.

BACKGROUND OF THE INVENTION

Services provided in telecommunications systems are more and more often produced in a multi-provider environment, where a network operator provides bearer services and one or more service providers provide the actual services. A service provider does not maintain a network but purchases the required bearer services from the network operator. Thus, the total price of a service is a combination of the price of the connection and the price of the actual service or content. Even in a multi-provider environment the best way to charge a client is that the network operator attends to authentication and billing of the user of the service according to the user's phone number also on behalf of the service provider. An actual bill is based on billing data transmitted by the service provider in a service response, and collected and processed by a billing data collecting system of the network operator.

A problem with such billing is that the operator and the service provider must have accurate contracts concerning the content and structure of the billing data in order that a service could be billed for in the way the service provider wants. In case of a large number of service providers, the network operator does not necessarily have time or is not able to agree in detail on the contents of the billing data with each service provider, which means that either the introduction of a service into the market will be delayed, or the service provider must arrange billing in some other manner or use an existing billing method, which may not be the best for the service in question.

BRIEF DESCRIPTION OF THE INVENTION

An objective of the invention is to develop a method and equipment implementing the method so as to solve the aforementioned problems. The objective of the invention is achieved by a method, system and network nodes, which are characterized by what is disclosed in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

The invention is based on detecting this problem and on solving it by providing a system of a network operator, preferably a system for process-

ing billing data, with a mechanism for informing the network operator of the form in which the billing data should be disclosed. The mechanism is preferably created by determining rules for defining billing parameters and by determining, by means of these rules, a billing content of a service, which is available to the network operator when forming a call detail record, and by storing the billing content in the system so as to be available to a process producing tickets. A billing content determines the service-specific parameters used in a call detail record, i.e. a ticket, and indicates how to locate the parameters in the billing data. The processing system can constitute a part of the system for collecting billing data.

An advantage of the invention is the ability to transmit and process billing data, which has different contents for different services since the billing parameters can be freely selected. Another advantage of the invention is that no specific service contract is needed between the network operator and the service provider, since the invention enables determining the structure of the billing data in such a manner that the network operator's system identifies the billing parameters and their values. Therefore the operator can provide user authentication and billing services globally to service providers. This even enables billing for free browsing, where a user is able to use all the services and not only the services of the operator or partners thereof.

BRIEF DESCRIPTION OF THE FIGURES

The invention will be described below in more detail by means of the preferred embodiments and with reference to the accompanying drawings, in which

Figure 1 shows a simplified network architecture,

Figure 2 shows an example of determining a billing content according to a first preferred embodiment of the invention,

Figure 3 shows formation of a ticket according to the first preferred embodiment of the invention, and

Figure 4 shows an example of a ticket according to the first preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention can be applied in connection with any telecommunications system where the data required for billing a subscriber is transmitted together with service data. Such systems include for example third-

generation mobile systems, such as the Universal Mobile Telecommunications System (UMTS), and mobile systems similar to the pan-European GSM (Global System for Mobile Communications), such as the GSM 1800 and the PCS (Personal Communication System), and systems based on the aforementioned systems, such as GSM 2+ systems. GSM 2+ services include the general packet radio service (GPRS) and customized applications for mobile network enhanced logic (CAMEL). The invention can also be applied in fixed systems. The invention will be described below by using as an example the GSM providing a WAP (Wireless Application Protocol) service, without restricting the invention thereto, however. The WAP is a protocol specification that enables apparatuses utilizing wireless data transmission, such as mobile phones, to use Internet services.

Figure 1 shows a simplified network architecture of a first preferred embodiment of the invention, and it illustrates only some elements of a system architecture J. Network nodes shown in Figure 1 are logical units, the implementation of which can differ from that of the figure. It is obvious to a person skilled in the art that the system can also comprise other functions and structures, which do not have to be described in more detail herein. The description of the system is by no means restrictive but only suggestive.

The system shown in Figure 1 consists of a system of a network operator VJ and a system of a service provider PJ. In the example of Figure 1, a mobile station MS user has set up a connection to a server S providing a WAP service via the network operator's network PLMN via a WAP gateway W_GW in a previously known manner. In the first preferred embodiment of the invention, the WAP gateway W_GW picks the billing data from a service response transmitted by the server and stores it in a log file, which is retrieved by a charging gateway CG connected to the network operator's network PLMN and which is processed into call detail records, i.e. tickets. An example of a ticket is shown in Figure 4. The tickets are then transmitted to a billing centre BC, which attends to billing of a user. The picking of billing data refers to picking of data used to form a ticket, such as a part of the service response containing the data required in billing. In a service response, billing data can be located for example in an HTTP (Hyper Text Transport Protocol) header. In another embodiment of the invention, the WAP gateway W_GW does not store the billing-related data that was picked into a log file but transmits the data to the charging gateway CG for example via a real-time interface. The details of

the billing, e.g. how billing data is transmitted, collected and retrieved and where it is stored, are not significant for the invention. For example, arranging billing for the WAP service is described in more detail in Finnish Patent Application 20000589 (Arranging billing in a telecommunications system), which is incorporated herein by reference.

The charging gateway CG comprises an interface I, via which service-specific billing contents LS can be determined in the charging gateway. Examples of such billing contents are shown in Figure 2. The interface I thus provides configuring means for determining the content and structure of the billing data and the ticket and for storing them by means of the definition rules for billing parameters. Billing contents are preferably stored in a memory M of the charging gateway. The network operator has usually determined the definition rules and the service provider determines the actual billing content of the service, i.e. it determines the required parameters and provides parameter specifications. The actual billing content is input/processed into the memory M of the charging gateway via the interface I by the operator or the service provider, depending on their mutual agreement. The interface I can also be arranged to check, in connection with the input or processing of the billing content, that the parameter specifications comply with the definition rules. The definition rules are preferably the same for all the service providers, but the network operator can also customize the rules separately for each service provider. Inputting billing contents does not preferably require a service contract between the service provider and the network operator, but the service provider may be able to input billing contents for example via the Internet after having accepted certain rules and passed a log-in process. The charging gateway CG also comprises processing means, i.e. a process P, which converts the billing data into a ticket by means of the billing content specified for the service. The operation of the process P will be described in more detail in connection with Figure 3.

Depending on the embodiment, the interface I can be located in a different network node than the stored billing contents LS. Neither has to be located in the charging gateway. A network node where the billing contents LS are stored comprises means for receiving requests on billing contents and means for processing and transmitting responses.

In addition to prior art means, a system implementing the functionality of the present invention and the network nodes of the system comprise

means for creating and storing service-specific billing contents. The system and the network nodes can also comprise means for processing a billing content. The means are preferably implemented by using the present network nodes, especially the processors and memory thereof. All the modifications required to implement the invention can be carried out in the form of added or updated software routines, application-specific integrated circuits (ASIC) and/or programmable circuits.

Figure 2 shows a manner according to the first preferred embodiment of the invention of determining service-specific billing contents stored in a database table where each service-specific parameter to be taken into account in billing is provided with required data, i.e. the parameters are determined according to the definition rules. It is assumed in the first preferred embodiment of the invention that a billing ticket consists of standard data and service-specific data. Parameters for the standard data are determined generally in the first preferred embodiment, i.e. they are shared by all services. Such standard data includes for example user identifier, service name, service status data, and time. Standard data or some part of it can be transmitted with service-specific billing data, but for example in case of WAP services they are usually obtained in some other manner. Service-specific data is determined in the billing content of a service. The parameters that should be or may be specified in the billing content naturally depend on the operator, the billing system used by the operator, and the form in which billing data is transmitted. These matters are described in the definition rules. The essential fact in the billing content of an individual service is that it can be connected to a specific service and that at least one billing parameter is determined in such a manner that the billing parameter and the value thereof can be somehow separated from the billing data. However, in the first preferred embodiment of the invention it is not necessary to determine a billing content for all the services if standard data is sufficient to bill for a service.

In the example shown in Figure 2, it is assumed for the sake of clarity that the service name identifies the service sufficiently, i.e. the service cannot be confused with any other service, and different service providers do not have services with similar names. In embodiments where a mere service name does not identify a service sufficiently accurately, a service to be billed for can be identified for example based on the names of both the service provider and the service.

In the first preferred embodiment of the invention, the definition rules do not restrict in any way the ability of service providers to determine the parameters to be taken into account in billing, and the only requirement is that each parameter of a service billing content is provided with not only a name N but also the following data:

- The service P to which the parameter is related. A parameter defined by means of a service can be connected to the service billing content,
- A parameter identifier ID used in billing data to help locate the parameter and the value thereof,
- A separator S1 between an identifier and the value thereof in the billing data,
- Value type V,
- The allowed range of variation of the value indicated by means of the lowest value SV and the highest value GV, and
- A separator S2 between the identifiers.

On the basis of this data, a single ticket may contain 1 to n items of service-specific billing data, which are mutually independent. The billing data can even consist of data not used by the network operator in its own billing. For example based on the specifications shown in Figure 2, a ticket formed of a service called 'Elvis' contains the billing value of two parameters in the service-specific data, and a ticket formed of a service called 'Iiris' contains the billing value of one parameter. The same parameter can also be used in different services and with different ranges of variation. Eliminating parameters from or adding new parameters into a service is easy and simple in the first preferred embodiment of the invention. It is also easy and simple to alter parameter specifications, for example to update the allowed range of variation.

In a preferred embodiment of the invention, the operator can restrict parameter specifications for example by limiting the maximum number of parameters used in one service or by restricting the allowed value types to numbers only. The operator can also determine its own set of billing parameters, which it offers to service providers. The service providers then select from the set of billing parameters the parameters they want to use in billing for each service.

In a preferred embodiment of the invention, parameters and their values to be used in standard data are also specified in the billing content of

each service. In this way standard data can also be configured specifically for each service/service provider.

In another preferred embodiment of the invention, a common billing content is also determined and used for services with no specified billing content of their own. A common billing content can also be determined specifically for each service provider and/or service type. If a service-type-specific billing content is used, the service type is indicated in a service response either directly or indirectly in order that the correct billing content can be selected when forming a ticket. The same applies to service-provider-specific billing contents as well. The service type can be concluded for example based on the service when the system maintains data that links each service to a service type.

In a preferred embodiment of the invention, also a broader description of a parameter, such as the manner of use or the meaning in billing, can be stored in the billing content.

In another preferred embodiment of the invention, several different identifiers with different value ranges can be stored for one parameter in a billing content. In this embodiment, only one such identifier is shown in the billing data.

If the highest allowed value of the identifiers is equal to the lowest allowed value, in a preferred embodiment of the invention the billing data does not have to contain a value for the parameter, but it is possible to use the value determined in the billing content when forming a ticket.

In the other embodiments of the invention, the predetermined definition rules can differ from what is shown in Figure 2. It is sufficient that the definition rules ensure that the parameters in the billing content are known and that they will be found from the billing data.

Figure 3 shows a flowchart of how a ticket (or a part thereof, if one ticket combines the billing data of several service responses) is formed according to the first preferred embodiment of the invention from the billing data in the service response. It is assumed in the example of Figure 3 that the service provider has transmitted billing data or that the billing data field is not empty. An empty billing data field is preferably not processed at all. The example of Figure 3 does not determine at which stage the tickets should be transmitted to the billing centre. In the first preferred embodiment of the invention, service-specific billing data is transmitted in HTTP headers of a service response. Transmitting billing data as a part of an HTTP header has an advantage that

the data is not transmitted from the gateway, such as the WAP gateway, to the subscriber of the service. Furthermore, an HTTP header is an efficient channel of data transmission between a service provider and an operator.

Since it is not significant for the invention how the billing data is found for example from a log file, the starting point of Figure 3 is that in step 301 the processing of billing data is initiated. For example in the first preferred embodiment of the invention, the WAP gateway picks the billing data from the HTTP header of the service response for the WAP service on the basis of a carriage return. An example of billing data will be described below. The payer is identified first in step 302. The payer can be for example the end user or the service provider, such as a service provider providing a commercial WAP/SMS push service. A payer is identified according to the system used. In the present WAP services, a user is identified based on a phone number received during the set-up of the connection. In the future third-generation mobile systems and in general Internet-based services, the end user can be identified for example from the service log-in data transmitted by the service provider. It is also possible to identify both the payer and the user. After the payer has been identified, the service to which the billing data is related is identified in step 303. The service can be identified either directly by means of an identifier indicating the service name in the HTTP header, or by means of an analysis of a URL (Uniform Resource Locator) address. After the service has been identified, the standard data is retrieved from the billing data and stored (or the part of the standard data not received via some other route/earlier) in a ticket in step 304, and the service billing content is retrieved in step 305. The service billing content is retrieved in the first preferred embodiment of the invention by checking the database table shown in Figure 2 and by picking all the parameters with their specifications that relate to the service to be billed for. In step 306, it is checked whether a billing content was obtained. In other words, it is checked whether a billing content has been specified for the service. If a billing content was obtained (i.e. has been specified), the processing of the first parameter is initiated in step 307 and a corresponding identifier is retrieved from the HTTP header in step 308. If such an identifier was found (step 309), the value given for the identifier is retrieved in step 310. It is thereafter checked in step 311 whether the value is allowed, i.e. whether it is within predetermined limits and of a specified type. If the value was allowed, the parameter name and value are stored in the ticket in step 312, and it is checked in step 313 whether the

parameter was the last parameter of the billing content. If the parameter was not the last one, the next parameter is subjected to processing in step 314, whereafter the process proceeds from step 308 by searching the HTTP header for the corresponding identifier.

If the parameter was the last one (step 313), the processing of the billing data is terminated in step 315.

If the parameter value was not allowed (step 311), a failure report is generated to the system in step 316, and the ticket field in question is left empty. After the failure report has been generated, the process proceeds to step 313 to check whether the processed parameter was the last one in the billing content.

If a parameter identifier was not located (step 309), the process proceeds to the last step 313 to check whether the processed parameter was the last parameter in the billing content. In other words, it is assumed in the first preferred embodiment of the invention that this time the service provider did not want to use this parameter for billing. Such a parameter can be for example an additional discount parameter.

If a billing content was not obtained (step 306), it has not been determined for the service, wherefore the processing of the billing data is terminated in step 315.

In a preferred embodiment of the invention, at least some of the parameter specifications of the standard data are contained in the service billing content. In this embodiment, the billing content must be retrieved (step 306) before step 304, i.e. the retrieval and storage of the standard data.

In a preferred embodiment of the invention, all the parameters, including the parameters of the standard data transmitted in the billing data, such as a service identifier, are determined at least specifically for each service provider. In this embodiment, the processing of the billing data is initiated by first identifying the service provider, whereafter the database table is checked in order to retrieve the service-provider-specific parameters, such as a service identifier and possibly at least some of the standard data. After the service has been identified, the parameters specified for the service are retrieved. This provides the billing content, and the parameter values thereof are retrieved in the manner described above.

The steps of Figure 3 are not in an absolute order of time. Some of the aforementioned steps can take place simultaneously or in another order,

such as steps 304 and 305. Some steps can be skipped, or steps not shown in Figure 3 can be implemented between the steps. Some steps can also be replaced with a corresponding step. For example in an embodiment where the log file only comprises notes containing billing data and where a service-type-specific billing content is used for each service, step 306 can be skipped and step 303 can be replaced with a step of identifying the service type.

Figure 4 shows an xml (eXtendable Mark up Language) ticket CDR according to the first preferred embodiment of the invention, where the WAP service 'Elvis' has been subscribed to from mobile phone number 040555555. The billing content of the service has been specified as shown in Figure 2 and the billing data is indicated as follows in the HTTP header of the service response:

X-up-billing-Info:SN=elvis&PT:67&EC=15

In the first preferred embodiment, the ticket comprises standard data 1 and a part 2 that changes according to the service. The service-specific part 2 is determined according to the billing content defined for the service. In the first preferred embodiment of the invention, the standard data 1 includes a calling party identifier 11, billing data 12 in the HTTP header, a service name 13, and a service price class 14, which is used to distribute different services of the same service provider to different price classes. The standard data is followed by the changing part 2 of the ticket, which is not found in tickets related to a service for which a billing content has not been specified. By means of the definitions shown in Figure 2, the process forming a ticket is able to retrieve from the billing data an identifier and a value corresponding to each parameter specified for the service 'Elvis'.

Even though the above description relates to the use of the billing content for altering a ticket, it can also be applied to other functions related to billing, such as selecting what to store in a log file.

It is obvious to a person skilled in the art that as the technology develops, the basic idea of the invention can be implemented in several manners. The embodiments of the invention described above or the individual characteristics thereof can be combined to provide new embodiments. Thus, the invention and the embodiments thereof are not restricted to the above examples, but they may vary within the scope of the claims.

CLAIMS

1. A method of providing service-specific billing in a telecommunications system, where a system of a network operator transmits services of at least one service provider to a subscriber, and forms call detail records to be used in billing and containing at least one billing parameter and the value thereof, **characterized** in that the method comprises at least the following steps of:

determining rules for defining billing parameters,

determining, by means of the definition rules, a billing content for at least one service, the content containing at least one service-specific billing parameter and indicating how the parameter is found from billing data transmitted during the use of the service, and

storing the billing content in the telecommunications system such that it is available to the system of the network operator.

2. A method according to claim 1, **characterized** in that the method also comprises a step of forming, from the billing data, a call detail record, which contains at least a service-specific part comprising service-specific billing parameters and their values defined in the billing content.

3. A method according to claim 1 or 2, **characterized** in that the method also comprises the steps of

determining at least one set of billing parameters, and

selecting the billing parameters to be used in the billing content from the set of billing parameters.

4. A method according to claim 1, 2 or 3, **characterized** by determining a billing content for one service.

5. A method according to claim 1, 2 or 3, **characterized** by determining a billing content for a service type, and indicating the service type in the billing data.

6. A telecommunications system (J) comprising

a system of a service provider (PJ) for transmitting at least one service to a subscriber and for providing billing data related to the service, and

a system of a network operator (VJ) for transmitting the service from the service provider's system to the subscriber of the service, and for providing a call detail record to be used in billing of the subscriber by means of the billing data, and

a memory (M) for storing different specifications,

characterized in that

the system of the network operator (VJ) comprises an interface (I) for storing a billing content (LS) in the memory (M) for the service, the billing content determining at least one service-specific billing parameter of the billing data according to the predetermined definition rules, such that the billing parameter is found from the billing data transmitted during the use of the service.

7. A system according to claim 6, **characterized** in that the system of the network operator (VJ) is arranged to utilize the specifications of the billing content in forming a call detail record from the billing data related to the service.

8. A system according to claim 6, **characterized** in that the system of the network operator (VJ) is arranged to form a call detail record (CDR) for the service from standard data (1) containing the same parameters for all the services, and from service-specific data (2) according to the billing content defined for the service.

9. A system according to claim 6, 7 or 8, **characterized** in that the interface (I) is also arranged to alter the specifications of the billing content.

10. A system according to claim 6, 7, 8 or 9, **characterized** in that the interface (I) is also arranged to check, in connection with said storage, whether the parameter specifications comply with the definition rules.

11. A system according to claim 6, 7, 8, 9 or 10, **characterized** in that the system (J) is based on a GPRS system.

12. A system according to claim 6, 7, 8, 9 or 10, **characterized** in that the system (J) is based on a UMTS.

13. A network node (CG) in a telecommunications system where a system of a network operator transmits services of at least one service provider to a subscriber and provides call detail records used in billing, and where the service provider transmits billing data in connection with a service,

characterized in that

the network node comprises configuring means (I) for specifying parameters contained in the service billing data according to predetermined definition rules, such that the system of the network operator can use the specifications in forming a call detail record related to the service.

14. A network node according to claim 13, **characterized** in

that the configuring means (I) are arranged to alter the parameter specifications.

15. A network node according to claim 13 or 14, **characterized** in that the network node also comprises processing means (P) for forming a call detail record from the billing data related to the service, such that at least a part of the call detail record is formed according to the parameter specifications for the service.

16. A network node (CG) in a telecommunications system, where a system of a network operator transmits services of at least one service provider to a subscriber, and where the service provider transmits billing data in connection with a service, the network node comprising processing means (P) for forming a call detail record from the billing data related to the service,

characterized in that

the processing means (P) are arranged to determine a billing content specified for the service according to predetermined definition rules in the system of the network operator, the billing content containing at least service-specific billing parameters and indicating how the parameters can be found from the billing data, the processing means being also arranged to form a call detail record in such a manner that at least a part of the call detail record complies with the billing content.

17. A network node (CG) according to any one of claims 13 to 16, **characterized** in that the means (I, P) are implemented by software routines.

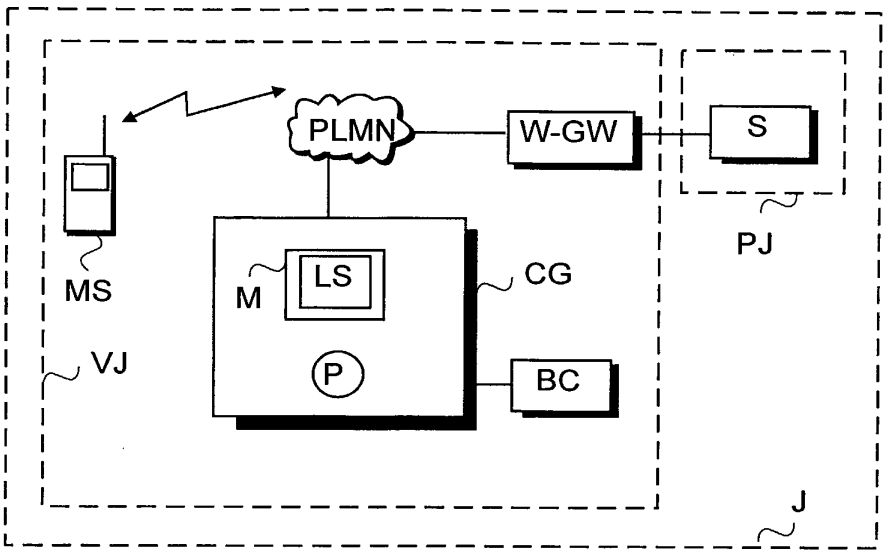


FIG.1

P	ID	N	S1	V	S2	SV	BV
Elvis	PT	price_today	:	number	&	0	500
Elvis	EC	extra_cutback	=	number	&	0	250
Iiris	SP	single_payment	-	number	*	250	250

FIG.2

CDR

<user_msisdn>040555555</user_msisdn>

11 <header>SN=elvis&RC=99&PT:67&EC=15</header>

12 <service_name>ELVIS</service_name>

13 <rate_category>99</rate_category>

1

<psd>
<price_today>67</price_today>
<extra_cutback>15</extra_cutback>
</psd>

2

FIG.4

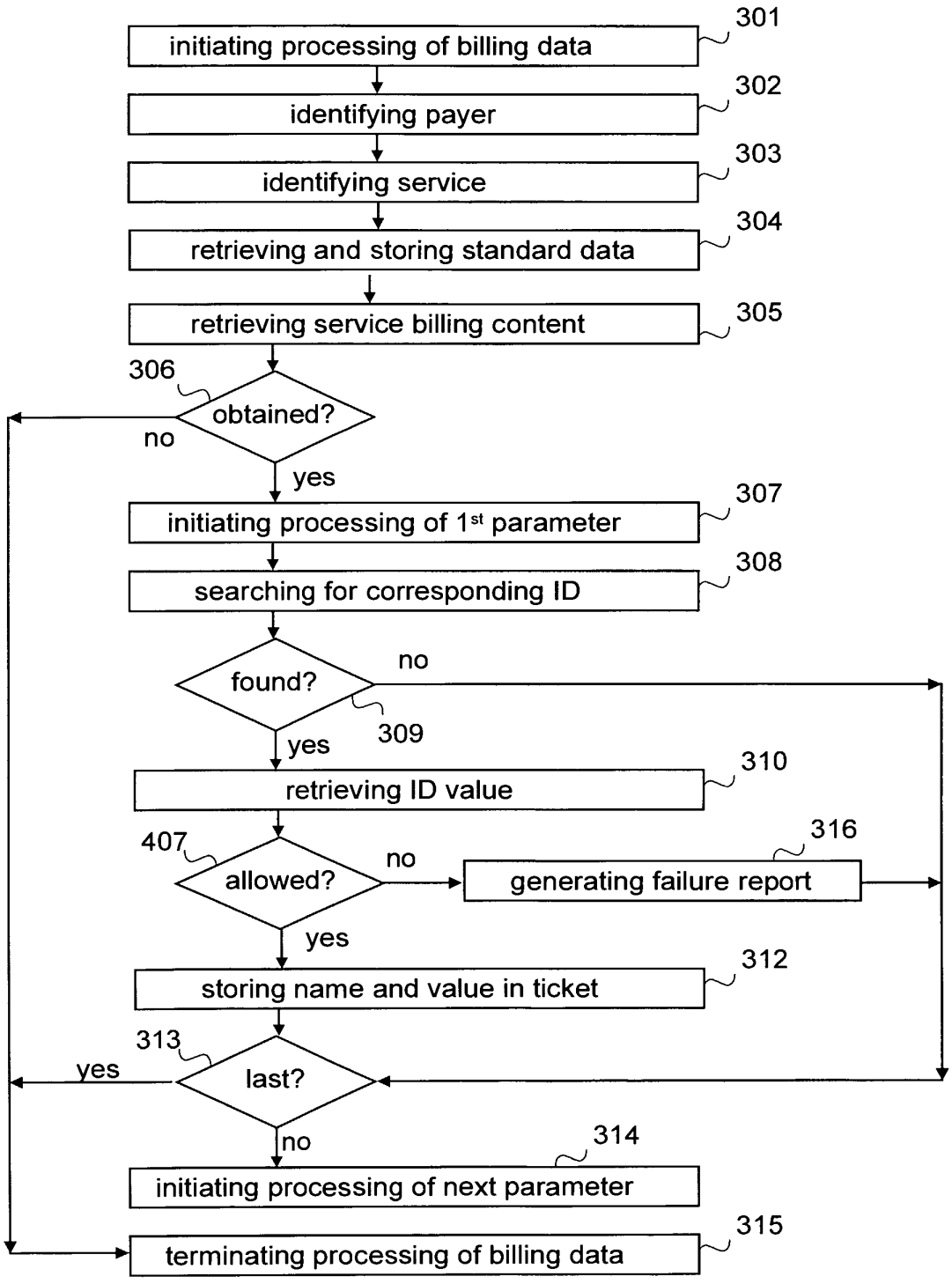

initiating processing of billing data
301
identifying payer
302
identifying service
303
retrieving and storing standard data
304
retrieving service billing content
305
306
obtained?
no
yes
initiating processing of 1st parameter
307
searching for corresponding ID
308
found?
no
309
yes
retrieving ID value
310
407
allowed?
no
316
generating failure report
yes
storing name and value in ticket
312
313
yes
last?
no
314
initiating processing of next parameter
315
terminating processing of billing data

FIG.3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00128

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04M 15/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5982864 A (JAGADISH ET AL), 9 November 1999 (09.11.99), column 3, line 48 - column 4, line 18, figure 1b, column 7, line 28 - line 32, column 5, line 19 - line 22	1-9,11-17
A	abstract	10
	--	
A	US 6047051 A (GINZBOORG ET AL), 2 April 2000 (02.04.00), abstract	1-17
	--	
P,A	WO 0191003 A2 (ZTANGO, INC), 29 November 2001 (29.11.01), claim 3, abstract	1-17
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 May 2002	06 -06- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Malin Söderman /js Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 0133456 A2 (AP ENGINES, INC), 10 May 2001 (10.05.01), page 2, line 15 - line 21, abstract ---	1-17
A	WO 0065812 A1 (TELIA AB), 2 November 2000 (02.11.00), page 19, line 6 - line 15 --- --------	1-17

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/05/02

International application No.
PCT/FI 02/00128

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5982864 A	09/11/99	NONE	
US 6047051 A	02/04/00	AU 730689 B	15/03/01
		AU 4871297 A	03/06/98
		BR 9713014 A	25/01/00
		EP 1012760 A	28/06/00
		FI 964524 A	12/05/98
		NZ 335701 A	27/10/00
		WO 9821676 A	22/05/98
WO 0191003 A2	29/11/01	AU 6333001 A	03/12/01
		US 2002029197 A	07/03/02
WO 0133456 A2	10/05/01	AU 1346901 A	14/05/01
WO 0065812 A1	02/11/00	AU 1191900 A	01/05/00
		EP 1117340 A	25/07/01
		EP 1180297 A	20/02/02
		NO 20015022 A	18/12/01
		SE 9901509 A	28/10/00

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2011 (06.01.2011)

PCT

(10) International Publication Number
WO 2011/002450 A1

(51) International Patent Classification:
H04M 15/00 (2006.01) *H04W 4/24* (2009.01)

(21) International Application Number:
PCT/US2009/049255

(22) International Filing Date:
30 June 2009 (30.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants *(for all designated States except US)*: **ALCATEL-LUCENT USA INC** [US/US]; 600-700 Mountain Avenue, Murray Hill, New Jersey 07974-0636 (US). **ALCATEL-LUCENT SHANGHAI BELL COMPANY** [CN/CN]; 388#, Ningqiao Road, Pudong Jinqiao, Shanghai 201206 (CN).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CAI, Yigang** [CN/US]; 23643 Royal Worlington Drive, Naperville, Illinois 60564 (US). **LI, Xiangyang** [CN/CN]; Bo Ya Xi Yuan 13-1-502# Nong Da Nan Lu, Hai Dian District, Beijing 100094 (CN).

(74) Agent: **BORNSEN, Brett**; Alcatel-Lucent Usa Inc, Docket Administrator - Room 2F-192, 600-700 Mountain Avenue, Murray Hill, New Jersey 07974-0636 (US).

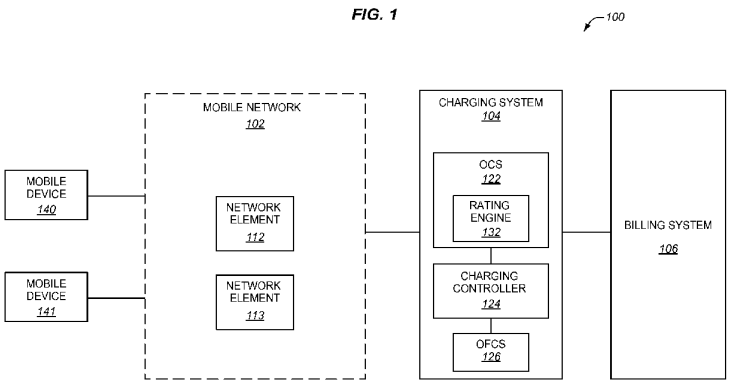
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) **Title**: FRONT-END CHARGING SYSTEM THAT GENERATES CHARGING DATA PER ENTITY HAVING A REVENUE SHARE

FIG. 1



(57) **Abstract**: Charging systems and methods are disclosed for determining the share of call revenue for multiple entities. One embodiment comprises a charging controller that is coupled to a mobile network and an online charging system. The charging controller receives charging data for a call in the mobile network, and processes the charging data and charging rules to identify entities that have a share in revenue for the call. The charging controller generates a charging request message indicating the entities having a revenue share in the call, and transmits the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

WO 2011/002450 A1

FRONT-END CHARGING SYSTEM THAT GENERATES CHARGING DATA PER ENTITY HAVING A REVENUE SHARE

Background

1. Field of the Invention

The invention is related to the field of communication networks and, in particular, to charging and billing in communication networks.

2. Statement of the Problem

When a phone call is placed over a communication network, there may be multiple entities that share in the revenue received for the call. For instance, the network operator that actually operates and maintains the network over which the call is placed shares in the revenue. If the call extends to a foreign communication network, such as for an international call, then the network operator of the foreign communication network shares in the revenue for the call. If a call extends to a roaming mobile user, then the network operator of the mobile network in which the user is roaming shares in the revenue. The process of determining which entities share in the revenue of a call is sometimes referred to as mediation.

In traditional communication networks, charging functions for calls are performed by network components, such as switches. Switches collect charging data for the calls, and generate Charging Detail Records (CDR) that include the charging data. Switches all over the entire network forward the CDRs to a billing system in service provider's IT system (often referred to as a back-end or back-office billing system). The back-office billing system stores information that may be used for the mediation process. For example, the billing system stores agreements that a network operator may have with a foreign network operator for international calls, stores agreements that a network operator may have with mobile networks for roaming scenarios, etc. The billing system also performs settlement processes to invoice customers for the telephone services, and to provide vouchers or credits to other entities.

In more recent charging architectures, postpaid charging is implemented through an Offline Charging System (OFCS) and an associated billing system. Similarly, prepaid charging is implemented through an Online Charging System (OCS) and an associated billing system. To provide offline and online charging, the OCS and the billing systems

each maintain their own rating engine. Also, the billing systems each maintain profiles for the subscribers, profiles for the wholesale customers, and profiles for other network operators having contractual agreements. The overlap of the rating engines and the profiles wastes significant resource in the network. Operational inefficiencies and technical overhead for maintaining two separate charging systems may lead to the drawback in marketing and business activities for a network operator. Presently, the network operators are subject to great pressures to reduce the operational costs.

Summary

Embodiments described herein are able to manage the flow of revenue to the appropriate entities for a call using a converged charging system. The converged charging system centralizes prepaid charging, postpaid charging, interconnect charging, wholesale charging, content charging, roaming charging, etc. Thus, revenues for a call may be divided among multiple entities based on the applicable charging types. This will significantly reduce the work in the back office, and create near real-time billing. The converged charging system also enables the rating or billing-related activity to share a common rating engine and a common account balance management function, which reduces the cost for system deployment, operation, and maintenance.

One embodiment comprises a charging controller that is coupled to a mobile network and an online charging system. The charging controller is operable to receive charging data for a call in the mobile network, and to process the charging data for the call and charging rules to identify entities that have a share in revenue for the call. The charging controller is further operable to generate a charging request message indicating the entities having a revenue share in the call, and to transmit the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

In another embodiment, the online charging system is operable to receive the charging request message from the charging controller, and to identify a profile for each of the entities having a revenue share. The online charging system is further operable to determine a revenue share amount for each of the entities based on their profile and a rating, to generate charging records indicating the revenue share amount for each of the entities, and to transmit the charging records to the charging controller.

In yet another embodiment, the charging controller is further operable to receive the charging records, to correlate the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities, and to transmit the consolidated charging record to a billing system.

Other exemplary embodiments may be described below.

Description of the Drawings

Some embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings. The same reference number represents the same element or the same type of element on all drawings.

FIG. 1 illustrates a communication network in an exemplary embodiment.

FIG. 2 is a flow chart illustrating a method of charging for a call by generating charging data for each entity having a revenue share in an exemplary embodiment.

FIG. 3 is a flow chart illustrating a method of determining the revenue share for multiple entities in an exemplary embodiment.

FIG. 4 is a flow chart illustrating a method of correlating charging records in an exemplary embodiment.

FIG. 5 illustrates another communication network in an exemplary embodiment.

FIG. 6 illustrates how the revenue for a call is divided among entities in an exemplary embodiment.

FIG. 7 is a message diagram illustrating how revenue for a call is divided in an exemplary embodiment.

Description of Embodiments

The figures and the following description illustrate specific exemplary embodiments of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the invention and are included within the scope of the invention. Furthermore, any examples described herein are intended to aid in understanding the principles of the invention, and are to be construed as being without limitation to such specifically recited examples and conditions. As a result, the invention is not limited to the specific embodiments or examples described below, but by the claims and their equivalents.

FIG. 1 illustrates a communication network 100 in an exemplary embodiment. Communication network 100 includes a mobile network 102, a charging system 104, and a billing system 106. Mobile network 102 may comprise a circuit-based network, such as a CDMA network or a GSM network, may comprise a packet-based network, such as an IP Multimedia Subsystem (IMS) network, or a mix of the two. Mobile network 102 is able to provide service to mobile devices 140-141 to place voice calls, to initiate data sessions, to send or receive text messages or multimedia messages, etc. Mobile network 102 includes a plurality of network elements 112-113 that are operable to serve a session/call or provide a service for a session/call within mobile network 102. For example, network element 112 may comprise a Serving-Call Session Control Function (S-CSCF) while network element 113 may comprise an application server (AS) in an IMS network. Alternatively, network element 112 may comprise a Mobile Switching Center (MSC) while network element 113 may comprise an SGSN of a UMTS network.

Charging system 104 comprises any system, server, or function operable to provide online and/or offline charging for sessions/calls in mobile network 102. For the online/offline charging, charging system 104 is able to generate consolidated charging records for sessions/calls within mobile network 102, and send the CDRs to billing system 106. Charging system 104 includes an online charging system (OCS) 122, a charging controller 124, and an offline charging system (OFCS) 126. OCS 122 includes a common rating engine 132 that may be shared by OCS 122 and OFCS 126, and may include other functions that are not shown. OFCS 126 may also include a variety of functions that are not shown for the sake of brevity, such as a Charging Data Function (CDF)/Charging Gateway Function (CGF) as defined by the 3GPP in Release 6, or a Charging Collector Function (CCF) as defined by the 3GPP in Release 5.

Billing system 106 comprises any system, server, or function operable to receive a consolidated charging record for a session/call, and to invoice one or more customers for the session/call based on the consolidated CDR or issue a voucher or credit.

For a call, there may be a variety of different types of charging involved. Some common types of charging are as follows. One type of charging is referred to as retail charging. Retail charging occurs between a mobile network operator (MNO) or a mobile virtual network operator (MVNO) and an end user. Thus, retail charging defines how end users pay for services provided by the MNO (or MVNO).

Another type of charging is referred to as wholesale (or MVNO) charging. Wholesale charging occurs between an MVNO and an MNO. A wholesale customer purchases mobile products and services from an MNO for resale. Wholesale charging defines how the MVNO pays for services provided by the MNO.

Another type of charging is referred to as content charging. Content charging occurs between a content provider and an MNO (or MVNO). The content provider supplies some content/service to end users via the MNO/MVNO network. Thus, content charging defines how the MNO/MVNO pays for the content supplied by the content provider.

Another type of charging is referred to as interconnect charging. Interconnect charging occurs between an MNO and another network operator. When a call is originated in the MNO's network but is terminated in network of the other operator (or vice-versa), interconnect charging defines how the MNO pays for services provided by the other network operator.

Another type of charging is referred to as roaming charging. Roaming charging occurs between an MNO and other MNO that is serving a roaming user. When an end user of one MNO (visiting MNO) is roaming in the network of another MNO (visited MNO), roaming charging defines how the visiting MNO pays for services provided by the visited MNO.

There may be other types of charging that apply to the description provided below. One common thread for each of these charging types is that multiple entities will share in the revenue of a call. Thus, the revenue has to be divided at some point and allocated appropriately to each of the entities. In a traditional charging architecture, a charging system generates CDRs that include charging data for a call. A back-office billing system then processes the charging data from the CDRs to divide the revenue for the call to entities that have a share. Thus, the revenue is divided in back-office systems instead of in the actual charging system. In the embodiments described below, a new charging controller 124 is implemented in the charging architecture to divide the revenue. Thus, revenue sharing entities for a call are identified in charging system 104 instead of in back office systems.

Assume for this embodiment that mobile device 140 is involved in a call over mobile network 102. One or both of network elements 112-113 may provide a service for the call, and generate charging data for providing the service. Those skilled in the art will appreciate that other mobile networks (not shown) and other fixed networks (not shown)

may also be involved in the call. Network elements 112-113 then transmit the charging data to charging system 104. For example, if prepaid charging applies for the call, then network elements 112-113 may transmit a Diameter Ro Credit Control Request (CCR) to charging system 104. If postpaid charging applies for the call, then network elements 112-113 may transmit a Diameter Rf Accounting Request (ACR) to charging system 104. Charging controller 124 manages charging for the call as is illustrated in FIG. 2.

FIG. 2 is a flow chart illustrating a method 200 of charging for a call by generating charging data for each entity having a revenue share in an exemplary embodiment. The steps of method 200 will be described with reference to communication network 100 in FIG. 1, but those skilled in the art will appreciate that method 200 may be performed in other networks and systems. The steps of the flow charts described herein are not all inclusive and may include other steps not shown. The steps may also be performed in an alternative order.

In step 202, charging controller 124 receives charging data for the call in mobile network 102. The charging data may be received in a charging request message from mobile network 102, such as a Diameter Ro CCR or a Diameter Rf ACR. Alternatively, the charging data may be received in a CDR from OCS 122 or OFCS 126. In step 204, charging controller 124 processes the charging data for the call and charging rules to identify entities that have a share in revenue for the call. Charging controller 124 stores charging rules that define conditions for different types of charging. For example, the charging rules may include retail rules defining conditions for retail charging. The charging rules may include wholesale rules defining conditions for wholesale charging. The charging rules may include interconnect rules defining conditions for interconnect charging. The charging rules may include content rules defining conditions for content charging. The charging rules may include roaming rules defining conditions for roaming charging.

As an example, charging controller 124 may process the calling party number and wholesale rules to determine that wholesale charging applies, and to determine the identity of the wholesale entity. Charging controller 124 may also process the called party number and interconnect rules to determine that interconnect charging applies, and to determine an identity of the network operator entity providing the interconnect service. Based on the charging data, charging controller 124 is able to generate a list of entities that have a share in the revenue for the call.

In step 206, charging controller 124 generates a charging request message indicating the entities having a revenue share in the call. For example, charging controller 124 may generate a Diameter Ro CCR, and insert the identities of the revenue sharing entities in the CCR. In step 208, charging controller 124 transmits the charging request message to OCS 122. Charging controller 124 may transmit a separate charging request message for each of the identified revenue sharing entities, or may transmit a single charging request message for all of the identified revenue sharing entities. Based on the data included in the charging request message, OCS 122 is able to determine the revenue share for each of the entities, which is further illustrated in FIG. 3.

FIG. 3 is a flow chart illustrating a method 300 of determining the revenue share for multiple entities in an exemplary embodiment. The steps of method 300 will be described with reference to communication network 100 in FIG. 1, but those skilled in the art will appreciate that method 300 may be performed in other networks and systems. In step 302, OCS 122 receives the charging request message from charging controller 124. In step 304, OCS 122 identifies a profile for each of the entities having a revenue share as indicated in the charging request message. OCS 122 may maintain a database of profiles for each entity. For example, OCS 122 may maintain a profile for mobile device 140 that indicates a service plan subscription of its end user. OCS 122 may maintain a profile of other MNO's having a roaming agreement with the operator of mobile network 102. OCS 122 may maintain a profile of fixed networks having an interconnect agreement with the operator of mobile network 102. OCS 122 may also maintain a profile of content providers having an agreement to supply content to end users of mobile network 102. Alternatively, the profiles may be maintained on an external database that is accessible to OCS 122.

In step 306, OCS 122 determines a revenue share amount for each of the entities based on their profile and a rating provided by rating engine 132. For example, assume that overall charging for a call is $30. Based on the profiles and the ratings, OCS 122 may determine that entity 1 shares $10 of the revenue, entity 2 shares $10 of the revenue, and entity 3 shares $10 of the revenue. In step 308, OCS 122 generates charging records, such as a CDR, indicating the revenue share amount for each of the entities. For example, OCS 122 may generate an individual charging record for each of the entities indicating the amount the entity is owed or the amount payable to the entity. OCS 122 then transmits the charging records to charging controller 124 in step 310.

The charging records generated by OCS 122 include a new set of data for each revenue sharing entity. The new set of data includes an entity ID, which may be an end user subscriber ID, an MNO ID, an MVNO ID, a content provider ID, another network operator ID, etc. The new set of data also includes a charging type, such as retail charging, wholesale charging, content charging, interconnect charging, roaming charging, etc. The new set of data also includes a revenue share amount. The revenue share amount indicates the monetary amount of service usage owed by each entity or payable to each entity. The revenue share amount may be an accumulated amount per payment billing cycle, or a special call charge amount. For retailing charging, the revenue share amount represents the service units the end user pays to the MVNO/MNO. For wholesale charging, the revenue share amount represents the service units the MVNO pays to the MNO for network/service usage. For content charging, the revenue share amount represents the service units the MNO pays for the content supplied by the content provider. For interconnect charging, the revenue share amount represents the service units the MNO pays for the other network operator that interconnects the call. For roaming charging, the revenue share amount represents the service units the visiting MNO pays to the visited MNO for a local user to roam in a foreign network.

FIG. 4 is a flow chart illustrating a method 400 of correlating charging records in an exemplary embodiment. The steps of method 400 will be described with reference to communication network 100 in FIG. 1, but those skilled in the art will appreciate that method 400 may be performed in other networks and systems. In step 402, charging controller 124 receives the charging records for the entities having a revenue share. In step 404, charging controller 124 correlates the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities. The consolidated charging record also includes the new set of data for each revenue sharing entity, such as entity ID, charging type, and revenue share amount. In step 406, charging controller 124 transmits the consolidated CDR to billing system 106.

Billing system 106 may then perform a settlement process based on the data included in the consolidated charging record to generate billing invoices and generate vouchers or credits for each revenue sharing entity. Because charging controller 124 has already divided the revenue for the call in the consolidated charging record, billing system 106 does not need to perform this process. Billing system 106 only needs to issue the

vouchers to the proper entities for the revenue share amounts indicated in the consolidated charging record.

Examples

FIG. 5 illustrates another communication network 500 in an exemplary embodiment. Communication network 500 includes a mobile network 502, a charging system 504, and a billing system 506. Mobile network 502 is able to provide service to mobile device 540 to place voice calls, to initiate data sessions, to send or receive text messages or multimedia messages, etc. Charging system 504 includes an online charging system (OCS) 522, a charging controller 524, and an offline charging system (OFCS) 526.

OCS 522 handles online charging (or prepaid) for calls in mobile network 502. OCS 522 includes an online charging function (OCF) 530, an account balance management function (ABMF) 531, a rating engine 532, a profile database 533, and a tariff database 534. OCS 522 is enhanced to perform multiple-event charging based on one request event (i.e., a CCR). OCS 522 will use the different subscription IDs of the request to access each account profile separately, so OCS 522 will rate the call charge for each entity. After charging is finished, OCS 522 will generate a CDR indicating each entity's call cost, such as for retail charging, wholesale charging, content charging, interconnect charging, roaming charging, etc.

OCF 530 comprises any system, server, or function operable to manage online charging in OCS 522 by accessing ABMF 531 and rating engine 532, exchanging charging messages with network elements in mobile network 502, and performing other functions. ABMF 531 comprises any system, server, or function operable to maintain accounts for users, and more particularly to maintain an amount of service units in the accounts of the users. Rating engine 532 comprises any system, server, or function operable to determine the cost of service usage according to a tariff defined by the network operator. Rating engine 532 will perform tariff plan determination by accessing the tariff index of each entity, such as a unit determination, a price determination, a tariff determination, a counter, etc.

Rating engine 532 will not only hold the retail tariff plan for end user's service usage, but also holds the tariff plan for MNO's partnership, such as the price plan with MVNO, content provider, or other operators based on the service level agreement. OCF

530 will use the price plan index in each retail/partner's account profile to access the tariff to determine each entity's call charge.

Profile database 533 comprises any database or data structure operable to store profiles for retail customers, wholesale customers, content providers, interconnect operators, roaming operators, etc. Profile database 533 may alternatively store addresses for the profiles in order to remotely access the profiles. Tariff database 534 comprises any database or data structure operable to store a tariff plan or tariff plan index. Rating engine 532 is able to perform a tariff plan determination by accessing the tariff plan data of an entity, such as a unit determination, a price determination, a tariff determination, a counter, etc. OCF 530 will use the price plan index in each retail/partner's account profile to access the rating tariff index to determine each entity's call charge.

OFCS 526 handles offline charging (or postpaid) for calls in mobile network 502. OFCS 526 may include a Charging Data Function (CDF), a Charging Gateway Function (CGF), or other charging elements which are not specifically shown in FIG. 5.

Charging controller 524 comprises any system, server, or function operable to control overall charging for calls in mobile network 502. Charging controller 524 processes charging rules to determine which entities share in revenue for calls in mobile network 502. Charging controller 524 then generates a separate Diameter Ro CCR for each of the revenue sharing entities, and transmits CCRs to OCS 522 to determine the cost or the amount payable to the entity.

Assume for example that an end user of mobile device 540 subscribes to a service offered by OnStar Corporation, which is an in-vehicle service providing in-vehicle security, hands free calling, turn-by-turn navigation, remote diagnostics, etc. OnStar may be considered an MVNO in this example. OnStar leases its mobile services from mobile network 502, which is operated by Verizon Wireless (or some other mobile service provider). Verizon Wireless may thus be considered the MNO for the end user in this example. Assume further that the end user of mobile device 540 places a call (through the OnStar service) to another end user. The called end user subscribes to a service offered by another service provider, such as Vodafone in England. Vodafone may thus be considered the MNO for the called end user in this example.

Assume further that the overall charge for the call from the calling end user to the called end user is $30, and that the calling end user is responsible for payment for the call. FIG. 6 illustrates how the revenue for the call is divided among the entities in an exemplary

embodiment. According to the retail agreement between the calling end user 602 and OnStar (MNVO 604), calling end user 602 pays $30 to MVNO 604 for the call. This is an example of retail charging. MVNO 402 (OnStar) leases its mobile services from Verizon Wireless (MNO 606). According to the wholesale agreement between MVNO 604 and MNO 606, MVNO 604 pays $20 to MNO 606 for the mobile services. This is an example of wholesale charging. To connect the call to called end user 610, MNO 606 needs to connect to a foreign network operated by Vodafone (MNO 608). According to the interconnect agreement between MNO 606 and MNO 608, MNO 606 pays $10 to MNO 608 for the interconnect fees. This is an example of interconnect charging. Thus, the revenue for the call is divided between MVNO 604 (OnStar), MNO 606 (Verizon Wireless), and MNO 608 (Vodafone). In the embodiments provided herein, the dividing of the revenue is performed in the charging system instead of in back office systems. FIG. 7 further illustrates how this is done.

FIG. 7 is a message diagram illustrating how revenue for a call is divided in an exemplary embodiment. Mobile network 502 transmits a Diameter Ro CCR to OCS 522. The CCR includes charging data for the call in mobile network 502, such as a calling party number, a called party number, time stamps, etc. Although a Diameter Ro CCR is received in this example, other charging messages may be received in other examples, such as INAP messages. OCS 522 processes a subscription ID (subscription ID = MSISDN of the end user of mobile device 540) to access to the account profile for the end user. OCS 522 then calculates the overall charge for the call, which is $30 that is owed from the end user to OnStar. OCS 522 also generates a rated CDR (CDR1) indicating the call charge of $30, and sends the rated CDR to a mediation device (such as CDF or CGF) in OFCS 526. OFCS 526 then sends the rated CDR to charging controller (CC) 524. Those skilled in the art will appreciate that OCS 522 may send the rated CDR to charging controller (CC) 524 directly.

In response to receiving the rated CDR having charging data for the call, charging controller 524 processes charging rules to identify which entities are entitled to share in the revenue for the call. The following illustrates some exemplary rules for the different types of charging that may apply to the call.

Retail Rules:

Rule 1: CDR is not rated AND calling party number belongs to local operator AND call direction = originated call THEN:

Retail chargeable entity = calling party;

Trigger a Diameter Ro CCR [subscription ID = MSISDN of calling party, subscription type = retail charging,…] to OCS to determine the call cost for the calling party.

Rule 2: CDR is not rated AND called party number belongs to local operator AND call direction = terminate call AND subscriber location in home zone THEN:

Terminated local call is free to hear/accept;

Set the CDR as free call.

Rule 3: CDR is not rated AND called party number belongs to local operator AND call direction = terminate call AND subscriber location in roaming zone THEN:

Retail chargeable entity = called party

Trigger a Diameter Ro request [Subscription ID = MSISDN of called party, Subscription Type = retail charging,…] to OCS to determine the call cost for the called party.

Wholesale Rules:

Rule 1: Calling party number belongs to local operator AND call direction = originated call AND the prefix number of the calling party number is an MVNO call number THEN:

Map out the MVNO ID based on prefix number of the calling party number;

Wholesale chargeable entity = MVNO;

Trigger a Diameter Ro CCR [Subscription ID = MVNO ID, Subscription Type = wholesale charging,…] to OCS to determine the call cost for the MVNO.

Rule 2: Called party number belongs to local operator AND call direction = terminated call AND the prefix number of the called party number is an MVNO call number AND subscriber location in roaming zone THEN:

Map out the MVNO ID based on prefix number of the called party number;

Wholesale chargeable entity = MVNO;

Trigger a Diameter Ro CCR [Subscription ID = MVNO ID, Subscription Type =wholesale charging,…] to OCS to determine the call cost for the MVNO.

Interconnect Rules:

Rule 1: Calling party number belongs to the local operator AND called party number doesn't belong to local operator AND call direction = originated call THEN:

Map out the Interconnect Partner ID based on prefix number of the called party number;

Interconnect Partner entity = Interconnect Operator ID;

Trigger a Diameter Ro CCR [Subscription ID = Interconnect Operator ID, Subscription Type = interconnect charging,…] to OCS to determine the call cost for the interconnect partner.

Roaming Rules:

Rule 1: Calling party number doesn't belong to the local operator AND calling party's visited PLMN belongs to local operator THEN:

Map out the Inbound Partner ID based on prefix number of the calling party number;

Inbound Partner entity = Inbound Partner ID;

Trigger a Diameter Ro CCR [Subscription ID = Inbound Partner ID, subscription type = inbound roaming charging,…] to OCS to determine the call cost for inbound roaming partner.

Content Rules:

Rule 1: Calling party number belongs to the local operator AND (Service ID = *xxx* OR Merchant ID = *yyy* OR Content Provider = *zzz*) THEN:

Map out the Content Provider ID based on Service ID, Content ID, or Merchant ID;

Trigger a Diameter Ro CCR [Subscription ID = Content Provider ID, subscription type = content revenue sharing charging,…] to OCS to determine the call cost for the content provider.

In this example, charging controller 524 processes the wholesale rules and the prefix number of mobile device 540 that is included in the CDR. Based on the wholesale rules, charging controller 524 determines that this is an MVNO number of Verizon Wireless. Thus, charging controller 524 maps out the MVNO ID based on IMSI prefix, wherein the

MVNO ID is the identifier for OnStar. Charging controller 524 then transmits a Diameter Ro CCR (with subscription ID = MVNO ID) to OCS 522.

OCS 522 uses the MVNO ID in the CCR to access the OnStar account profile in profile database 533. OCS 522 then determines the call charge for the MVNO, which is the amount OnStar pays to Verizon Wireless ($20). OCS 522 then generates the rated CDR (CDR2) that includes the wholesale charge amount of $20, and transmits the rated CDR to OFCS 526.

Charging controller 524 also processes the interconnect rules and the prefix number of called party number in the CDR. Based on the interconnect rules, charging controller 524 determines that the call is an interconnect call. Charging controller 524 maps out the MNO ID based on called party number prefix, wherein in MNO ID is the identifier for Vodafone. Charging controller 524 then transmits a Diameter Ro CCR (with subscription ID = MNO ID) to OCS 522.

OCS 522 uses the MNO ID in the CCR to access the Vodafone account profile in profile database 533. OCS 522 then determines the call charge for the MNO, which is the amount Verizon Wireless pays to Vodafone ($10). OCS 522 then generates the rated CDR (CDR3) that includes the interconnect charge amount of $10, and transmits the rated CDR to OFCS 526.

OFCS 526 correlates the three rated CDRs to generate a consolidated CDR that indicates the revenue share amount for each of the entities. In this example, the consolidated CDR indicates the retail charge of $30, the wholesale charge of $20, and the interconnect charge of $10. The consolidated CDR includes the new set of data for each revenue sharing entity, such as entity ID, charging type, and revenue share amount. OFCS 526 then transmits the consolidated CDR to billing system 506. Although OFCS 526 is shown as correlating the CDRs in this embodiment, charging controller 524 may correlate the CDRs in other embodiments.

Billing system 506 may then perform a settlement process based on the data included in the consolidated CDR to generate billing invoices and generate vouchers or credits for each revenue sharing entity. In the above example, Verizon Wireless will receive a $20 voucher from OnStar, and Vodafone will receive a $10 voucher from Verizon Wireless for this call. Because charging controller 524 has already divided the revenue for the call in the consolidated CDR, billing system 506 does not need to perform this process.

Billing system 506 only needs to issue the vouchers to the proper entities for the revenue share amounts indicated in the consolidated CDR.

Any of the various elements shown in the figures or described herein may be implemented as hardware, software, firmware, or some combination of these. For example, an element may be implemented as dedicated hardware. Dedicated hardware elements may be referred to as "processors", "controllers", or some similar terminology. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, a network processor, application specific integrated circuit (ASIC) or other circuitry, field programmable gate array (FPGA), read only memory (ROM) for storing software, random access memory (RAM), non volatile storage, logic, or some other physical hardware component or module.

Also, an element may be implemented as instructions executable by a processor or a computer to perform the functions of the element. Some examples of instructions are software, program code, and firmware. The instructions are operational when executed by the processor to direct the processor to perform the functions of the element. The instructions may be stored on storage devices that are readable by the processor. Some examples of the storage devices are digital or solid-state memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media.

Although specific embodiments were described herein, the scope of the invention is not limited to those specific embodiments. The scope of the invention is defined by the following claims and any equivalents thereof.

CLAIMS:

We claim:

1. A charging system comprising:

a charging controller coupled to a mobile network and an online charging system, the charging controller operable to receive charging data for a call in the mobile network, to process the charging data for the call and charging rules to identify entities that have a share in revenue for the call, to generate a charging request message indicating the entities having a revenue share in the call, and to transmit the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

2. The charging system of claim 1 further comprising:

the online charging system operable to receive the charging request message from the charging controller, to identify a profile for each of the entities having a revenue share, to determine a revenue share amount for each of the entities based on their profile and a rating, to generate charging records indicating the revenue share amount for each of the entities, and to transmit the charging records to the charging controller.

3. The charging system of claim 2 wherein the charging records each include an entity ID, a charging type, and the revenue share amount.

4. The charging system of claim 3 wherein the revenue share amount indicates a monetary amount owed to another entity.

5. The charging system of claim 2 wherein:

the charging controller is further operable to receive the charging records, to correlate the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities, and to transmit the consolidated charging record to a billing system.

6. The charging system of claim 1 wherein the charging rules include retail rules defining conditions for retail charging.

7. The charging system of claim 1 wherein the charging rules include wholesale rules defining conditions for wholesale charging.

8. The charging system of claim 1 wherein the charging rules include interconnect rules defining conditions for interconnect charging.

9. The charging system of claim 1 wherein the charging rules include content rules defining conditions for content charging.

10. The charging system of claim 1 wherein the charging rules include roaming rules defining conditions for roaming charging.

11. A method of determining the share of call revenue for a call, the method comprising:

receiving charging data for a call placed over a mobile network in a charging controller that is coupled to the mobile network and to an online charging system;

processing the charging data for the call and charging rules to identify entities that have a share in revenue for the call;

generating a charging request message indicating the entities having a revenue share in the call; and

transmitting the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

12. The method of claim 11 further comprising:

receiving the charging request message in the online charging system from the charging controller;

identifying a profile for each of the entities having a revenue share;

determining a revenue share amount for each of the entities based on their profile and a rating;

generating charging records indicating the revenue share amount for each of the entities; and

transmitting the charging records from the online charging system to the charging controller.

13. The method of claim 12 wherein the charging records each include an entity ID, a charging type, and a revenue share amount.

14. The method of claim 13 wherein the revenue share amount indicates a monetary amount owed to another entity.

15. The method of claim 12 further comprising:

receiving the charging records in the charging controller from the online charging system;

correlating the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities; and

transmitting the consolidated charging record from the charging controller to a billing system.

16. The method of claim 11 wherein the charging rules include retail rules defining conditions for retail charging.

17. The method of claim 11 wherein the charging rules include wholesale rules defining conditions for wholesale charging.

18. The method of claim 11 wherein the charging rules include interconnect rules defining conditions for interconnect charging.

19. The method of claim 11 wherein the charging rules include content rules defining conditions for content charging.

20. The method of claim 11 wherein the charging rules include roaming rules defining conditions for roaming charging.

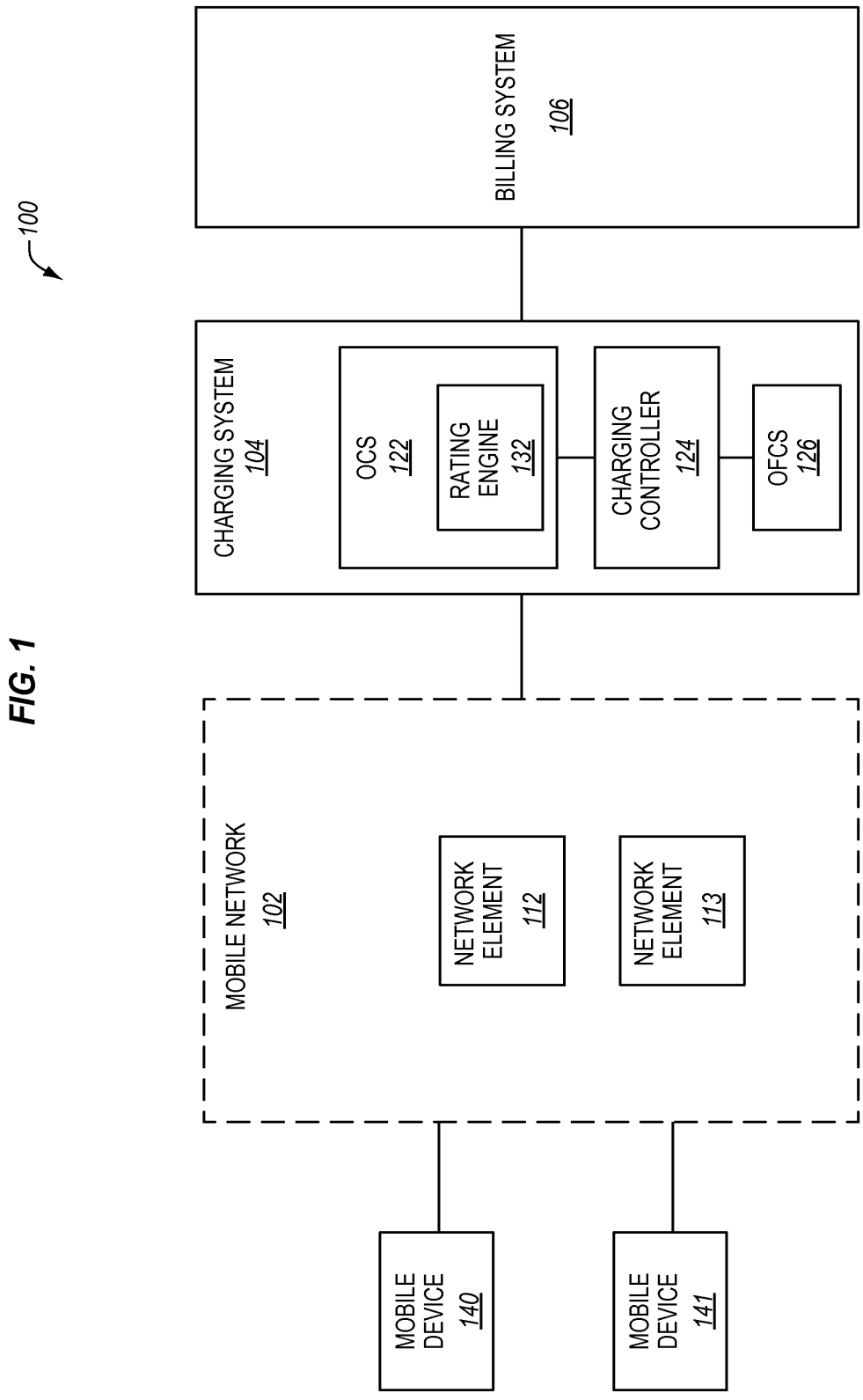

100
BILLING SYSTEM
106
CHARGING SYSTEM
104
OCS
122
RATING
ENGINE
132
CHARGING
CONTROLLER
124
OFCS
126
MOBILE NETWORK
102
NETWORK
ELEMENT
112
NETWORK
ELEMENT
113
MOBILE
DEVICE
140
MOBILE
DEVICE
141

FIG. 1

FIG. 2

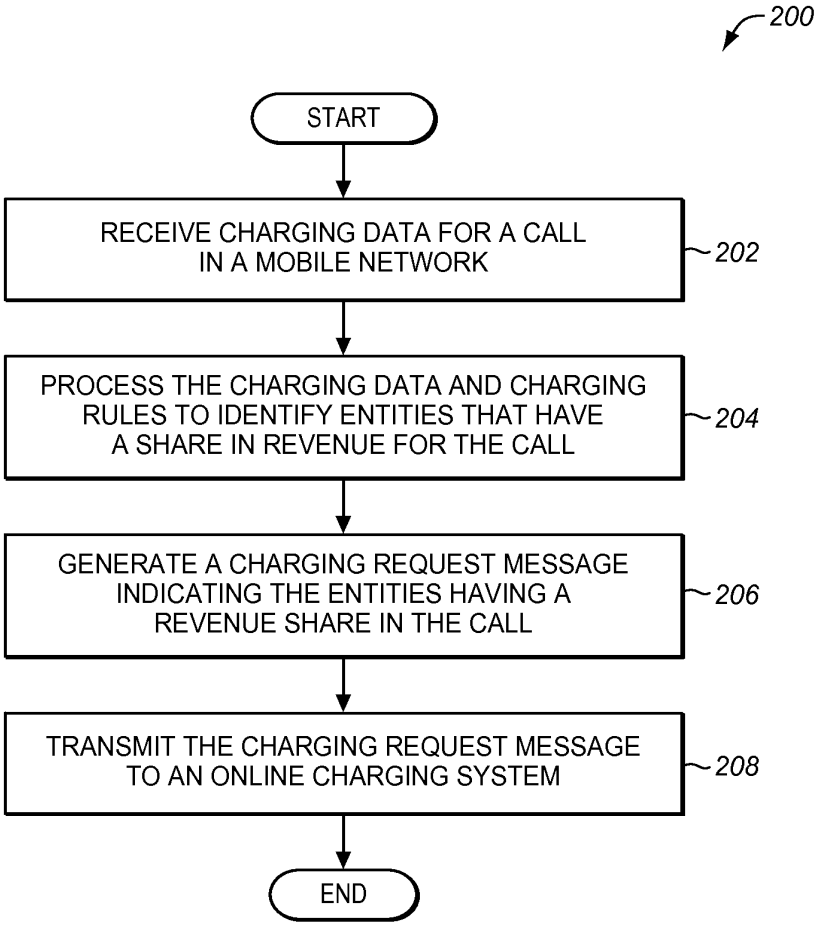

200
START
RECEIVE CHARGING DATA FOR A CALL IN A MOBILE NETWORK
202
PROCESS THE CHARGING DATA AND CHARGING RULES TO IDENTIFY ENTITIES THAT HAVE A SHARE IN REVENUE FOR THE CALL
204
GENERATE A CHARGING REQUEST MESSAGE INDICATING THE ENTITIES HAVING A REVENUE SHARE IN THE CALL
206
TRANSMIT THE CHARGING REQUEST MESSAGE TO AN ONLINE CHARGING SYSTEM
208
END

FIG. 3

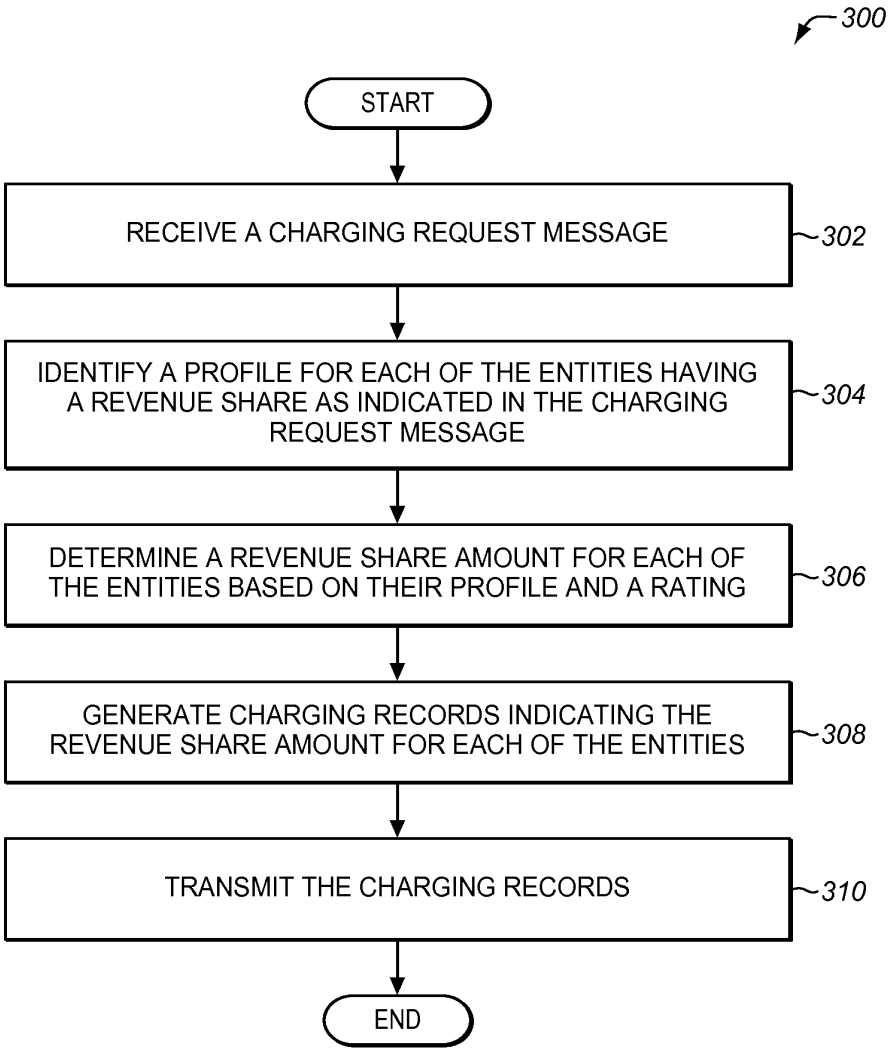

300
START
RECEIVE A CHARGING REQUEST MESSAGE
302
IDENTIFY A PROFILE FOR EACH OF THE ENTITIES HAVING A REVENUE SHARE AS INDICATED IN THE CHARGING REQUEST MESSAGE
304
DETERMINE A REVENUE SHARE AMOUNT FOR EACH OF THE ENTITIES BASED ON THEIR PROFILE AND A RATING
306
GENERATE CHARGING RECORDS INDICATING THE REVENUE SHARE AMOUNT FOR EACH OF THE ENTITIES
308
TRANSMIT THE CHARGING RECORDS
310
END

FIG. 4

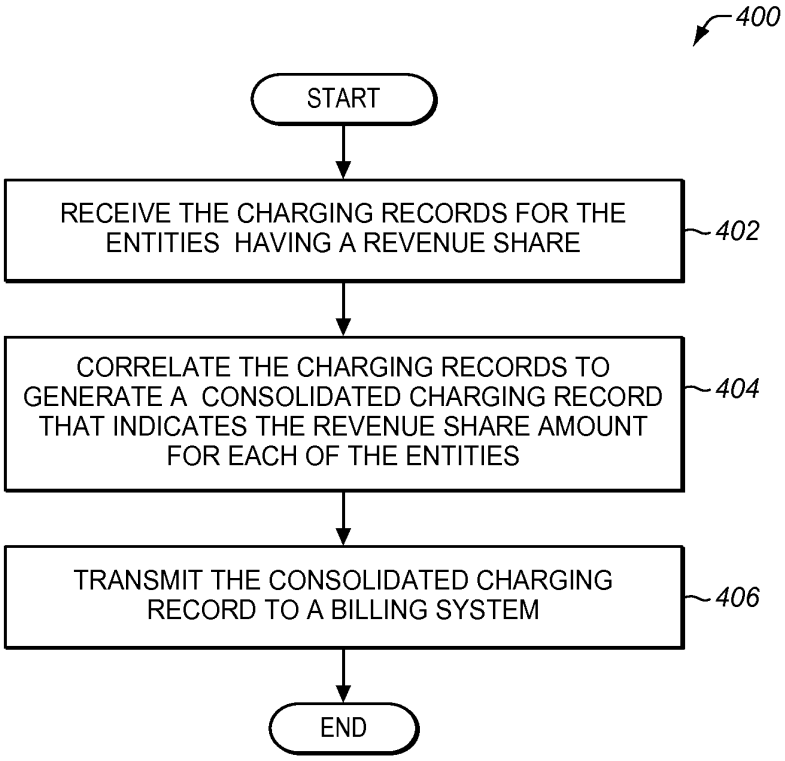
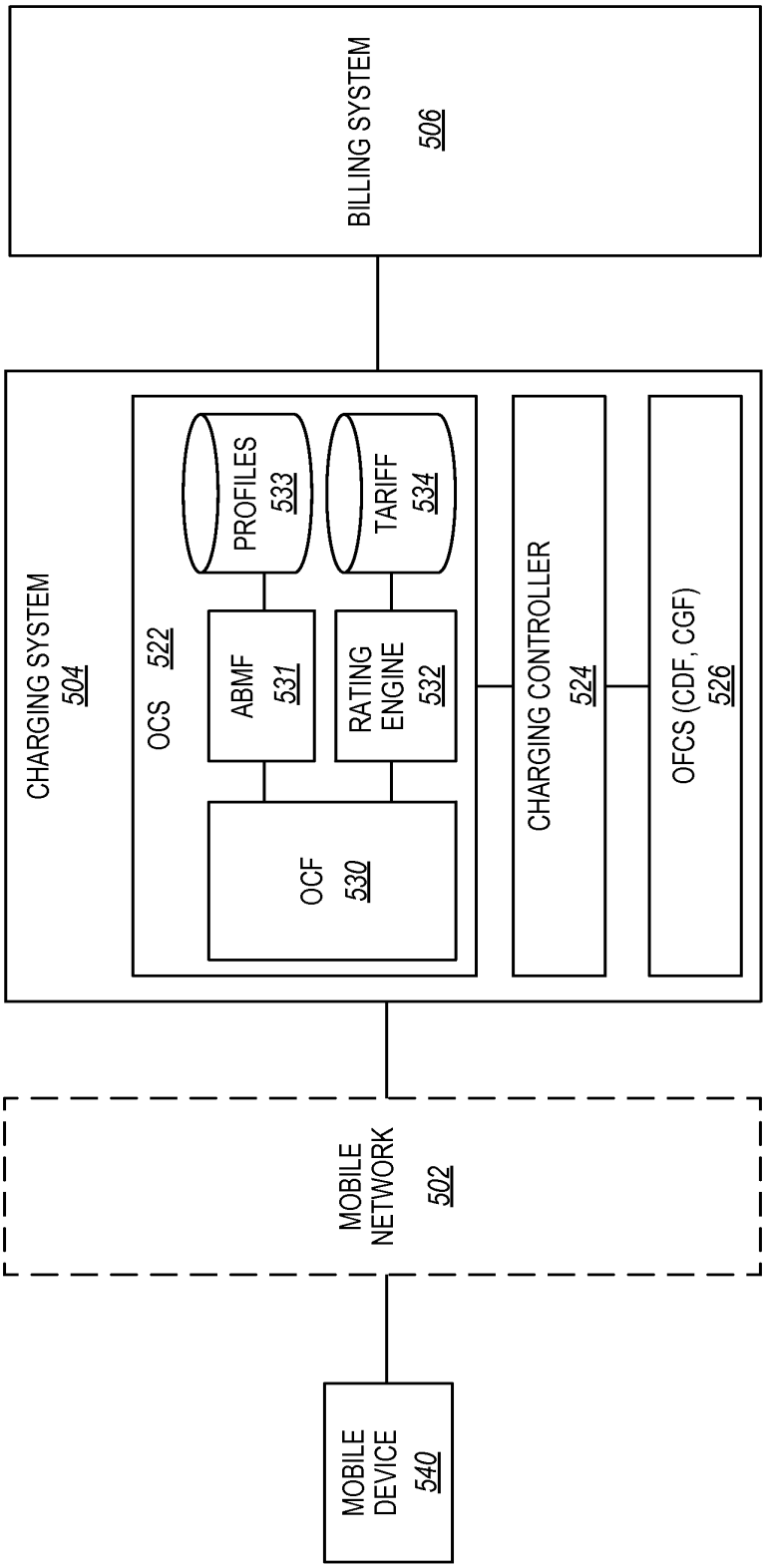

400
START
RECEIVE THE CHARGING RECORDS FOR THE ENTITIES HAVING A REVENUE SHARE
402
CORRELATE THE CHARGING RECORDS TO GENERATE A CONSOLIDATED CHARGING RECORD THAT INDICATES THE REVENUE SHARE AMOUNT FOR EACH OF THE ENTITIES
404
TRANSMIT THE CONSOLIDATED CHARGING RECORD TO A BILLING SYSTEM
406
END

FIG. 5


500
BILLING SYSTEM
506
CHARGING SYSTEM
504
OCS
522
PROFILES
533
TARIFF
534
ABMF
531
RATING ENGINE
532
OCF
530
CHARGING CONTROLLER
524
OFCS (CDF, CGF)
526
MOBILE NETWORK
502
MOBILE DEVICE
540

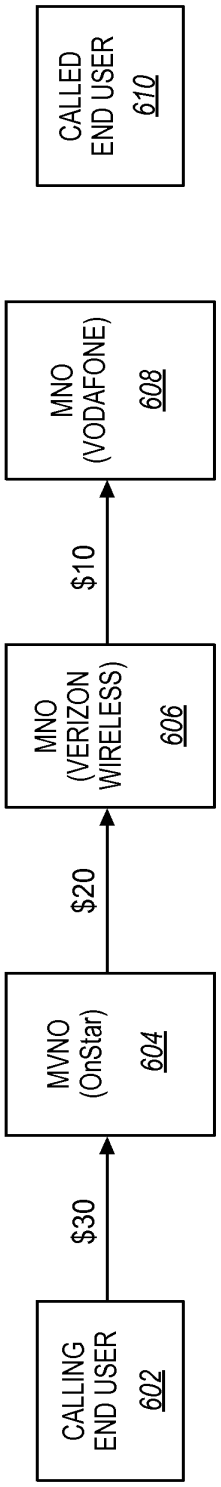
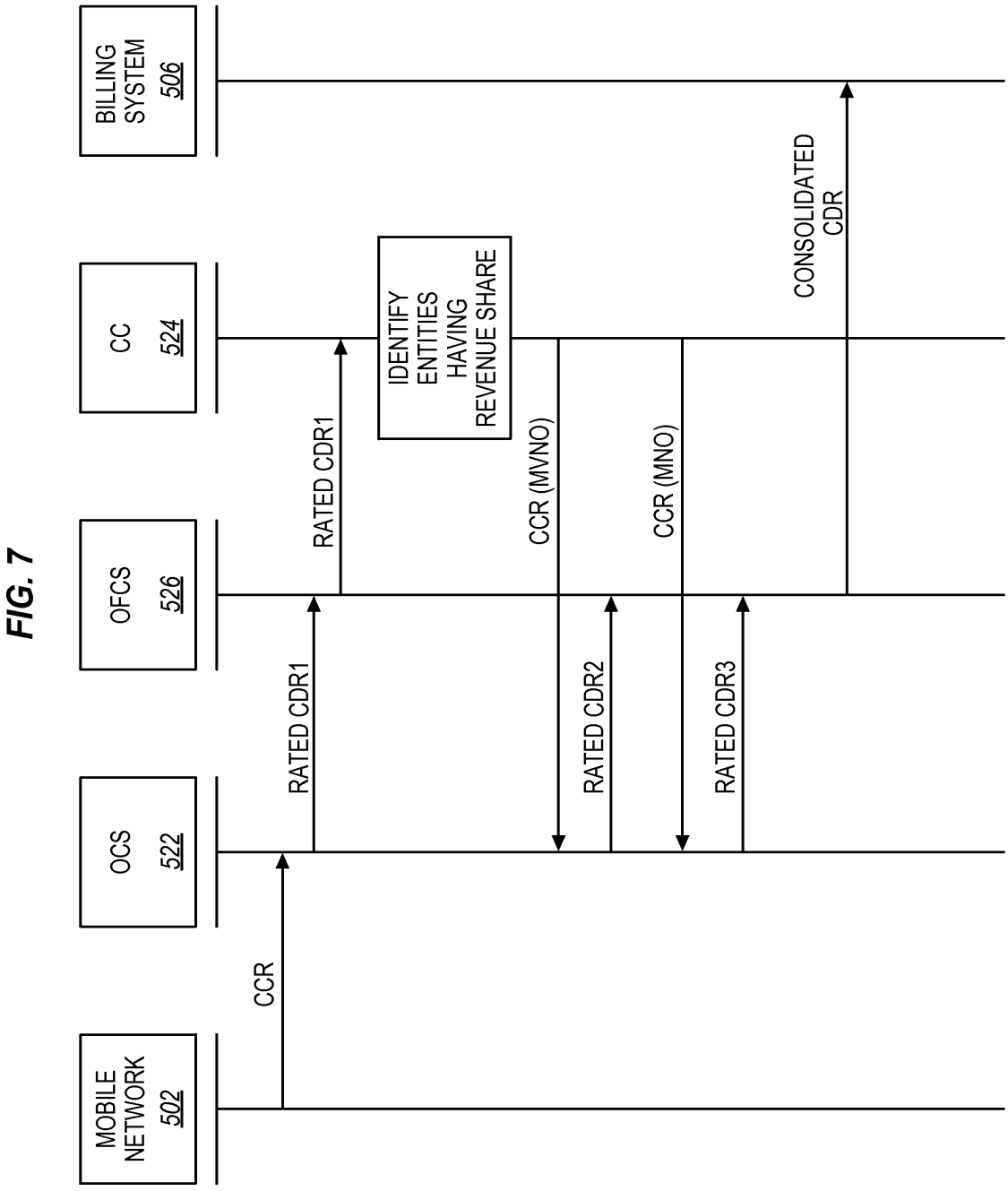

CALLING END USER 602
$30
MVNO (OnStar) 604
$20
MNO (VERIZON WIRELESS) 606
$10
MNO (VODAFONE) 608
CALLED END USER 610

FIG. 6

FIG. 7


MOBILE NETWORK 502
OCS 522
OFCS 526
CC 524
BILLING SYSTEM 506
CCR
RATED CDR1
RATED CDR1
IDENTIFY ENTITIES HAVING REVENUE SHARE
CCR (MVNO)
RATED CDR2
CCR (MNO)
RATED CDR3
CONSOLIDATED CDR

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/049255

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M15/00 H04W4/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04M H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	XIANG YANG LI ET AL: "Converged network common charging controller function" BELL LABS TECHNICAL JOURNAL, WILEY, CA, US, vol. 13, no. 2, 21 June 2008 (2008-06-21), pages 161-183, XP001514359 ISSN: 1089-7089 page 167 - page 179 figures 4-15 ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 March 2010	09/04/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Patlaka, Efi

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/049255

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Maria Koutsopoulou: "A platform for charging, billing and accounting in future mobile networks" 24 January 2005 (2005-01-24), XP002574421 Retrieved from the Internet: URL:http://cgi.di.uoa.gr/~mkoutsop/data/Koutsopoulou_NGNM2004_almost_final.pdf> [retrieved on 2010-03-23] paragraph [0003] - paragraph [0005] -----	1-20
A	EP 1 545 114 A1 (CIT ALCATEL [FR] ALCATEL LUCENT [FR]) 22 June 2005 (2005-06-22) claims 1-10 paragraph [0028] -----	1-20
A	ANONYMOUS: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; Charging specification for Release 1; Draft ETSI DTS 02032" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. TISPAN, no. Version 1, 1 October 2005 (2005-10-01), XP014031462 ISSN: 0000-0001 the whole document -----	1-20
A	US 2004/224662 A1 (O'NEIL DOUGLAS R [US] ET AL) 11 November 2004 (2004-11-11) claim 8 claims 12, 13 claims 19, 20 -----	1-20
A	WO 03/017065 A2 (APOGEE NETWORKS [US]; DESHMUKH ABHI [US]; HERNANDEZ MILTON [US]; GUHA) 27 February 2003 (2003-02-27) the whole document -----	1-20
A	EP 1 320 214 A1 (MARKPORT LTD [IE]) 18 June 2003 (2003-06-18) paragraph [0044] paragraph [0047] paragraph [0051] -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/049255

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1545114 A1	22-06-2005	AT 372643 T	15-09-2007
		CN 1630239 A	22-06-2005
		US 2005135577 A1	23-06-2005
US 2004224662 A1	11-11-2004	US 2009286507 A1	19-11-2009
		US 2007042750 A1	22-02-2007
WO 03017065 A2	27-02-2003	AU 2002332604 A1	03-03-2003
EP 1320214 A1	18-06-2003	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017065 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/26595

(22) International Filing Date: 20 August 2002 (20.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/934,123 21 August 2001 (21.08.2001) US

(71) Applicant *(for all designated States except US)*: **APOGEE NETWORKS** [US/US]; 1455 Broad Street, 4th Floor, Bloomfield, NJ 07003 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DESHMUKH, Abhi** [IN/US]; 253A, Kinderkamack Road, River Edge, NJ 07661 (US). **HERNANDEZ, Milton** [DM/US]; Apt. D, 1 Cononial Court, River Edge, NJ 07661 (US). **GUHA, Jayanta** [—/US]; 860 Main Street, Apt. 5B, Hackensack, NJ 07601 (US).

(74) Agents: **DUNNAM, Michael, P.** et al.; Woodcock Washburn LLP, One Liberty Place, 46th Floor, Philadelphia, PA 19103 (US).

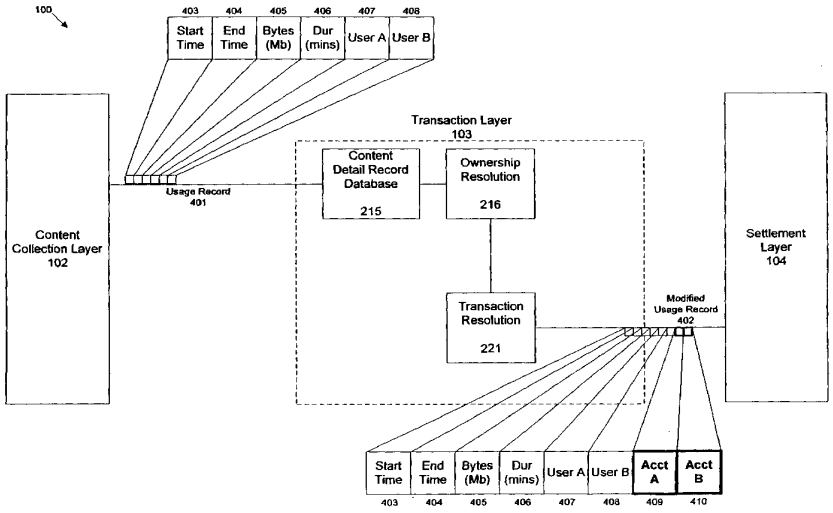
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: CONTENT OWNERSHIP RESOLUTION



(57) Abstract: The invention describes a method, system, and computer-readable medium having computer-executable instructions for determining parties to a transaction. The inventive method includes receiving data related to an event, where the data includes one or more data elements. The inventive method also includes selecting the data elements that identify the parties to the transaction, determining whether additional data elements are required to identify the parties to the transaction, and identifying the additional data elements. The event may be an exchange of data between the parties over a communication network, and the data related to the event may be stored in a usage record. The additional data element may identify an owner or party to the transaction, called an accountable. The party may have direct or indirect association in the transaction and may not be obvious from the record of the transaction itself.

WO 03/017065 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTENT OWNERSHIP RESOLUTION

Technical Field

The invention relates generally to the processing of data, and more particularly to efficiently and generically aggregating data available on a communication network.

Background of the Invention

Recently, the collection and processing of data transmitted over communication networks, like the Internet, has moved to the forefront of business objectives. In fact, with the advent of the Internet, new revenue generating business models have been created to account for the consumption of content received from a data network (*i.e.*, content-based billing). For example, content distributors, application service providers (ASPs), Internet service providers (ISPs), and wireless Internet providers have realized new opportunities based on the value of the content and services that they deliver. As a result of this content-and-services-billing initiative, it has become increasingly important to resolve intelligently and flexibly the corresponding transactions according to the business needs of the customer.

Often, even in traditional commerce streams, there a many different participants between the maker and the consumer of the goods. Some of these so-called "middlemen" simply may facilitate access to the good, while others may add useful characteristics to the good. This is especially true in a distributed network environment, like the Internet,

that impose additional burdens on capturing the transaction process because of the unlimited number of data sources and the correspondingly unlimited number of data types. As a result, adequately describing the transacting of the goods and services in such an environment, or even across any of the traditional environments requires a technique that is capable of understanding and processing the participants and the various types of data.

To date, resolving the characteristics of a transaction has been accomplished over data-specific environments using certain application-specific (*i.e.*, "non-generic" or custom) methods. For example, a typical telephone bill captures the characteristics of a voice-based telecommunications transaction. In particular, the participants may be identified as the party initiating the call (*i.e.*, the "calling party" telephone number), the party receiving the call (*i.e.*, the "called party" telephone number), and one or more parties connecting the communication (*i.e.*, the "local" or "long distance carrier"). This simple example adequately captures all of the necessary aspects of the telephone call to properly account for the transaction by requiring payment from certain parties (*e.g.*, the calling and/or the called party) to certain other parties (*e.g.*, the local and/or long distance carrier). While these "hard-coded" transaction resolution techniques are sufficient to accommodate only specific environments involving well-defined participants (e.g., the telecommunications network), they are correspondingly too rigid to efficiently satisfy the ever-changing face of a communication network like the Internet. Also, these "hard-

coded" techniques are too specific to operate across the many and varied transaction environments and domains that exist throughout the business world.

Therefore, there exists a need to provide a flexible technique that can capture and resolve transactions of any type in any business domain involving any number and kind of participants without requiring modification of the technique for each type. Such a technique would serve to accommodate multi-faceted networked environments like the Internet, as well as to provide a single solution that would apply to any business environment.

Summary of the Invention

The invention describes a method, system, and computer-readable medium having computer-executable instructions for determining parties to a transaction. The inventive method includes receiving data related to an event, where the data includes one or more data elements. The inventive method also includes selecting the data elements that identify the parties to the transaction, determining whether additional data elements are required to identify all or some of the parties to the transaction, and identifying the additional data elements. The event may be an exchange of data between the parties over a communication network, and the data related to the event may be stored in a usage record. The additional data element may identify an owner or party to the transaction, called an accountable. Determining whether additional elements are required may be a function of the received data, and/or a function of the requirements of a customer

settlement system. The customer settlement system may be a data security system, a network capacity planning system, a content monitoring system, and/or a billing application, for example. The identifying of additional data elements or accountables may be initiated by a building block known as a primitive that includes multiple specific methods, including a database lookup, a direct value assignment, a regular expression parsing or match, a CDR database lookup, hard-coded, network address, area code, substring manipulation or a custom code execution. All or some of the inventive method steps may be conducted on a computer-readable medium using computer-executable instructions.

The inventive system for determining parties to a transaction includes an instrumentation layer, a content collection layer in communication with the instrumentation layer, and a transaction layer in communication with the content collection layer. The instrumentation layer provides raw data, while the content collection layer generically processes the raw data, and the transaction layer identifies one or more parties to the transaction. Also, the content collection layer may provide the raw data to the transaction layer in a usage record, and the transaction layer may modify the usage record as a function of identifying the parties to the transaction. The inventive system may further include a settlement layer in communication with the transaction layer, wherein the settlement layer rates the modified usage record. The transaction layer may include a database for storing the data processed by the content collection layer.

Brief Description of the Drawings

Other features of the invention are further apparent from the following detailed description of the embodiments of the invention taken in conjunction with the accompanying drawings, of which:

Figure 1 is a block diagram of a system for analyzing content transmitted over a communication network, according to the invention;

Figure 2 is a block diagram further describing the components of the system described in Figure 1;

Figures 3A and 3B provide a flow diagram further detailing the operation the system described in Figure 1;

Figure 4 provides a block diagram of the system described in Figure 1, providing greater detail of a configuration and operation of a transaction layer;

Figures 5A and 5B provide a flow diagram of a method for identifying the characteristics of a transaction, according to the invention;

Figure 6 is a block diagram further detailing the operation and configuration of the transaction layer, according to the invention; and

Figure 7 is a flow diagram that details the operation and configuration of the transaction layer of transaction layer, according to the invention.

Detailed Description of the Invention

System Overview

Figure 1 is a block diagram of a system 100 for analyzing content transmitted over a communication network. Although the following description will be discussed in the context of collecting, processing and billing for data transmitted over the Internet, it should be appreciated that the invention is no so limited. In fact, the invention may be applied to any type of network, including a private local area network, for example. Also, the invention may be used for purposes other than billing for the usage of content. For example, the invention may be used to analyze the type of data transmitted over a particular network, or to determine the routing patterns of data on a network. Furthermore, the invention may be used to facilitate the intelligent collection and aggregation of data relevant to a particular industry. In addition, the invention may be used to track specific Internet protocol (IP) network resources and to detect fraud, for example. It should also be appreciated that the invention may contemplate non-network and non-computer related business domains like commodity trading (*e.g.,* grains, crude oil) where multiple parties are involved. Therefore, although the invention is often described in the context of the Internet, it should be appreciated that the invention may equally applied to traditional business environments.

In addition, it should be appreciated that the term "content" may be defined as data that is transmitted over the network. In the context of the Internet, content may include .mp3 files, hypertext markup language (html) pages, videoconferencing data, and streaming audio, for example. The terms "content provider" and "customer" will be used throughout the description as well. Content provider may refer to the primary creator or

provider of the content, while customer is the primary recipient of the content. Both the producer and customer may be a human or a computer-based system.

As shown in Figure 1, an instrumentation layer 101 provides raw data to a content collection layer 102. Instrumentation layer 101 may consist of various data sources, for example, network routers. The network routers may provide information regarding the various types of routed data, including for example, data format, originating Internet protocol (IP) address, and destination IP address. One example of such information is Cisco System's NetFlow™.

Content collection layer 102 collects information about the delivery of the content, as well as the substance of the content itself. Content collection layer 102 also may sort, filter, aggregate, correlate and store the content according to the particular needs of the end user. In effect, content collection layer is responsible for extracting meaningful information about IP traffic, and so it is provided with an understanding of the data sources in instrumentation layer 101. Content collection layer 102 also may transform the data from the plurality of sources in instrumentation layer 101 into standard formats for use in a transaction layer 103.

Content collection layer 102 is in communication with transaction layer 103. Generally, content collection layer 102 reports to transaction layer 103 that a relevant communication event has occurred and should be considered by the remainder of system 100. A communication event may be defined as any transfer of data between systems. Transaction layer 103 captures the predetermined agreements among all of the parties

involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 is in communication with a settlement layer 104. Settlement layer 104 captures the operations that are necessary to understand the significance of the transaction defined by transaction layer 103. For example, settlement layer 104 may rate a particular transaction by assigning a monetary value to the transaction. Settlement layer 104 also may divide the burdens and benefits of the monetary value among the relevant parties. In this way, settlement layer 104 ensures that certain parties receive a particular portion of the payment made by the other parties. Settlement layer 104 also may be responsible for delivering this burden and benefit information to the appropriate parties with the appropriate identifiers (*e.g.*, account numbers).

Figure 2 is a block diagram further describing the components of system 100. As shown in Figure 2, instrumentation layer 101 includes data sources 201-203 that each provide raw data 204-206, respectively, to collection layer 102. As discussed, data sources 201-203 may include various internetworking devices like routers, bridges, and network switches. Data sources 201-203 provide raw data to an input data adapter 207. Accordingly, input data adapter 207 understands the operation of and the data provided

by data sources 201-203. Although one input data adapter is shown in Figure 2, it should be appreciated that more than one input data adapter may be used in system 100. For example, each data source may have a dedicated input data adapter.

Input data adapter 207 understands the incoming data and extracts the data into the appropriate fields. This field-delimited data, called flow objects 208, are sets of attributes. The attributes may be any characteristics that are provided by, or can be derived from, raw data 204-206 provided by data sources 201-203, respectively. For example, flow objects 208 may include a set of attributes describing the source and destination, including source IP address, destination IP address, source interface, and destination interface. Because input data adapter 207 is charged with understanding raw data 204-206 from data sources 201-203, as well as the required flow objects 208 of system 100, it is capable of transforming the raw data to the flow objects, where the flow objects may all be of a standard format.

Input data adapter 207 provides flow objects 208 to a content data language 209. Content data language 209 may transform the attributes in flow objects 208 into other attributes that are desired by a particular customer. For example, content data language 209 may derive a network identifier attribute that is not readily available from a data source, from a source address attribute and a destination address attribute that are provided by flow object 208 attributes from input data adapter 207. This derivation may be based on a customer's desire to determine which network conveyed the transaction between the source and the destination. Therefore, following this example, content data

language 209 will know to extract the source address attribute and the destination address attribute from flow objects 208.

Content data language 209 may perform other functions as well. For example, content data language 209 may perform a generic lookup function 219 that is built into content data language 209. Generally, generic lookup 219 describes a technique for mapping any number of attributes to any number of other derived attributes. For example, generic lookup 219 may be used to map a unique resource locator (URL) attribute to a particular content-type attribute.

Content data language 209 also is in communication with a correlator 211. Generally, correlator 211 connects the many daily network content events from various network devices, like routers for example. Often, the connected data may come from distinctly different data sources at distinctly unrelated times. Correlator 211 allows this data to be intelligently connected to each other, regardless of how different the sources or of how disparate the time received. For example, a Netflow™ enabled router and a Radius™ enabled network access switch may each provide certain data that is relevant to one particular transaction. However, because portions of the data come from different devices, the data may arrive at system 100 at different times, and in different formats. Also, because each provides data that is necessary to complete one transaction, the data from each cannot be considered separately. Correlator 211 allows this data to be intelligently grouped regardless of the format of the data or of the time the data pieces are received.

Furthermore, correlator 209 may rearrange the order of the received flow objects 208 to suit the needs of the remainder of system 100. By performing such correlation without having to first store all of the data on a disk (*e.g.*, a database), significantly faster processing is achieved. Correlator 209 may perform this correlation in real-time, for example.

Although system 100 has been described using content data language 209 and correlator 211, it should be appreciated that flow objects 208 may proceed directly to a filter 212, if no correlation is required and if no attribute derivation is required, for example. Filter 212 analyzes flow objects 208 to ensure that the provided attributes are desired by system 100. If flow objects 208 are not needed (*i.e.*, a mismatch), filter 212 may prevent flow objects 208 from passing to an aggregator 213. Also, although filter 212 has been shown as a separate device in system 100, it should be appreciated that the functionality of filter 212 may be incorporated into aggregator 213.

Filter 212 passes the matching flow objects to aggregator 213. Aggregator 213 may provide additional filtering and classification of the multitude of daily network content transactions, based on user criteria. Aggregator 213 may perform such filtering and classification in real-time. Aggregator 213 will be discussed in greater detail with reference to Figures 4-7. Aggregator 213 provides the filtered and classified information to an output data adapter 214. Output data adapter 214 may convert the data from aggregator 213 into one or more content detail records for storage in CDR database 215. Therefore, CDR database 215 stores a complete description of a content event.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 passes the CDR onto ownership resolution component 216. A proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. These tasks are accomplished by ownership resolution component 216 and transaction resolution component 221.

Ownership resolution component 216 serves to define the direct and indirect participants of the communication event. In particular, because raw data 204-206 may not provide sufficient "ownership" data relating to the parties involved in the content transaction, such "ownership" data must be provided by system 100 to properly account for the entire transaction. Ownership resolution component 216 operates to provide such ownership-based data to system 100.

Ownership resolution component 216 is in communication with transaction resolution component 221. Transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Such predetermined relationships may be previously agreed upon by the participants, or may be created and agreed upon with the implementation of system 100. Therefore, transaction component 103 understands the nature of the parties, the actions that one or

more parties perform, and the influence of such action on the respective parties. Ownership resolution component 216 and transaction resolution component 221 will be discussed in greater detail.

Transaction component 216 provides the transaction information to a rating component 217. Rating component 217 provides a weight or significance (*e.g.*, a price) to the transaction, so as to provide a tangible value to the transaction. Rating component 217 may make this determination based on various metrics including the type of the content, the quantity of content consumed, the place and time delivered, or the quality of the content for example. Therefore, rating component 217 allows system 100 to provide some contextual value, indicting the significance or relevance that certain content or information has to the individual customer.

Rating component 217 provides the rated transaction to a presentment component 218. Presentment component 218 may provide the capability for a customer 220 to view their real-time billing information, for example, over the network. Presentment component 218 also may attach relevant identifiers to the bill (*e.g.*, account numbers, etc.).

Figures 3A and 3B provide a flow diagram further detailing the operation 300 of system 100. As shown in Figure 3A, in step 301, raw data 204-206 is received from data sources 201-203. In step 302, input data adapter 207 converts raw data 204-206 to flow objects 208, where flow objects 208 are sets of attributes, determined from raw data 204-206. In step 303, it is determined whether there is a need to derive new attributes from

the existing attributes found in flow objects 208. If there is such a need, in step 304, CDL 209 is used to derive new attributes from existing attributes. Also, as discussed above, attributes may be correlated by correlator 211.

In step 305, flow objects 208 are filtered by filter 212. In step 306, the matching flow objects (*i.e.*, those passed by filter 212) are further filtered and classified by aggregator 213 (as discussed more fully with reference to Figures 4-7). In step 307, output data adapter 214 converts the data aggregated by aggregator 213 to a format compatible with transaction layer 103.

As shown in Figure 3B, in step 308, output adapter 214 may format the aggregated data into one or more content data records for storage in CDR database 215. In step 309, ownership resolution component 216 identifies the parties involved in the transaction. In step 310, transaction resolution component 221 captures the predetermined agreements among the parties, as well as the value added by each of the individual parties. In step 311, the CDR is rated based on predetermined metrics (*e.g.*, time of transmission, quality of content). In step 312, a bill is presented to the customer.

Content Transaction Layer

A transaction, including a business transaction for example, may be any activity between two or more participants that affects certain parties. The affected parties may be considered the participants to the transaction, although parties and participants may be mutually exclusive entities. It should be appreciated that the terms "parties" and "owners" may be used interchangeably throughout. Also, a transaction may include one or more events, where an event may be some action (*e.g.,* the transfer of a service or good) that the participants conduct with each other. Such events may be the exchange of data over a communication network, for example. Also, it should be appreciated that the same event or action may take place in any direction (*e.g.,* from party A to party B or from party B to party A). The "subject" of the action is the party who performs the activity, while the "object" of the action is the party who is affected or influenced in any way by the action.

Transaction layer 103 is responsible for capturing the characteristics of the transaction, including the parties, participants, subject, object, event/action type, direction of the action, for example. The scope of the characteristics captured by transaction layer 103 will vary with the nature of instrumentation layer 101, the capability of content collection layer 102, and the requirements of settlement layer 104. Generally, transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer

103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 is a data store that holds each CDR for further processing by ownership resolution component 216 and transaction resolution component 221. In the context of a billable electronic business transaction, a proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. As discussed, ownership resolution component 216 serves to define the participants of the communication event, while transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216.

Transaction layer 103 is generic in that it operates without requiring an understanding of instrumentation layer 101 and content collection layer 102. Instead, transaction layer 103 takes the relevant characteristics of the transaction provided by instrumentation layer 101 and content collection layer 102, and selects and generates those characteristics required by settlement layer 104.

Although the operation of transaction layer 103 will be described in the context of an electronic event over a communication network for the purposes of billing for the event, it should be appreciated that the invention is not so limited, but is so described the

purpose of clarity. For example, it should be appreciated that the invention may include functions other than billing, including security, network capacity planning, and content monitoring, for example. Also, the generic techniques described may be applied beyond the context of an electronic event over a communication network.

Figure 4 provides a block diagram of system 100 providing greater detail of the configuration and operation of transaction layer 103. As shown in Figure 4, content collection layer 102 provides a usage record 401 to transaction layer 103. A series of fields 403-408 comprise usage record 401. Although fields 403-408 will be identified by certain labels for the purpose of clarity, it should be appreciated that fields 403-408 may identify any of the many possible characteristics of the transaction.

In the example provided by Figure 4, fields 403 and 404 identify the parties or participants to the transaction. In particular, field 403 identifies "User A" and field 404 identifies "User B." User A may be the subject party and User B may be the object party. For example, in the context of a telecommunication event, User A may be the "calling" party and User B may be the "called" party. Field 405 and field 406 identify a measurable quantity of the event. In particular, following the example of the telecommunications event, field 405 identifies a duration (in minutes) of the event and field 406 identifies the quantity of data exchanged during the event (in megabytes). Field 407 and field 408 may identify a "start time" and an "end time," respectively, of the communication event.

Although fields 403-408 provide just one example, in any case, it should be appreciated that user record 401 will include certain characteristics provided by instrumentation layer 101 and/or derived by content collection layer 102. These characteristics typically are provided to transaction layer 103 because they have some particular significance to identifying the characteristics necessary to allow settlement layer 104 to provide some accounting of the transaction. Therefore, usage record 401 may not necessarily include all of the characteristics provide by instrumentation layer 101 and/or derived by content collection layer 102, because certain characteristics may not relevant to the settlement of the transaction (*e.g.*, network type). Yet, usage record 401 will include those available characteristics that pertain to permitting settlement layer 104 to properly account for the transaction.

Once usage record 401 passes through transaction layer 103, a modified usage record 402 may be provided to settlement layer 104. Modified usage record 402 may be modified by transaction layer 103 to include additional details of the transaction event required by settlement layer 104 and/or required by the customer's system to which the usage record applies (*e.g.*, a usage billing system). As shown for modified usage record 402, an account A field 409 and an account B field 410 may be added to further identify the transaction. In one example, account A field 409 may include an alphanumeric designator that identifies the account number that has been assigned by the customer's billing system for User A. In the context of the telecommunications system, account A field 409 may hold User A's ten-digit home telephone number, for example.

In any case, the components of transaction layer 103 operate to identify these additional fields, based on the requirements of the customer's system and of settlement layer 104. In particular, ownership resolution component 216 operates to ensure that the necessary participants or parties to the transaction are identified, while transaction resolution component 221 operates to ensure that the relationships among the parties or participants are identified.

Identification of the relevant entities and their relationships may be accomplished using "lookups" in data stores located within ownership resolution component 216 or user-defined actions specified on external systems and applications and transaction resolution component 221, for example. For example, a data table may have a "User" data field and an associated "Account" data field. When User A is received by ownership resolution component 216, it will conduct a lookup in the data table and identify Account A as the appropriate account associated with User A. Also, transaction resolution component 221 may have a data table that permits a lookup of the relationship between User A and User B, identified in usage record 401. For example, upon receiving field 407 designating User A and field 408 designating User B, transaction resolution component 221 may conduct a lookup of an algorithm that identifies the appropriate burdens and benefits (*e.g.*, debit and credit of money) assigned to each of the users with respect to each other.

It also should be appreciated that transaction layer 103 may not provide additional characteristics to usage record 401, as described but may select the relevant

characteristics (*i.e.*, those characteristics needed by settlement layer 104) from the characteristics made available by instrumentation layer 101 and/or derived by content collection layer 102. In fact, usage record 401 may include all of the necessary characteristics to properly account for the transaction. In this case, ownership resolution component 216 and transaction resolution component 221 select the relevant characteristics from the available characteristics.

Figures 5A and 5B provide a flow diagram of a method 500 for identifying the characteristics of a transaction using system 100. As shown in Figure 5A, in step 501, raw data 204-206 is received into system 100. Raw data 204-206 includes certain characteristics provided by data sources 201-203, respectively, in instrumentation layer 101. In step 502, content collection layer 102 processes (*e.g.*, aggregates, correlates and filters) raw data 204-206. In step 503, content collection layer 102 provides the processed data to CDR database 215 in transaction layer 103. CDR database 215 stores the data for further processing by transaction layer 103.

In step 505, it is determined whether the contents of the data provided to transaction layer 103 already include the needed ownership data. If the data includes the needed ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507. If, on the other hand, the data provided to transaction layer 103 does not already include the needed ownership data, the required data is identified (*e.g.*, using database lookups, accountable primitives) by ownership resolution component 216, in step 506. Once ownership

resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507.

As shown in Figure 5B, in step 508 it is determined whether the contents of the data provided to transaction layer 103 already include the needed relationship data (*i.e.*, data defining the burdens and benefits encountered by the parties/participants to the transaction). If the data includes the needed relationship data, the relevant data is selected by transaction resolution component 221 and provided to settlement layer 104, in step 510. If, on the other hand, the data provided to transaction layer 103 does not already include the needed relationship data, the required data is identified (*e.g.*, using database lookups) by transaction resolution component 221, in step 509. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 510.

Ownership and Transaction Resolution

Figure 6 is a block diagram further detailing the operation and configuration of transaction layer 103. It should be appreciated that elements described for transaction layer 103 are not exclusive, but provide just one example of a configuration for transaction layer 103. In particular, the functionality of the previously described ownership resolution component 216 and transaction resolution component 221 will be

descried in greater detail in the various components described with reference to Figure 6. In practice, however, it should be appreciated that transaction layer 103 may comprise of any number of components that ensure that the necessary parties to a transaction are identified generically.

As shown in Figure 6, transaction layer 103 includes a configuration repository 601, a configuration database 610, a configuration manager 603, and a fail over detector 604. In addition, transaction layer 103 includes a transaction layer engine 608 in communication with configuration repository 601, configuration manager 603, and fail over detector 604.

Transaction layer engine 608 includes a rules processor 605, a CDR reader 606, and a transaction writer 607. Transaction layer engine 608 processes raw data 204-206 in usage record 401 and creates a modified usage record 402, based upon the requirements of settlement layer 104. It should be appreciated that there may be more than one transaction layer engine 608 for each transaction layer 103. However, a single transaction layer engine 608 is shown for the purpose of clarity and brevity.

CDR reader 106 understands the nature of the transaction and operates to read a particular usage record 401 stored in CDR database 215. CDR reader 106 then submits usage record 401 to rules processor 605. Rules processor 605 applies rules (*e.g.*, written in XML) to usage record 401 so as to determine ownership and the relationships among the ownership, for each individual usage record 401. Rules processor 605 may then generate one or more modified usage records 402, based on the application of the rules to

usage record 401. Once rules processor 605 generates the modified usage record 402, transaction writer 607 operates to write a transaction (based on the modified usage record 402) to CDR database 215. Modified usage record 402 is then used by settlement layer 104 to further process the transaction (*e.g.*, rate the transactions monetarily).

Fail over detector 604 operates to provide fault tolerance and initiate a fail over engine (not shown) for a failed transaction layer engine, in accordance with one or more mathematical algorithms, the discussion of which is beyond the scope of the invention. Configuration manager 603 provides an external interface to transaction layer 103 using a business editor 609. Business editor 609 may be manipulated by a user or customer using a graphics user interface (GUI). In particular, the GUI of business editor 609 receives commands from a user and translates them into actions to be performed on usage record 401, for example, by rules processor 605. Configuration repository 601 operates to provide an abstraction to configuration database 610. Configuration database 610 may be a relational database or a set of extensible markup language (XML) computer-readable files, for example.

Figure 7 is a flow diagram that details the operation of transaction layer 103, as shown in Figure 6. As discussed, it should be appreciated that multiple transaction engines may be used to implement a process. Where the invention is instituted using computer-readable instruction, transaction layer engine 608 may be implemented as a computer-executable instruction or thread. Therefore, multiple transaction layer engines may be implemented by having multiple computer-readable instructions.

In step 701, transaction layer engine 608 reads usage record 401 using CDR reader 606. In step 702, rules processor 605 applies one or more rules to usage record 401 read by CDR reader 606, so as to determine one or more "accountables." Accountables are labels that are used to facilitate identifying the parties or owners to a transaction. Accountables may be defined and/or modified by an external user (*e.g.*, a customer) using the graphical user interface provided by business editor 609. Also, it should be appreciated that accountables may be defined for a new usage types for which no rules in rules processor 605 are provided. The identification of accountables is the function of ownership resolution component 216, as described with reference to Figure 4.

In step 703, "contracts" are identified that define the relationships or agreements between one or more accountables. In the context of a billing system, a contract identifies which party pays (*i.e.*, the billed party) and which party receives payment (*i.e.*, the billing party). A particular contract may be identified and executed when one based on "conditions" are satisfied, however, such conditions may not be required. The identification of contracts is conducted by transaction resolution component 221, as described with reference to Figures 2 and 4. A condition is an expression of a logical assertion that can be evaluated as true or false. In transaction layer 103, for example, a condition may be true if a certain data element is present and false if the data element is not present. The following is an example of a condition in XML:

<condition name="condition1" function="IsPresent" outcome="true" type="Accountable" id="ColoProvider"/>

In step 704, once the contracts are determined, they are executed. In step 705, usage record 401 is changed to modified usage record 402 based upon the execution of the contract and the identification of the accountables. In step 706, modified usage record 402 may be written to a data table using transaction writer 607, so that settlement layer 104 can rate it, in step 707. Therefore, a transaction may be represented as modified usage record 402, where modified usage record may include the elements of usage record 401 in addition to the accountable and contract elements (*e.g.*, fields 409-410 as discussed with reference to Figure 4).

Although the discussion provided an example of a single contract and two accountables for a single usage record, it should be appreciated that many contracts and many accountables (*i.e.*, and therefore many "transactions") may be derived from a single usage record, because there may be multiple transactions implicated from a single usage record 401. For example, usage record 401 may involve three parties each having a contract with the other respective parties. In this example, therefore, there may be three separate contracts for a single usage record 401, and three individual accountables for each party or owner.

In addition to requiring a certain accountable, it may be necessary to determine a value of the accountable. For example, transaction layer 103 may determine not only that the "called party" accountable be a part of the transaction, but also that a value for the

called party (*e.g.*, "856-555-1212" or "John Doe") be identified. Also, it may be necessary to transform one accountable into another accountable to satisfy the requirement of settlement layer 104. For example, settlement layer 104 may require the called party accountable (either determined by transaction layer 103 or provided in usage record 401) be transformed into a network identifier accountable.

In either case, the value or transformation of accountables or contracts may be determined using certain predetermined functions or "primitives." A primitive allows the user to specify how to find the value of a particular accountable or how to find billing and/or billed account numbers associated with a particular contract. As discussed, transformations may allow a value of an accountable to be determined using another accountable (*i.e.*, called "linked accountables"), for example. Primitives define and direct such transformations. The input to a primitive can be one of fields 403-408 from usage record 401 or a previously determined accountable, for example.

Primitives may be described and distinguished based on their prescribed functionality. For example, one type of primitive may be an external database lookup. A database lookup is a primitive that operates to transform one accountable or contract to another accountable or contract. Also, a database lookup primitive may function to assign a value to an accountable or contract, as a result of conducting a lookup of the accountable or contract in a database. It should be appreciated that the database lookup primitive also allows flexibility in that any database that has Java Database Connectivity (JDBC) drivers (*e.g.*, Oracle, Microsoft SQL Server, Sybase, Database 2) can be used to

perform complex lookups. For native databases that do not have JDBC connectivity, however, it should be appreciated that native methods for native databases may be accommodated through the primitives. In this way, therefore, previous accountable or contact transformations can be linked to find new accountables or contracts, respectively.

Other types of primitives may include direct value assignment, and a function primitive. A function primitive provides flexibility and extensibility by allowing a third party based library (*e.g.*, Java-based or native libraries) to be used. The arguments of a function primitive may be text strings. Also, the arguments of a function primitive may be expressed in terms of fields in CDR database 215 (*i.e.*, string-based fields in usage record 401), and other previously determined accountables. Therefore, function primitives permit the integration of proprietary and domain-specific algorithms to be implemented to perform ownership related processing.

Another primitive may be a "regular expression" based primitive that allows parsing of complex text-based fields with a full feature (*e.g.*, PERL5 compliant) pattern specification. Common used techniques would include parsing URLs, filenames and paths, calling/called telephone numbers, email address, for example. In addition, a CDR database 215 lookup primitive allows holding on to an ownership entity if no further processing is required. This primitive is used where usage record 401 provides the information needed by settlement layer 104 without any need for more data correlation and/or manipulation by transaction layer 103.

A default primitive may be a hard-coded primitive that is used where the value is known and/or is not dependent on usage record 401. For example, such a primitive may be used where a party is always present in a consumption event, regardless of the other relevant parties. A network address primitive allows determination of a network entity given an arbitrary string. An area code primitive may be used to determine an area code of a telephone number given the complete telephone number. This primitive may be relevant for a Voice-over-IP application. These examples primitives are not exclusive, but are meant to provide a few examples of the manipulation and correlation that may be achieved by the primitives on the accountables and contracts.

The following is an example of an accountable primitive in XML:

```
<accountable>
<name> ColoProvider </name>
<role> ServiceProvider </role>
<usageType> RMONHost </usageType>
<valid from="past" to="present" />
<primitive type="default">
<value> Exodus </value>
</primitive>
</accountable>
```

Each accountable that is involved in a contract will have an assigned "role." It follows, therefore, that an accountable that is not involved in a contract may not need to have an assigned role. The role associates the particular accountable for integration with settlement layer 104. This means that the concept of a role is used for the TL/AMI integration.

Similar to the accountable, a contract is implemented using a set of primitives. The following is an example of a contract primitive in XML, and is provided to further describe the invention. In the example, a Web hosting scenario is present where a content provider (*e.g.,* CNN) places content on one or more Web servers and pays a Web Hoster for doing so based on some predefined pricing plan.

In order to define the accountables, certain elements of usage record 401 may be assumed as follows: Web Hit Time, Web Server Name/IP address, Client IP address, bytes, Mime type, and URL. In this example, if a rule in the business world requires the "Content Provider" of the Web Server (*e.g.,* CNN) to pay to the Web Hoster, there are two accountables: Web Hoster and Content Provider. The XML definition of a contract that captures this business rule may be as follows:

```
01  <contract>
02  <name> ContentProvider-Pays-WebHoster </name>
03  <usageType> WebHosting </usageType>
04  <valid from="past" to="present" />
05  <condition function="IsPresent" type="Accountable"
    name="condition1"  id=" ContentProvider " />
06  <condition function="IsPresent" type="Accountable"
    name="condition2" id="WebHoster" />

07  <billedFunction>
08  <status> enabled </status>
09  <primitive type="internal-account-lookup">
10  <database name="GlobalDB"/>
11  <argument order="1" type="Accountable"
    name="ContentProvider"/>
12  </primitive>
13  </billedFunction>
```

```
14    <billingFunction>
15    <status> disabled </status>
16    <primitive type="internal-account-lookup">
17    <database name="GlobalDB"/>
18    <argument order="1" type="Accountable" name="WebHoster"/>
19    </primitive>
20    </billingFunction>
21    </contract>
```

In this example, a contract has a name defined in line 02 as "ContentProvider-Pays-WebHoster." The contract also defines an element or usage type called "WebHosting" in line 03. The contract also has two sets of conditions in lines 05 and 06, called "IsPresent," which consider whether "ContentProvider" and "WebHoster" elements are present, respectively. Therefore, this particular contract will be selected and executed by transaction layer 103 if these elements are present.

Also, in this contract example, there are two primitives that are specified. There is a first primitive for finding the account number of the billed entity "ContentProvider," which begins on line 07 and ends on line 13, and there is a primitive for determining the account of the billing entity "WebHoster" beginning on line 14 and ending on line 20. Therefore, the example contract contemplates the "who pays to whom" logic, and results in the execution of a contract that creates a modified usage record 402, which captures the transaction. Notably, in lines 09 and 16, both primitives are defined as database lookups.

The invention is directed to a system and method for of determining of direct and/or indirect parties involved in a transaction. The invention often was described in the context of the Internet, but is not so limited to the Internet, regardless of any specific description in the drawing or examples set forth herein. For example, the invention may be applied to wireless networks, as well as non-traditional networks like Voice-over-IP-based networks, private networks, and/or non-technology related business environments, like commodity trading for example. It will be understood that the invention is not limited to the use of any of the particular components or devices herein. Indeed, this invention can be used in any application that requires the determining of direct or indirect parties involved in a transaction. Further, the system disclosed in the invention can be used with the method of the invention or a variety of other applications.

While the invention has been particularly shown and described with reference to the embodiments thereof, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art will appreciate that various changes and adaptations of the invention may be made in the form and details of these embodiments without departing from the true spirit and scope of the invention as defined by the following claims.

What is Claimed is:

1. A method of determining parties to a transaction, comprising:

receiving data related to an event, wherein said data comprises one or more data elements;

selecting said data elements that identify the parties to the transaction;

determining whether additional data elements are required to identify the parties to the transaction; and

identifying the additional data elements.

2. The method of claim 1, wherein said event is an exchange of data between the parties over a communication network.

3. The method of claim 1, wherein said data related to said event is stored in a usage record.

4. The method of claim 1, wherein the parties include at least one of the following: a subject party and an object party.

5. The method of claim 1, wherein said determining is a function of the received data.

6. The method of claim 1, wherein said determining is a function of the requirements of a customer settlement system.

7. The method of claim 6, wherein said customer settlement system includes at least one of the following: a data security system, a network capacity planning system, and a content monitoring system.

8. The method of claim 1, wherein said data element is an accountable.

9. The method of claim 1, wherein said identifying of additional data elements is initiated by a primitive.

10. The method of claim 9, wherein said primitive includes at least one of the following: a database lookup, direct value assignment, regular expression, CDR database lookup, hard-coded, network address, substring manipulation, area code, and a user-specified action.

11. A system for determining parties to a transaction, comprising:

an instrumentation layer, wherein the instrumentation layer provides raw data;

a content collection layer in communication with the instrumentation layer, wherein the content collection layer generically processes the raw data; and

a transaction layer in communication with the content collection layer, wherein the transaction layer identifies one or more parties to the transaction.

12. The system of claim 11, wherein said content collection layer provides said raw data to said transaction layer in a usage record.

13. The system of claim 12, wherein said transaction layer modifies said usage record as a function of identifying the parties to the transaction.

14. The system of claim 11, further comprising a settlement layer in communication with said transaction layer, wherein the settlement layer rates the modified usage record.

15. The system of claim 12, wherein said transaction layer comprises a data base for storing said data processed by said content collection layer.

16. A computer-readable medium having computer-executable instructions for:

receiving data related to an event, wherein said data comprises one or more data elements;

selecting said data elements that identify the parties to the transaction;

determining whether additional data elements are required to identify the parties to the transaction; and

identifying the additional data elements.

17. The computer-readable medium of claim 16, wherein said computer-executable instructions are extensible.

18. The computer-readable medium of claim 16, wherein said event is an exchange of data between the parties over a communication network.

19. The computer-readable medium of claim 16, wherein said data related to said event is stored in a usage record.

20. The computer-readable medium of claim 16, wherein the parties include at least one of the following: a subject party and an object party.

21. The computer-readable medium of claim 16, wherein said determining is a function of the received data.

22. The computer-readable medium of claim 16, wherein said determining is a function of the requirements of a customer settlement system.

23. The computer-readable medium of claim 22, wherein said customer settlement system includes at least one of the following: a data security system, a network capacity planning system, and a content monitoring system.

24. The computer-readable medium of claim 16, wherein said data element is an accountable.

25. The computer-readable medium of claim 16, wherein said identifying of additional data elements is initiated by a primitive.

26. The computer-readable medium of claim 25, wherein said primitive includes at least one of the following: a database lookup, direct value assignment, regular expression, CDR database lookup, hard-coded, network address, substring manipulation, area code, and user-specified action.

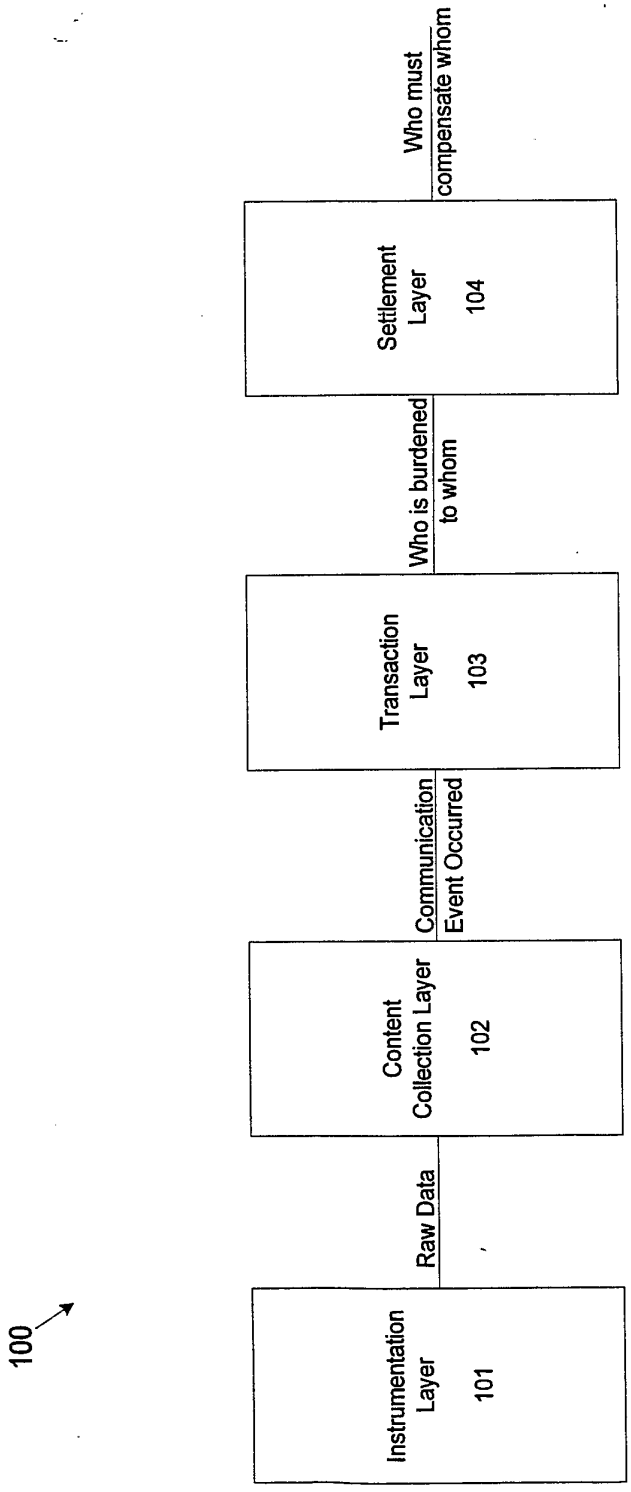

100
Instrumentation Layer 101
Raw Data
Content Collection Layer 102
Communication Event Occurred
Transaction Layer 103
Who is burdened to whom
Settlement Layer 104
Who must compensate whom

Figure 1

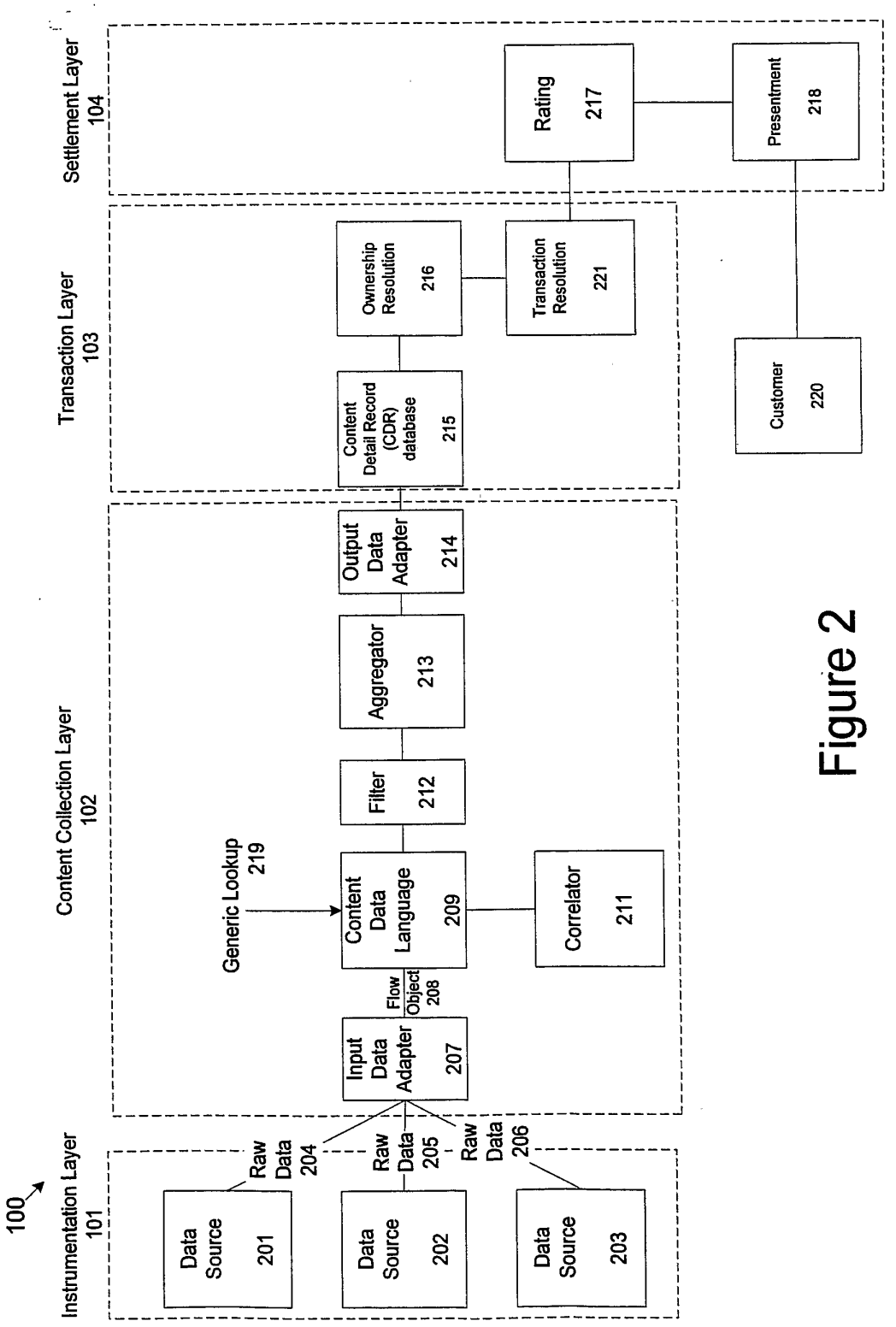

100
Instrumentation Layer
101
Data Source
201
Data Source
202
Data Source
203
Raw Data
204
Raw Data
205
Raw Data
206
Content Collection Layer
102
Input Data Adapter
207
Flow Object
208
Content Data Language
209
Generic Lookup
219
Filter
212
Aggregator
213
Output Data Adapter
214
Correlator
211
Transaction Layer
103
Content Detail Record (CDR) database
215
Ownership Resolution
216
Transaction Resolution
221
Settlement Layer
104
Rating
217
Presentment
218
Customer
220

Figure 2

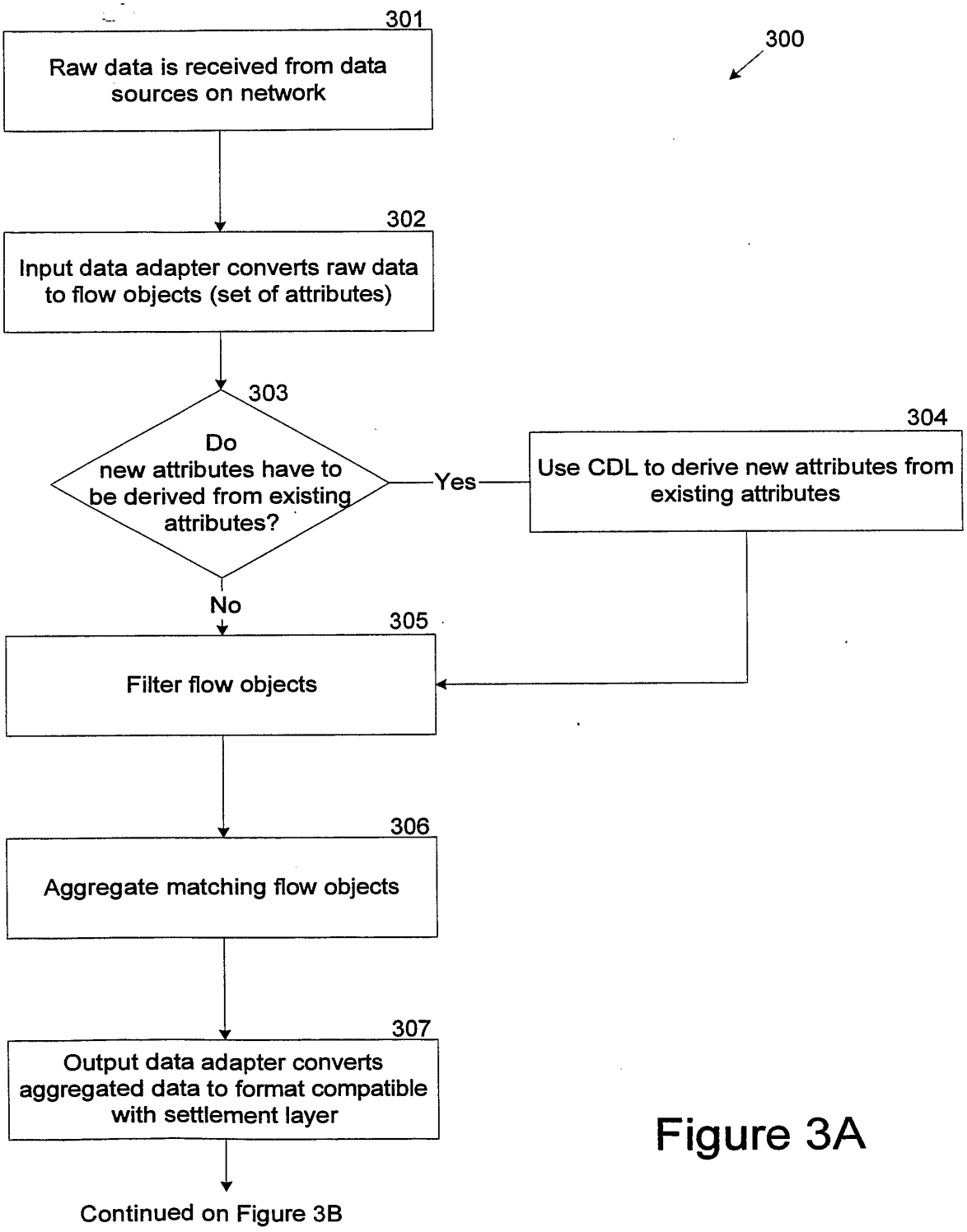

301
Raw data is received from data sources on network
300
302
Input data adapter converts raw data to flow objects (set of attributes)
303
Do new attributes have to be derived from existing attributes?
Yes
304
Use CDL to derive new attributes from existing attributes
No
305
Filter flow objects
306
Aggregate matching flow objects
307
Output data adapter converts aggregated data to format compatible with settlement layer
Continued on Figure 3B

Figure 3A

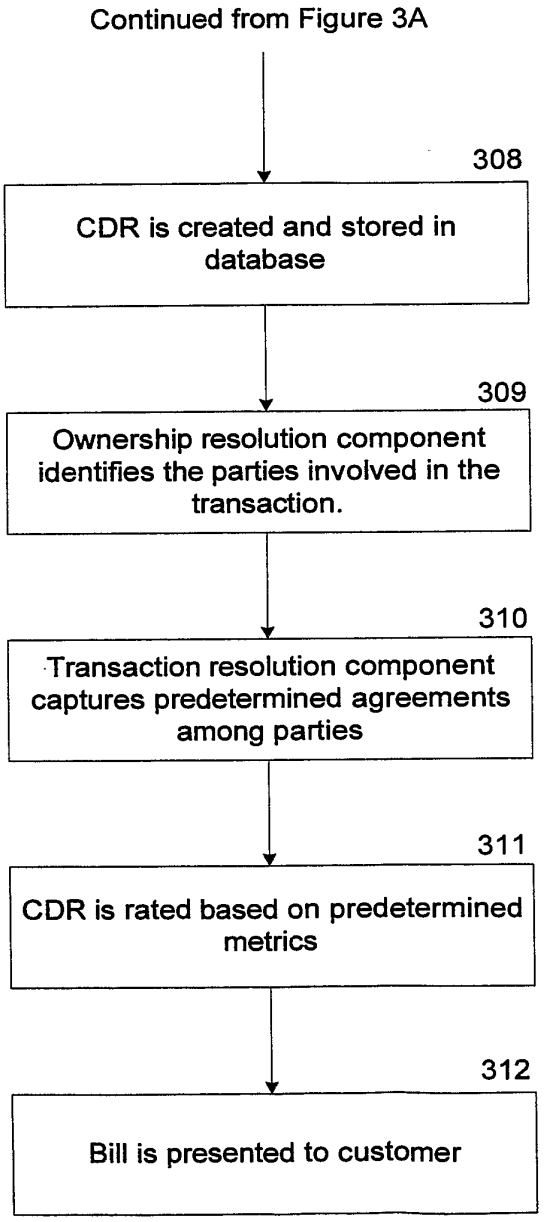

Continued from Figure 3A
308
CDR is created and stored in database
309
Ownership resolution component identifies the parties involved in the transaction.
310
Transaction resolution component captures predetermined agreements among parties
311
CDR is rated based on predetermined metrics
312
Bill is presented to customer

Figure 3B

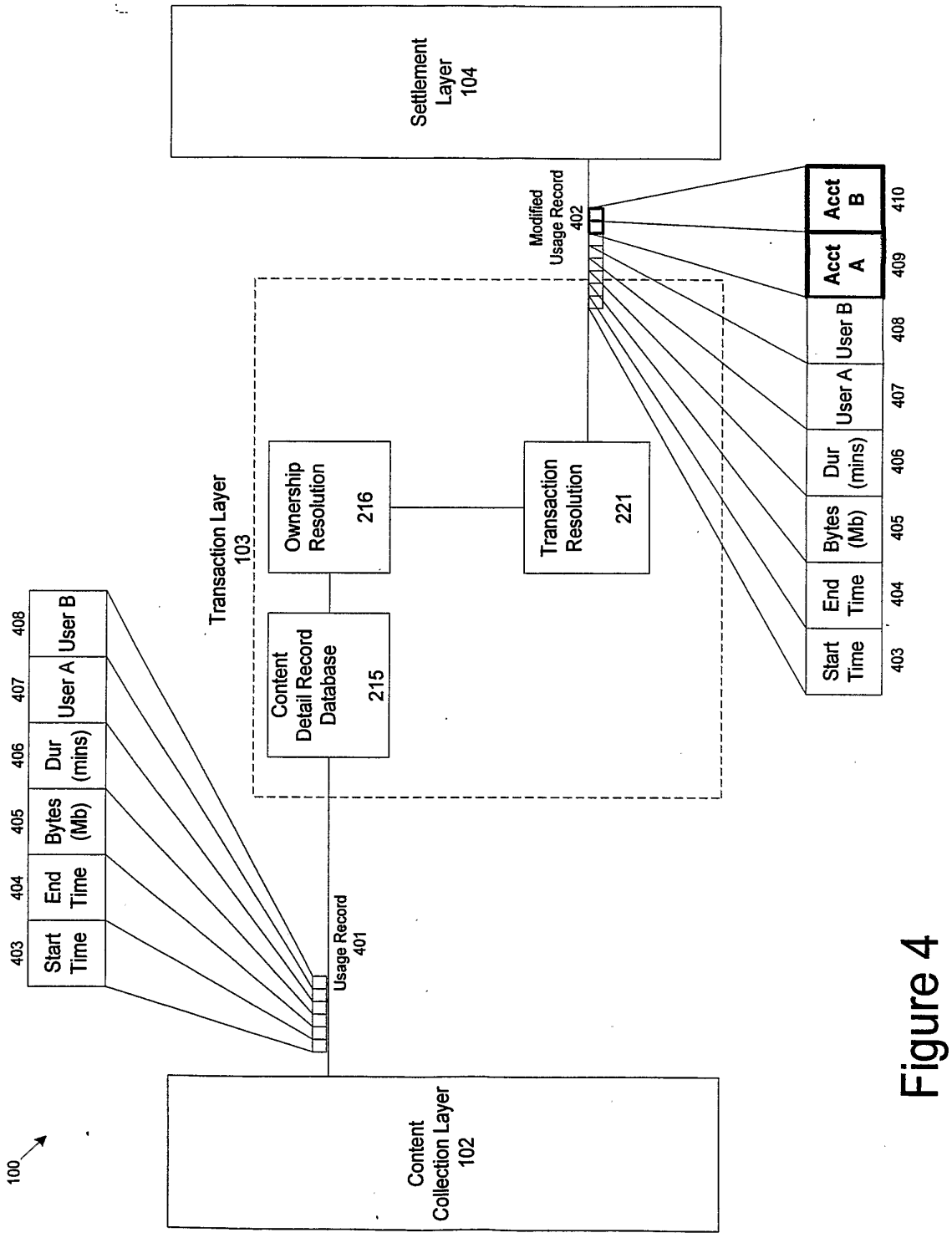

100
Content Collection Layer 102
Settlement Layer 104
Transaction Layer 103
Content Detail Record Database 215
Ownership Resolution 216
Transaction Resolution 221
Usage Record 401
Modified Usage Record 402
403 Start Time
404 End Time
405 Bytes (Mb)
406 Dur (mins)
407 User A
408 User B
409 Acct A
410 Acct B

Figure 4

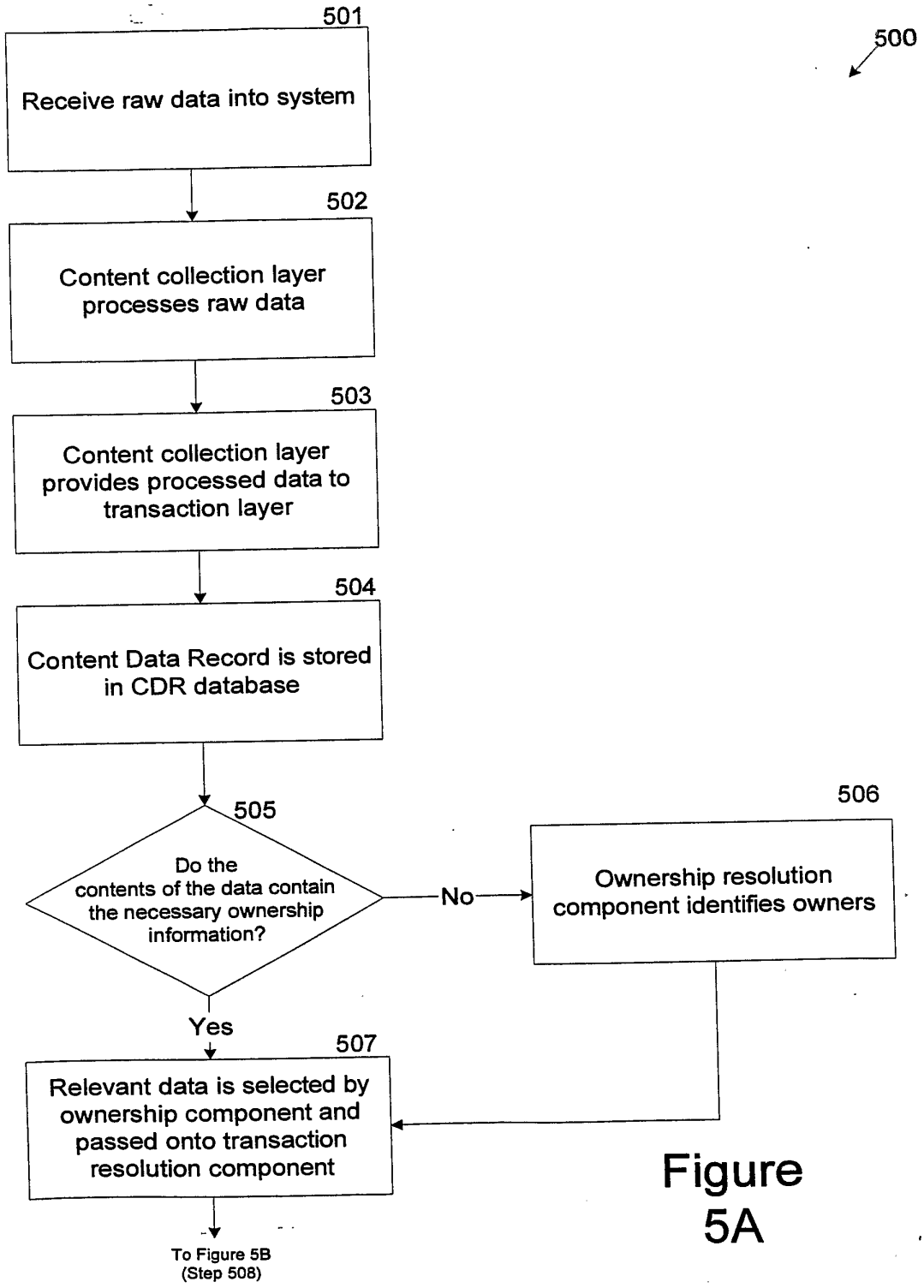

500
501
Receive raw data into system
502
Content collection layer processes raw data
503
Content collection layer provides processed data to transaction layer
504
Content Data Record is stored in CDR database
505
Do the contents of the data contain the necessary ownership information?
No
506
Ownership resolution component identifies owners
Yes
507
Relevant data is selected by ownership component and passed onto transaction resolution component
To Figure 5B (Step 508)

Figure 5A

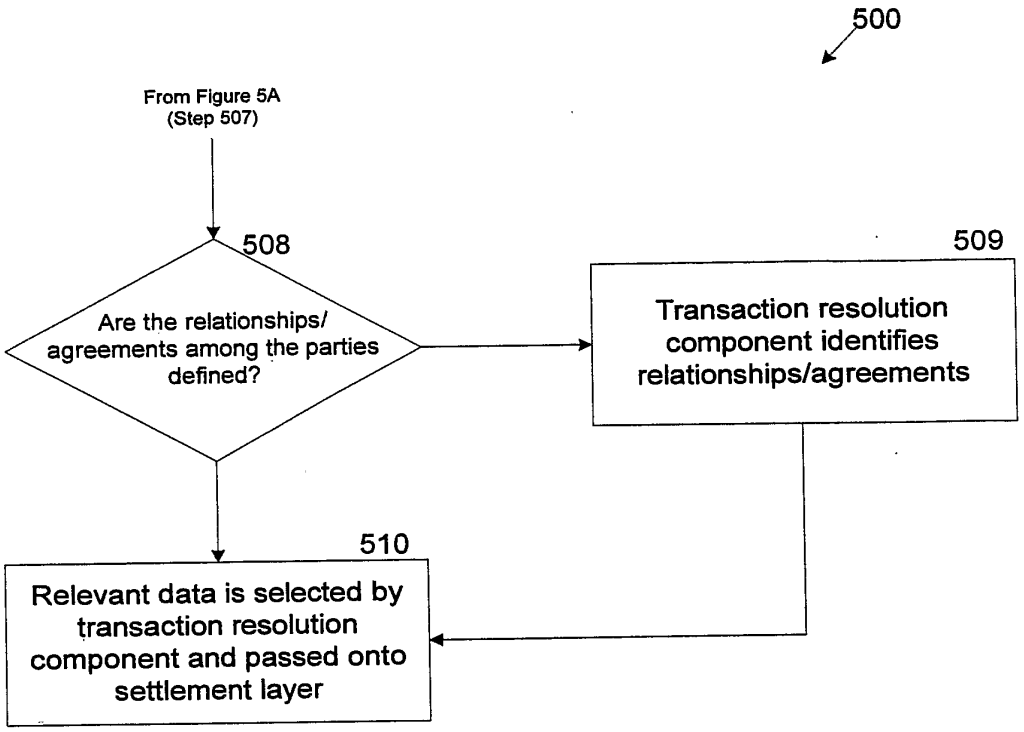

500
From Figure 5A
(Step 507)
508
Are the relationships/ agreements among the parties defined?
509
Transaction resolution component identifies relationships/agreements
510
Relevant data is selected by transaction resolution component and passed onto settlement layer

Figure 5B

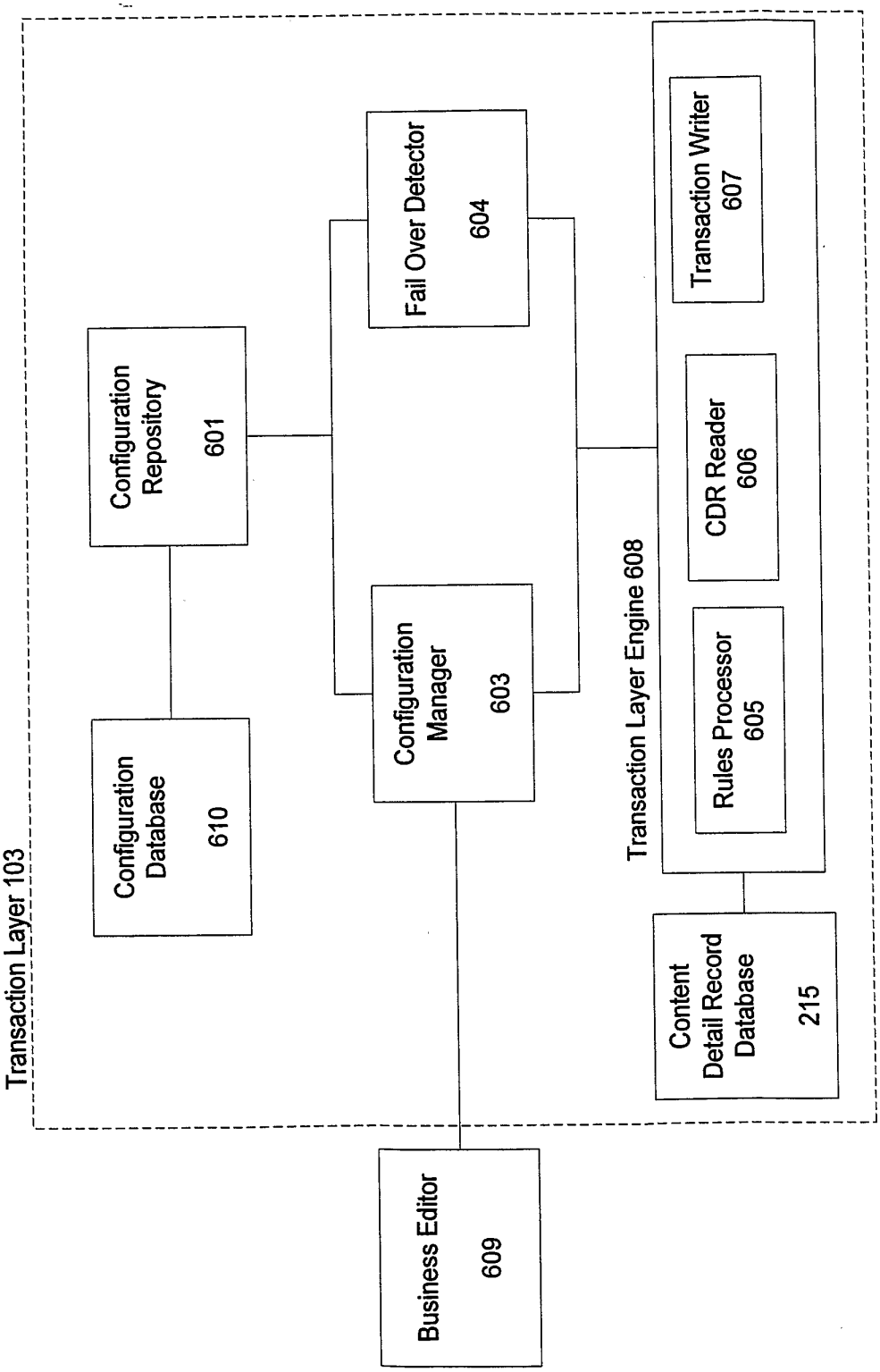

Transaction Layer 103
Configuration Repository 601
Configuration Database 610
Fail Over Detector 604
Configuration Manager 603
Transaction Layer Engine 608
Transaction Writer 607
CDR Reader 606
Rules Processor 605
Content Detail Record Database 215
Business Editor 609

Figure 6

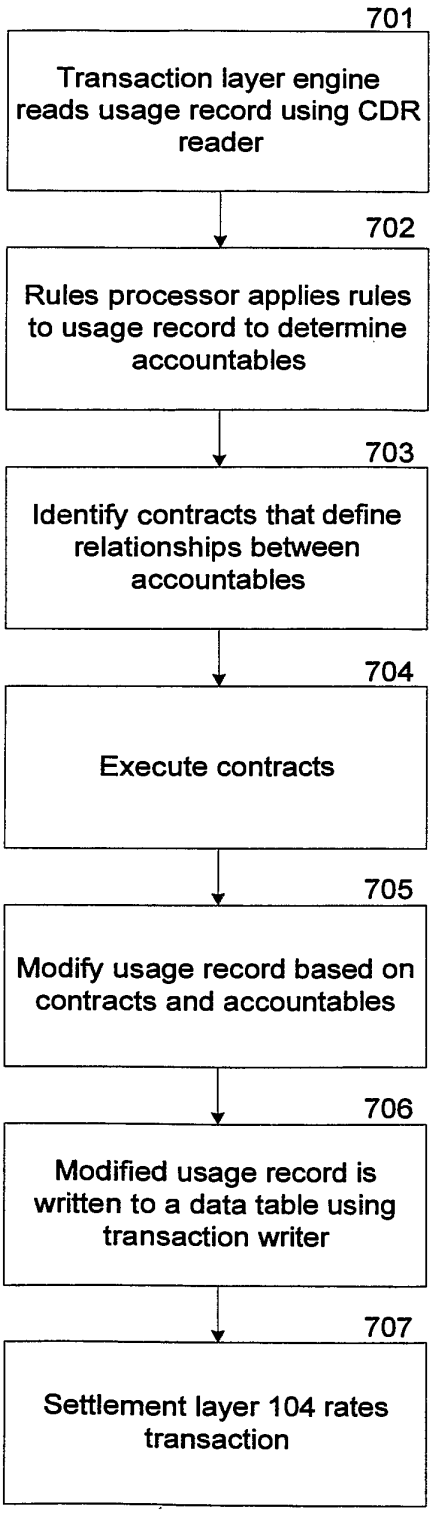

701
Transaction layer engine reads usage record using CDR reader
702
Rules processor applies rules to usage record to determine accountables
703
Identify contracts that define relationships between accountables
704
Execute contracts
705
Modify usage record based on contracts and accountables
706
Modified usage record is written to a data table using transaction writer
707
Settlement layer 104 rates transaction
700

Figure 7

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 545 114 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.06.2005 Bulletin 2005/25

(51) Int Cl.[7]: **H04M 15/00**, H04Q 3/00

(21) Application number: **04027514.1**

(22) Date of filing: **19.11.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK YU

(30) Priority: **19.12.2003 CN 200310122726**

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventors:
- **ShuGuang, Jin,**
CTO, Alcatel Shanghai Bell Co. Ltd.
201206 Shanghai (CN)
- **Yan, Chen, CTO, Alcatel Shanghai Bell Co. Ltd.**
201206 Shanghai (CN)
- **Peiliang, Xu, CTO, Alcatel Shanghai Bell Co. Ltd.**
201206 Shanghai (CN)

(74) Representative:
Dreiss, Fuhlendorf, Steimle & Becker
Patentanwälte
Postfach 10 37 62
70032 Stuttgart (DE)

(54) A method and apparatus for division of revenue of communication among different proprietors

(57) A method and apparatus for division of revenue of communication among different proprietors is provided in this invention, where the division of revenue among the different proprietors is performed by a gateway office, wherein the gateway office will set a source parameter and a destination parameter respectively from the source and the destination when a call goes through the gateway office; Judge the two parameters to get a revenue zone index; Judge the value of the revenue zone index, and modulate the revenue zone index to get a revenue class index; The gateway office generates contents related to the revenue class index; A central memory receives all these contents, adds an increment of each counter of the revenue class memory related to the revenue class index to a corresponding counter and carries out multiple safety mechanisms; Output the information in the revenue class memory to a storage medium for storing, then output it to a billing center for revenue sorting. The billing mode present in this invention is based on group pairs, so it is more adaptive for the gateway office to divide revenue.

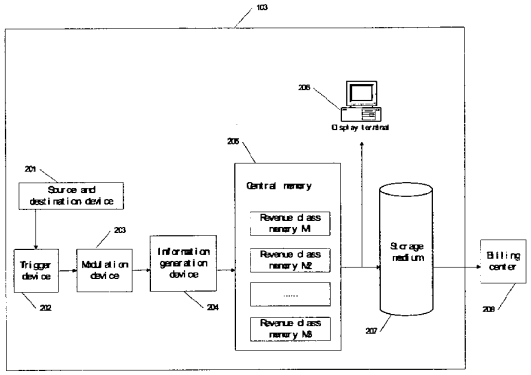


Fig. 2

Printed by Jouve, 75001 PARIS (FR)

EP 1 545 114 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a method and apparatus for division of revenue of telecommunication among different proprietors.

RELATED ART

[0002] As to the relay jumping table billing, in the SPC exchange, it takes relay groups (income and outgoing) as revenue billing units, and accumulates all metering impulses of the relay group as the billing content. Although this technology is simple, it is not able to provide enough flexibility in resource sorting and billing content selecting.

[0003] As to the detail billing, in the SPC exchange, it generates a detail record for each call. All these records (telephone billing list) will be sent out from the SPC exchange after a specific period. A specific sorting department sorts all received telephone billing list, which will be treated as the billing content after sorting and summation. It can satisfy all kinds of user's customized demands, but there is a large number of temporary data transferring between the SPC exchange and the sorting department, and the investments on the equipments will be expanded greatly in order to satisfy demands.

SUMMARY OF THE INVENTION

[0004] In order to solve said problems of existing technology, this invention provides all kinds of methods for the division of revenue at the SPC exchange level of the gateway office, to satisfy various potential billing demands among the proprietors. Moreover, it is needless for proprietors to add investments immediately to meet with the additional demands for detail billing because of this demand.

[0005] The present invention provides a method for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the method comprising that:

a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2... n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue

wherein in said step c), said revenue zone index is modulated by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

wherein in said step d), said contents related to the revenue class index R_j as said in step c) include static and dynamic information on the call as said in step a);

[0006] In said step e), the revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

[0007] In said step f), the central memory sends the information in the revenue class memory M_j as said in step e) to a display terminal.

wherein in said step e), the multiple safety mechanisms include:

[0008] The central memory introducing a windowing mechanism during a receiving procedure;

[0009] The accumulation of each counter having a hot backup;

[0010] Each counter backups its information to a pair of hard disks with specific intervals.

wherein in said step f), the predefined formatted scheme is either a general scheme or a scheme customized according to user's needs.

[0011] The present invention provides an apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the apparatus comprising a source and destination device located in the gateway office, and further a trigger device, a modulation device, an information generation device□a central memory and a storage medium which are all located in the gateway office, wherein:

[0012] When a call goes through the gateway office, the source and destination device located in the gateway office respectively extracts a source parameter and a destination parameter according to a source of calling user and a destination of called user;

[0013] The trigger device judges values of the source parameter and the destination parameter, and if there is one of the values of the parameters corresponding to a parameter value for stopping a function on the division of revenue , the revenue division is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter, and then judges a value of said revenue zone index, if it corresponds to the parameter value for stopping the revenue division function, t the revenue division function is stopped, otherwise, said revenue zone index is sent to the modulation device;

[0014] The modulation device, according to said call, modulates said revenue area index from the trigger device, and obtains the corresponding revenue class index R_j, j=1, 2...n;

[0015] The information generation device, according to said revenue class index R_j, j=1, 2...n, generates contents related to said revenue class index R_j, and sends them to the central memory after said call is finished;

[0016] The central memory receives the contents related to said revenue class index R_j, and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter, and performs multiple safety mechanisms, and then sends information in said revenue class memory M_j to the storage medium;

[0017] The storage medium stores the information in said revenue class memory M_j with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

wherein said revenue zone index is modulated in the modulation device by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

[0018] Wherein said contents related to the revenue class index R_j include static and dynamic information on the said call;

[0019] Said revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

[0020] Said apparatus also includes a display terminal, which is used to display the information in said revenue class memory M_j.

wherein said multiple safety mechanisms include:

[0021] The central memory introducing a windowing mechanism during a receiving procedure;

[0022] The accumulation of each counter having a hot backup;

[0023] Each counter backups its information to a pair of hard disks with specific intervals.

wherein the predefined formatted scheme is either a general scheme or a customized scheme according to user's needs.

[0024] The division of revenue of this invention is a kind of billing method based on group pairs, making it more adaptive for gateway offices to divide revenue. Moreover, the division of revenue method present in this invention is not only based on relays, but it can also be realized by other billing units, comparing to the present technology whose billing unit is simply based on relays. The revenue class in this invention is abstract, and can be a mixture of several different entity types. Besides, the present invention also adopts a new normalized input and output format for the division of revenue.

DESCRIPTION OF THE DRAWINGS

[0025]

Fig .1 is a flowchart illustrating different proprietors realizing division of revenue by the gateway office in accordance with a preferred embodiment of the invention;

Fig .2 is a map of the gateway office realizing division of revenue in accordance with a preferred embodiment of the invention;

Fig .3 is a flowchart illustrating the safety mechanisms of the central memory in accordance with a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0026] This invention will be further explained with reference to the drawings and an embodiment.

[0027] This invention provides a method and a apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office.

[0028] Here, the gateway office is an interface exchanging office carrying out transmission of telephone services among different proprietors. For instance, a user of the Shanghai Mobile makes a call to another fixed phone user of the Shanghai Telecom, which will reach the fixed phone user via a gateway office between the two companies. Since the Shanghai Telecom proprietor has supplied its resource, it will count this kind of resource at the gateway office, and then come to a settlement with the Shanghai Mobile for the revenue. Therefore, the main function of the gateway office is to separately count resources occupied and divide revenue among different proprietors. At the same time, it also provides other gateway services such as the call identification authority and black/white list. The Division of Revenue (DOR) is used to count communication resource among different proprietors.

[0029] As shown in Fig.1, the user 101 is a user of the proprietor A 102 and the user 105 is a user of the proprietor B 104. When a call from the calling user 101 to the called user 104 go in and out from the gateway office 103, the gateway office 103 will get a source from the proprietor A, such as Beijing, and get a destination from the proprietor B, such as Shanghai.

[0030] Fig.2 is a map of the gateway office implementing division of revenue in accordance with an embodiment of the invention, including a source and destination device 201, a billing center 208, which are existing technology, and a trigger device 202, a modulation device 203, an information generation device 204, a central memory 205, a display terminal 206 and a storage medium 207, which are added in this invention. As shown in Fig.2, the source and destination device 201 of the gateway office 103 gets a source parameter and a destination parameter respectively from the source and the destination, which is a numeric value (0-255). For example, if the source is Beijing, the value of the source parameter is "1", and if the destination is Shanghai, the value of the destination parameter is "2".

[0031] At this time the route is already elected to pass, namely when the called user starts ringing, the trigger device 202 of the gateway office 103 judges the value of source and destination parameters. If there is a parameter's value corresponding to the value for stopping the division of revenue function, for example, in this embodiment, if there is a parameter whose value is 0, the division of revenue function is stopped. Those users who do not need this function shield it to consume the least resources. Otherwise, the trigger device 202 obtains a revenue zone parameter according to the source parameter and the destination parameter, as show in table 1.

Destination / Source	Beijing	Shanghai	...	...
Beijing	X1 (north china revenue zone index(1))	X2 (north china-east china revenue zone index (2))	...	...
Shanghai	X3 (east china - north china revenue index (3))	X4 (east - china revenue zone index (4))	...	...
...	...	...	...	...
...	...	...	...	Xn

Table.1

[0032] x_1, x_2, x_3, x_4 ... x_n in the table 1 are revenue zone indices. In this embodiment, the source is Beijing (1) and the destination is Shanghai (2). The trigger device 202 judges the source parameter value and the destination parameter value, if neither of them is zero, the corresponding revenue zone index x_2 is obtained, namely North China - East China revenue zone index, whose revenue zone index value is "2". As shown in table 1, in this invention, the revenue zone indices with different values can simply correspond to the different revenue class indices, which means obtaining many different revenue class indices. In existing technology, if the source and the destination are respectively output relay group and input relay group, it realizes the relay jump table function, and the largest number of the relay group soft table is 10 or 14. In this invention, we can dynamically assign many revenue class indices to one input relay group + several destinations, or to one output relay group + several sources, which actually means a relay group can have the nearly infinite number of the soft tables. This already breaks through the number limitation of the relay group soft table,

which is 10 or 14 in the existing technology, therefore, this invention actually functions better than the current relay jump table technology.

[0033] The trigger device 202 judges the revenue zone index value, if the value is 0, the function of division of revenue is stopped. This is helpful to users' flexible choice, and save system resource to the greatest extent. Otherwise, the modulation device 203 will modulate the revenue zone index. For instance, in this embodiment, the value of the revenue zone index x_2 is "2", not "0", so x_2 is modulated. Refer to table 2 for detailed modulation process.

[0034] As shown in table 2, for instance, proprietors are interested in the voice service of this call, namely require to count and charge the voice service, then said revenue zone index is modulated with one of the modulation parameters and the corresponding revenue class index R_j, j=1, 2...n is obtained. In this embodiment, the revenue zone index x_2 is modulated with the type of call (voice) modulation parameter and the corresponding revenue class index R1 is obtained, which corresponds to the voice service of the DDD call, namely the DDD call list. Furthermore, if there are other calls corresponding to the ISDN call, the revenue zone index x_2 will be modulated with the type of call (voice) modulation parameter, and the corresponding revenue class index R2 will be obtained, which means R2 corresponds to the voice service of the ISDN, namely the ISDN call list.

Revenue zone index	Type of call	Revenue class index	Billing list
X2 (north china- east china revenue zone index(2))	Type of call (voice)	R1 (east china - north china revenue class index (1)) (DDD call)	DDD billing list
		R2 (east china - north china revenue class index (2)) (ISDN call)	ISDN billing list
		R3 (east china - north china revenue class index (3)) (IN call)	IN billing list
		...	...

		R4 (east china - north china revenue class index (n)) (other types of call)	Other types of billing lists

Table.2

[0035] This invention provides an extremely flexible modulation method, wherein said modulating characteristics in this invention means modulating said revenue zone index using one or several modulation parameters, and the different corresponding revenue class indices by different combinations of these modulation parameters are obtained. The purpose of the modulation is to further conclude and arrange all revenue by different modulation parameters, and make revenue sortable according to the proprietor's demand, namely to perform revenue class indexing. At the end, various billing data will be obtained through different revenue class indices. The modulation parameters can be type of call (voice), bear capacity, high level carrying(HLC), analog or ISDN user and so on.

[0036] Said modulation in this invention is carried out during the calling process. In the existing technology, the relationship between each revenue zone index and revenue class index is usually one-to-one correspondence, which could satisfy the demand of most users. In this case, the modulation step can be ignored.

[0037] After the called user 105 gives reply, and before the call is released, the information generation device 204 of the gateway office 103 generates contents related to said revenue class index, such as R1, which include static and dynamic information on the call. The static information contains the modulating characteristics as shown in table 2, the calling number, the called number, the route and so on, the dynamic information contains the call holding time, the answering time and so on. These static information and dynamic information related to the call will be sent to the central memory 205 of the gateway office 103 after the call is finished.

[0038] After the call is released, namely the call is finished, the central memory 205 of the gateway office 103 receives these contents related to said revenue class index R_j, and based on these contents, adds the increment values of every counter of the revenue class memory M_j (j=1, 2...n), which is related to said revenue class index R_j, to the corresponding counter. For example, in this call there are several counters in the revenue class memory M1 corresponding to the revenue class index R1 of the central memory 205, such as a total-number-of-calls counter□total-length-of-calls counter, etc, which respectively accumulate the total number of calls and the total length of calls, based on this call. This revenue class memory M_j (j=1, 2...n) is set according to users' needs during the gateway office initializing procedure.

[0039] Because of the importance of the resource, multiple safety mechanisms are performed in the present invention, which including: The central memory 205 introduces a windowing mechanism during the receiving procedure. The accumulation of each counter has a hot backup, as shown in Fig.3, the central memory 205 is comprised of primary central storage region 301, hot backup central storage region 302, primary hard disk 305 and standby hard disk 307, the primary central storage region 301 and the hot backup central storage region 302 stores at the same time, as arrow 303 shows, one-region working task can be performed under certain circumstances. However, synchronous working starts as soon as the two-region working task takes over.Each counter backups its information to a pair of hard disks with specific intervals, namely to the primary hard disk 305 and the standby hard disk 306, the backuping task is executed by the primary central storage region 301, as arrow 304 shows. Since these safety mechanisms are existing technology, just a simply introduction is provided.

[0040] The central memory 205 sends the information of said revenue class memory M_j to the storage medium 207, which stores the information with reference to a predefined formatted scheme and sends the information to the billing center 208 for revenue sorting the same way as other bill documents. The central memory 205 also can send the information of said revenue class memory M_j to the display terminal 206. For example, display contents of each counter of the revenue class memory M_j through display terminal 206, then the network resource occupation situation of each

proprietor can be observed directly and instantly, which realizes flexible online operation. The revenue sorting here means arranging the billing data (such as the detailed billing phone list, the double counting jump table file, all said revenue class indices) generated in the gateway office in a document, sending the entire document to the billing center 208, where the document will be operated according to the predefined procedure and reorganized into a list of each revenue class and the corresponding total number of calls, total length of calls.

[0041] The predefined format can be a general style, as shown in table 3, the first part is a file header, such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc. The following is a revenue class index sequence, the last part is a file trailer, such as an end-of-file indicator; The format can also be a customized style according to the user's need, as shown in table 4, the first part is a file header, such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc, the following is a each revenue class index arranged in an order of the relay group and the bear type, the last part is a file trailer, such as an end-of-file indicator.

Table.3

<table>
<tr><td colspan="2">File header (such as: such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc)</td></tr>
<tr><td rowspan="4">Arranging each revenue class index in order</td><td>Revenue class index sequence number 1</td></tr>
<tr><td>Total number of calls</td></tr>
<tr><td>Total length of calls</td></tr>
<tr><td>Total number of pulses</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td colspan="2">File trailer (such as end-of-file indicator)</td></tr>
</table>

Table.4

<table>
<tr><td colspan="2">File header (such as: such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc)</td></tr>
<tr><td rowspan="4">Arranging each revenue class index in an order of the relay group and the bear type</td><td>Revenue class index sequence number (1, 2, 3)</td></tr>
<tr><td>Corresponding relay group name</td></tr>
<tr><td>Corresponding bear type</td></tr>
<tr><td>Total number of calls</td></tr>
<tr><td rowspan="2"></td><td>Total length of calls</td></tr>
<tr><td>Total number of pulses</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td colspan="2">File trailer (such as end-of-file indicator)</td></tr>
</table>

[0042] Therefore, the output format adopted in this invention greatly meets the users' demand, and makes it very convenient for the users to introduce this new function. Moreover, the output format can be customized to meet the needs of various high-end users. The output format provides more options, such as bureau name, file generation time, relay group name and other specific information, making it more supportive to on-line transmission.

[0043] More detailed steps corresponding to the embodiment of this invention are as follows:

a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue

area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2... n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue

[0044] As to a medium-sized gateway office (10 hours when busy, 100CAPS bill list), the data volume ratio of detail billing in existing technology to the division of revenue in the present invention is over 100:1.

[0045] The present invention also greatly reduces the massive dump of the exchanger, the mass data processing of the sorting center and the mass data storage and transmission, saving various resources.

[0046] The division of revenue of this invention is a kind of billing method based on group pairs, making it more adaptive for gateway offices to divide telecommunication revenue. Moreover, the division of revenue method present in this invention is not only based on relays, but it can also be realized by other billing units, comparing to the exiting technology whose billing unit is simply based on relays.

[0047] It should be understood that the said embodiment has been presented by way of example only, and not limitation. Thus, all modifications that fall within the scope of this invention are intended to be included therein.

Claims

1. A method for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the method comprising that:

   a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

   b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

   c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

   d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

   e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

   f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

2. The method according to claim 1, wherein in said step c), said revenue zone index is modulated by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

3. The method according to claim 1, wherein in said step d), said contents related to the revenue class index R_j as said in step c) include static and dynamic information on the call as said in step a);

   In said step e), the revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

   In said step f), the central memory sends the information in the revenue class memory M_j as said in step e)

to a display terminal.

4. The method according to claim 1, wherein in said step e) the multiple safety mechanisms include:

The central memory introducing a windowing mechanism during a receiving procedure;
The accumulation of each counter having a hot backup;
Each counter backups its information to a pair of hard disks with specific intervals.

5. The method according to claim 1, wherein in said step f), the predefined formatted scheme is either a general scheme or a scheme customized according to user's needs.

6. An apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the apparatus comprising a source and destination device located in the gateway office, and further a trigger device, a modulation device, an information generation device, a central memory and a storage medium which are all located in the gateway office, wherein:

When a call goes through the gateway office, the source and destination device located in the gateway office respectively extracts a source parameter and a destination parameter according to a source of calling user and a destination of called user;
The trigger device judges values of the source parameter and the destination parameter, and if there is one of the values of the parameters corresponding to a parameter value for stopping a function on the division of revenue ,the revenue division is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter, and then judges a value of said revenue zone index, if it corresponds to the parameter value for stopping the revenue division function, the revenue division function is stopped, otherwise, said revenue zone index is sent to the modulation device;
The modulation device, according to said call, modulates said revenue area index from the trigger device, and obtains the corresponding revenue class index R_j, j=1, 2...n;
The information generation device, according to said revenue class index R_j, j=1, 2...n, generates contents related to said revenue class index R_j, and sends them to the central memory after said call is finished;
The central memory receives the contents related to said revenue class index R_j, and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter, and performs multiple safety mechanisms, and then sends information in said revenue class memory M_j to the storage medium;
The storage medium stores the information in said revenue class memory M_j with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

7. The apparatus according to claim 6, wherein said revenue zone index is modulated in the modulation device by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

8. The apparatus according to claim 6, wherein:

Said contents related to the revenue class index R_j include static and dynamic information on the said call;
Said revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;
Said apparatus also includes a display terminal, which is used to display the information in said revenue class memory M_j.

9. The apparatus according to claim 6, wherein said multiple safety mechanisms include:

The central memory introducing a windowing mechanism during a receiving procedure;
The accumulation of each counter having a hot backup;
Each counter backups its information to a pair of hard disks with specific intervals.

10. The apparatus according to claim 6, wherein the predefined formatted scheme is either a general scheme or a customized scheme according to user's needs.

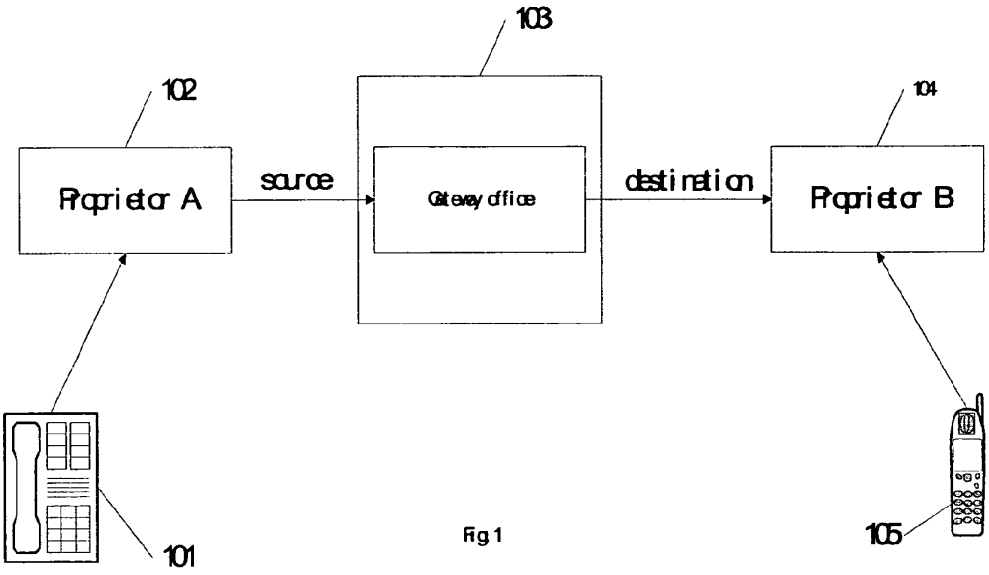

103
102
104
Proprietor A
source
Gateway office
destination
Proprietor B
101
105

Fig 1

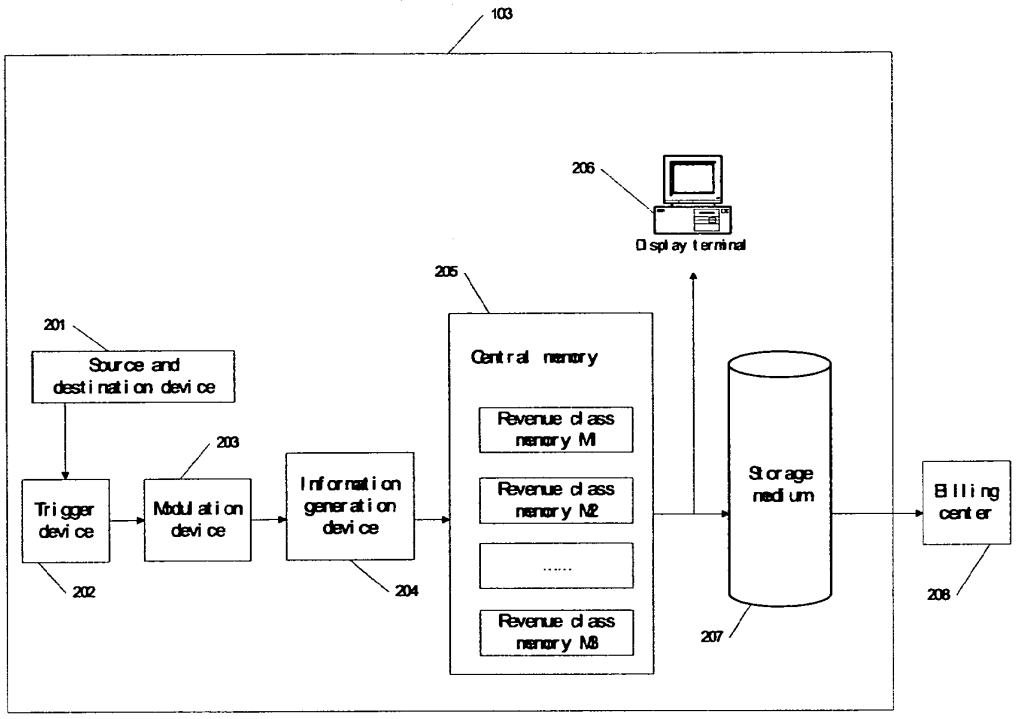

103
206
Display terminal
205
201
Source and destination device
Central memory
Revenue class memory M1
203
Trigger device
Modulation device
Information generation device
Revenue class memory M2
.....
Revenue class memory M8
Storage medium
Billing center
202
204
207
208

Fig. 2

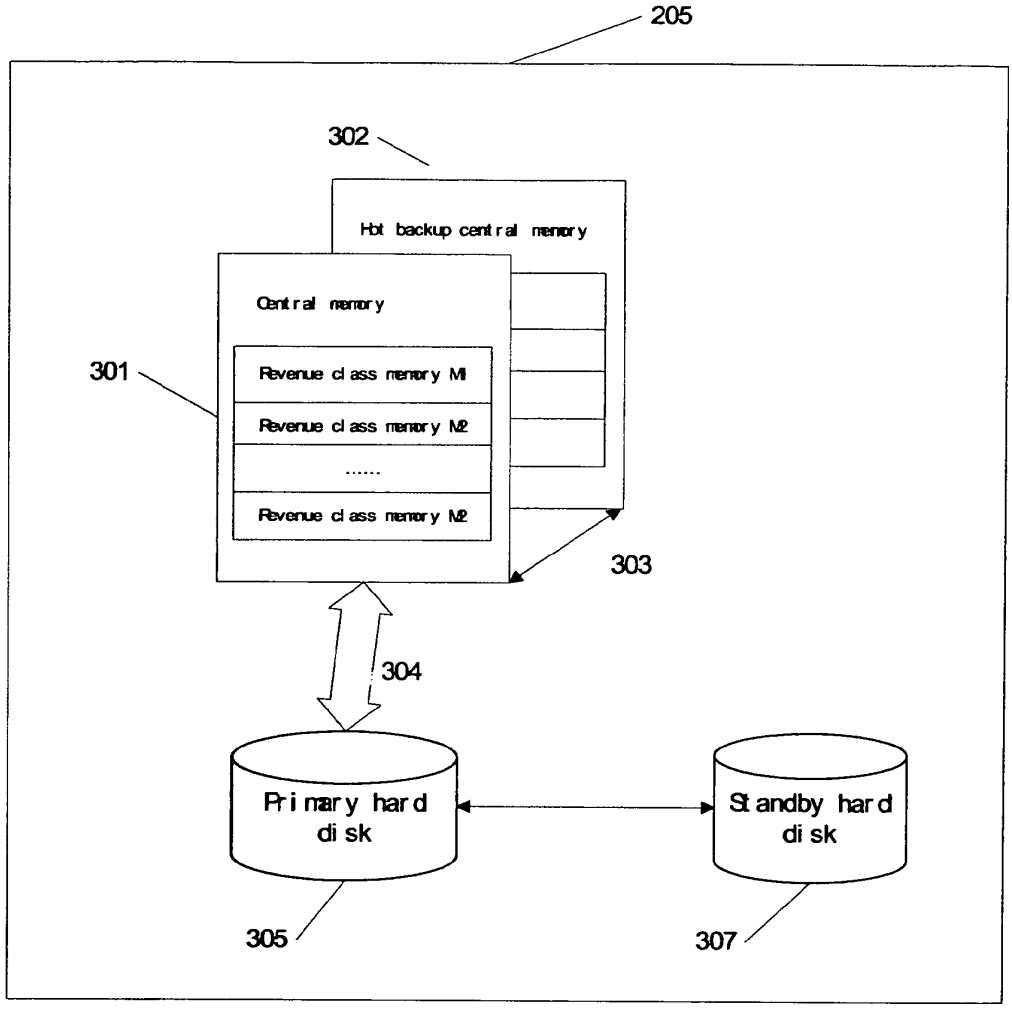

205
302
Hot backup central memory
Central memory
301
Revenue class memory M1
Revenue class memory M2
.....
Revenue class memory M2
303
304
Primary hard disk
Standby hard disk
305
307

Fig. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 02 7514

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 5 768 353 A (BROWNE ET AL) 16 June 1998 (1998-06-16) * column 1, line 33 - column 3, line 26 * * column 5, line 25 - column 7, line 39 * * column 10, line 22 - column 15, line 58 * * claims 1-17 *	1-10	H04M15/00 H04Q3/00
P,A	US 2004/033797 A1 (RAIVISTO TOMMI ET AL) 19 February 2004 (2004-02-19) * claims 1-20 * * figures 1,2 *	1-10	
A	EP 0 483 091 A (ERICSSON - GE MOBILE COMMUNICATIONS HOLDING INC; ERICSSON INC) 29 April 1992 (1992-04-29) * column 2, line 30 - line 47 * * claims 1-3 *	1-10	
A	WO 03/049351 A (CIBERNET, INC) 12 June 2003 (2003-06-12) * page 10, line 3 - page 11, line 29 * * page 12, line 21 - page 13, line 13 * * page 14, line 29 - page 16, line 28 * * page 18, line 1 - page 23, line 16 * * page 41, line 15 - page 44, line 7 * * figures 1-4,9 *	1-10	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04M H04Q
P,A	US 2004/210522 A1 (BISSANTZ ANNETTE S ET AL) 21 October 2004 (2004-10-21) * paragraph [0027] - paragraph [0029] *	1-10	
A	US 6 134 307 A (BROUCKMAN ET AL) 17 October 2000 (2000-10-17) * column 4, line 13 - column 5, line 17 *	1-10	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 April 2005	Patlaka, E.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 02 7514

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 569 175 A (AMERICAN TELEPHONE AND TELEGRAPH COMPANY; AT&T CORP) 10 November 1993 (1993-11-10) * column 6, line 24 - column 7, line 19 * * figure 5 * * claims 1-3 *	1-10	
A	US 5 910 979 A (GOEL ET AL) 8 June 1999 (1999-06-08) * claims 1-3 *	1-10	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 April 2005	Patlaka, E.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 02 7514

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768353 A	16-06-1998	AU 697367 B2	01-10-1998
		AU 6383094 A	24-10-1994
		AU 697499 B2	08-10-1998
		AU 6383194 A	24-10-1994
		CA 2159000 A1	13-10-1994
		CA 2159002 A1	13-10-1994
		CN 1122639 A ,C	15-05-1996
		CN 1122640 A ,C	15-05-1996
		DE 69404452 D1	28-08-1997
		DE 69404452 T2	15-01-1998
		DE 69433814 D1	01-07-2004
		DK 692172 T3	02-03-1998
		EP 0692172 A1	17-01-1996
		EP 0692173 A1	17-01-1996
		ES 2107200 T3	16-11-1997
		FI 954627 A	09-11-1995
		FI 954628 A	10-11-1995
		WO 9423529 A1	13-10-1994
		WO 9423530 A1	13-10-1994
		HK 1001747 A1	03-07-1998
		HK 1014410 A1	11-03-2005
		JP 8508619 T	10-09-1996
		JP 8508620 T	10-09-1996
		JP 2002199130 A	12-07-2002
		NO 953898 A	29-11-1995
		NO 953899 A	29-11-1995
		NZ 263224 A	26-07-1996
		NZ 263225 A	26-01-1998
		SG 48839 A1	18-05-1998
		SG 50490 A1	20-07-1998
		US 5802142 A	01-09-1998
		US RE37856 E1	24-09-2002
		US RE37857 E1	24-09-2002
US 2004033797 A1	19-02-2004	AU 2003255864 A1	25-02-2004
		WO 2004015971 A1	19-02-2004
EP 0483091 A	29-04-1992	CA 2098191 A1	02-05-1993
		US 5063591 A	05-11-1991
		CN 1061692 A ,C	03-06-1992
		CN 1108851 A ,C	20-09-1995
		EP 0483091 A2	29-04-1992
		NZ 240072 A	25-02-1994
		WO 9309639 A1	13-05-1993
		DE 69127161 D1	11-09-1997
		DE 69127161 T2	18-12-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 02 7514

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0483091 A		ES 2107448 T3	01-12-1997
		HK 1001948 A1	17-07-1998
WO 03049351 A	12-06-2003	US 2003120594 A1	26-06-2003
		AU 2002365834 A1	17-06-2003
		WO 03049351 A2	12-06-2003
US 2004210522 A1	21-10-2004	NONE	
US 6134307 A	17-10-2000	NONE	
EP 0569175 A	10-11-1993	US 5333184 A	26-07-1994
		CA 2092590 A1	07-11-1993
		DE 69332461 D1	12-12-2002
		DE 69332461 T2	28-08-2003
		EP 0569175 A2	10-11-1993
		ES 2184736 T3	16-04-2003
		JP 2795596 B2	10-09-1998
		JP 6037936 A	10-02-1994
US 5910979 A	08-06-1999	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 887 732 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
13.02.2008 Bulletin 2008/07

(21) Application number: **06742044.8**

(22) Date of filing: **30.05.2006**

(51) Int Cl.:
H04L 12/14 *(2006.01)*

(86) International application number:
PCT/CN2006/001156

(87) International publication number:
WO 2006/128371 (07.12.2006 Gazette 2006/49)

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priority: **30.05.2005 CN 200510073415**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District
Shenzhen
Guangdong 518129 (CN)

(72) Inventor: **ZHAO, Hang,**
Huawei Administration Building
Shenzhen Guangdong 518129 (CN)

(74) Representative: **Pfenning, Meinig & Partner GbR**
Patent- und Rechtsanwälte
Theresienhöhe 13
80339 München (DE)

(54) **A METHOD AND SYSTEM FOR CONTENT CHARGING**

(57) A method for content charging includes: the portal server transmits the service activation request to the policy server based on the request for user using the service; the policy server determines the service policy corresponding to the service request after responding to the service activation request and distributes the service policy activation message to the content control gateway; the content control gateway performs the service policy and reports the user service usage message to the policy server; the policy server performs the charging according to the user service usage message. The solution provided by the present invention can realize the exact and low-cost charging for the content service and meet the requirement of QoS dynamic adjustment of the content service.

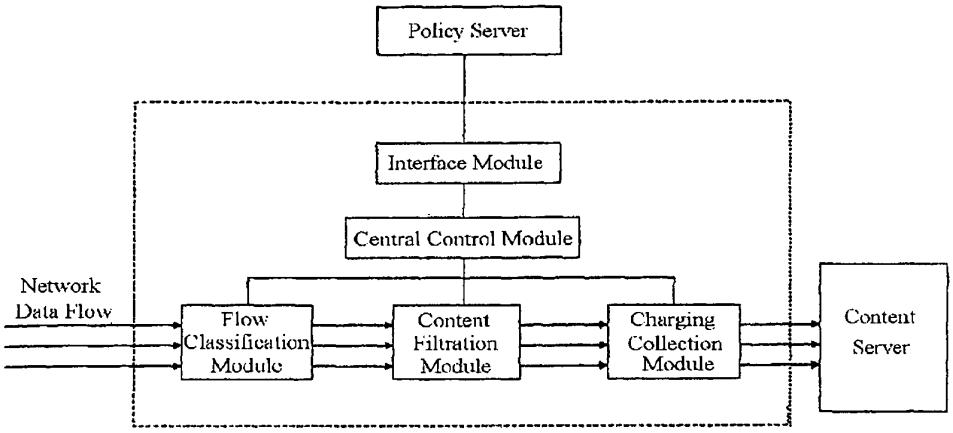


Fig.3

EP 1 887 732 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to the technical field of network communications, in particular, to a method and a system for content charging.

Background of the Invention

[0002] With the rapid development of the Internet, content services become more and more abundant. Correspondingly, Internet Content Providers (ICPs) for getting profit by providing contents come on the scene. By cooperating with the ICP, service providers may increase the income of the access service by expanding the scale of network userson one hand, and earn the profit sharing of content income of the ICP on the other hand. At the same time, the ICP may obtain a low-cost channel for selling its content service rapidly.

[0003] The content platform of the service provider is developed on such background. The general mode of the content platform is as follows: The service provider provides a technical platform, and the ICP issues its content service via this platform. The service provider performs advertising, authentication, charging for the use of the content service via the platform. The user uses the content service provided by each ICP via the platform. The content platform records various fees caused by the user, and all of the fees will be recorded on a content account provided to the user by the service provider. With this content platform, the user does not need to settle accounts with each ICP; instead, the user only needs to settle accounts with the service provider.

[0004] The existing content charging solution for this content platform is usually implemented as follows:

[0005] A user connects to the network, logs in a portal website Portal Server, and connects to a Content Server of an ICP via a content channel. If the user is interested in a content provided by the ICP, then he/she clicks the button "OK", and the ICP Content Server will send an authentication request to the content platform of the service provider. If the authentication is passed, the right to use the content is assigned to the user and a charging start message is sent to the content platform.

[0006] To ensure the accuracy of the charging, the Content Server of the ICP sends an intermediate charging message to the content platform at a certain time interval during the usage of the content. When the user logs out the Content Server, the Content Server of the ICP sends a charging completion message to the content platform.

[0007] The content platform processes the charging message in real time, and performs rating and accounting on the content consumption of the user according to the information in the charging message such as service number, time length traffic flow, etc., together with the charging policy of the service.

[0008] In the prior art, strict requirements are laid on the interconnection technology between the content platform and the ICP. The ICP has to carry out customized development according to the content platform authentication and charging interface provided by the service provider, and joint debugging and testing should be performed after the development. Services may only be formally issued after the testing is passed. Thus, the cost is very high.

[0009] Some small-scale ICPs are weak in technical strength and they are not able to carry out customized development according to the charging interface. Some other ICPs purchase their service contents, such as multiplayer-fighting games, from other software company, so they have no source code for interface development, and are not able to implement content charging for such services.

[0010] Quality of Service (QoS) is required for some content services. For example, Video On Demand (VOD) service requires a broad bandwidth. However, in the mode aforementioned, the bandwidth may not be dynamically adjusted according to the service, and it is disadvantageous for operation and management.

[0011] In the actual operation of the ICP, it is difficult for the service provider to control the correctness of the service number, traffic flow and time length in the charging message, thus accurate charging may not be performed.

Summary of the Invention

[0012] The present invention provides a method and a system for implementing content charging at low cost, so that the service charging may be more accurate and reasonable, and the bandwidth may be adjusted dynamically according to the service.

[0013] The present invention provides a method for content charging, including:

[0014] sending, by a Portal Server, a service activation request to a Policy Server, based on a service request from a user;

[0015] responding to the service activation request, determining a service policy corresponding to the service request, and delivering a service policy activation message to a content control gateway, by the Policy Server;

[0016] executing the service policy and reporting user service consumption information to the Policy Server by the content control gateway; and permitting the user to use the service, and charging according to the user service consumption information reported by the content control gateway, by the Policy Server.

[0017] The method further includes:

[0018] sending, by the Portal Server, a service deactivation request to the Policy Server, when a request for stopping the service from the user is received; and

[0019] responding to the service deactivation request, delivering a service policy cancellation message, performing rating and accounting according to the consump-

tion information, by the Policy Server.

[0020] The content control gateway reports the user service consumption information to the Policy Server periodically during the service;

[0021] The Policy Server performs rating according to the user service consumption information, and settles accounts on the service consumption of the user according to each rating information after the user stops using the service.

[0022] After responding to the service activation request, the Policy Server queries a preset correlation table between the service and the service policy according to the service activation request, determines the service policy corresponding to the service, and extracts the parameters needed for executing the service policy, then fills the parameters in the service policy activation message and delivers the service policy activation message to the content control gateway.

[0023] Wherein, the service policy message includes the information of the source IP address, destination IP address, destination port, destination service resource and traffic flow information of the network packet.

[0024] The content control gateway grants the right to the source IP address of the user network packet to access the destination IP address, destination port and destination service resource, and controls the network flow according to the traffic flow information in the policy message.

[0025] The content control gateway distinguishes between the content data flows according to the Content Server or the service port of the content, controls the content data flow and collects the consumption information.

[0026] In another aspect of the invention, there is provided a system for content charging, which includes a Portal Server and a Content Server, wherein

[0027] the system further includes a Policy Server and a content control gateway, the Policy Server is connected with the Portal Server and the content control gateway and is adapted to deliver a service policy activation message and a service policy cancellation message, perform rating and charging according to user service consumption information reported by the content control gateway;

[0028] the content control gateway is connected with the Content Server and is adapted to control access to the Content Server of the user according to the access right, count the service consumption information and report the user service consumption information to the Policy Server for charging.

[0029] The Policy Server includes a central control module, a charging engine module, a portal interface module and a device interface module.

[0030] The central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to respond to a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver a service policy activation message via the device interface module, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating.

[0031] The portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request.

[0032] The device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module.

[0033] The charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

[0034] The content control gateway includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0035] The central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy.

[0036] The flow classification module is adapted to check, classify, control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and permit a network flow that conforms to the policy to pass.

[0037] The content filtration module is adapted to check, classify, control resources to be accessed by the network packet on the application layer, and permit the network flow that conforms to the policy to pass.

[0038] The charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module.

[0039] The interface module is adapted to provide an interface between the central control module and the Policy Server.

[0040] In still another aspect of the invention, there is provided a Policy Server for implementing content charging, which includes a central control module, a charging engine module, a portal interface module and a device interface module.

[0041] The central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to receive a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver the service policy activation message via the device interface, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating.

[0042] The portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request.

[0043] The device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module.

[0044] The charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

[0045] The server further includes a database interface and a memory database, Through the database interface, an external database and the memory database may be accessed. The memory database is adapted to store policy data, charging data, configuration data and user session data, and receive an instruction from the central control module for updating the data.

[0046] The invention further provides a content control gateway for implementing the charging method according to claim 1, which includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0047] The central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy.

[0048] The flow classification module is adapted to check, classify and control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and only permit a network flow that conforms to the policy to pass.

[0049] The content filtration module is adapted to check, classify and control resources to be accessed by the network packet on the application layer, and only permit the network flow that conforms to the policy to pass.

[0050] The charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module.

[0051] The interface module is adapted to provide an interface between the central control module and the Policy Server.

[0052] In summary, in the method and system for content charging according to the embodiments of the invention, by determining the service policy corresponding to the service information and executing the service policy, the user is controlled to use the service, the content data flows are distinguished according to the Content Server or the service port of the content, and the content data flow is controlled and the consumption information is collected. So that charging may be performed according to the user service consumption information reported. As a result, the interconnection difficulty and interconnection cost between the ICP Content Server and the content platform of the service provider may be lowered greatly, and a non-coding interconnection operation solution may be provided. Thus, the service provider may rapidly dispose a content service, the ICP may be effectively prevented from falsifying data, and accurate charging data may be provided. At the same time, the corresponding network QoS may be ensured according to the requirements of a certain content service, thus an overall QoS may be provided, and the market competitive power may be improved.

Brief Description of the Drawings

[0053] Figure 1 is a schematic diagram showing an exemplary system structure according to an embodiment of the invention;

[0054] Figure 2 is a schematic diagram showing the structure of the Policy Server according to an embodiment of the invention;

[0055] Figure 3 is a schematic diagram showing the structure of the content control gateway according to an embodiment of the invention; and

[0056] Figure 4 is a flow chart of the method according to an embodiment of the invention.

Detailed Description of the Embodiments

[0057] To make the principle, characteristics and advantages of the invention clearer, the invention will now be described in detail hereinafter in conjunction with the embodiments and the drawings of the invention.

[0058] As shown in Figure 1, the system for content charging according to an embodiment of the invention includes a Portal Server, a Policy Server, a Content Control Gateway (CCG) and a Content Server. Wherein, the Policy Server is connected with the Portal Server and the content control gateway, for delivering or canceling a service policy message, and performing rating and charging according to the service usage information reported by the CCG, such as traffic flow and time length. The CCG is connected with the Content Server, for controlling the access to the Content Server of the user, counting the service consumption information, and periodically reporting the related data to the Policy Server for charging. The Portal Server provides a portal for user access, and provides the user with functions such as login, service channel, service selection, self-help service. The Content Server is a server through which the ICP provides contents. There may be a plurality of Content Servers connected with a CCG, and various contents may also be issued on a Content Server. The servers on which the contents exist may be different, and the service ports of the contents, i.e. Transmission Control Protocol/User Data Protocol (TCP/UDP) ports may be different. The CCG distinguishes between the content data flows according to the server on which the contents exist or the service port of the content, and controls the content

data flows and collects data respectively for executing the policy.

[0059] The service policy message may be regarded as an indication message for the service data flow rules, which comprises parameters such as the source IP address, destination IP address, destination port, service resource information and traffic flow information of a network packet. For example, when a Content Server provides a game service, if a user wants to access the game server, the content of the corresponding service policy message may include the following information: the source IP address (which may be the IP address of the user), the IP address of the game server, the port of the game server (which may refer to the TCP/UDP port), the upstream bandwidth, the downstream bandwidth, the Universal Resource Locator (URL), etc. Thus, if the Policy Server delivers the policy and notifies the CCG, the CCG grants the user the right to access the game server after applying the policy. If the Policy Server instructs the CCG to remove the policy, the current user will lose the right to access the game server.

[0060] If the user wants to access a streaming server, the content of the corresponding service policy message may include the following information: the source IP address, the IP address of the streaming server, the port of the streaming server, the upstream bandwidth, the downstream bandwidth and the URL. The Policy Server delivers a policy and notifies the CCG, and the CCG grants the user the right to access the streaming server after applying the policy and reserves a designated bandwidth for the video/audio stream. If the Policy Server instructs the CCG to remove the policy, then the current user will lose the right to access the streaming server.

[0061] Similarly, if the user wants to access a download server, the content of the corresponding service policy message may include the following information: the source IP address, the IP address of the download server, the port of the download server, the upstream bandwidth, the downstream bandwidth, and the path of the download file. The Policy Server delivers a policy and notifies the CCG, and the CCG grants the user the right to access the download server after applying the policy and reserves a designated download bandwidth. If the Policy Server instructs the CCG to delete the policy, then the current user will lose the right to access the download server.

[0062] Each service and its corresponding service policy are stored in the form of a correlation table between the service and the service policy.

[0063] The internal structure of the Policy Server is as shown in Figure 2, which may include a central control module, a charging engine, a portal interface module, a device interface module, a database interface module and a local memory database (Built-in-Memory).

[0064] The central control module is the core module of the Policy Server, and is mainly responsible for scheduling and controlling other modules in the system. The central control module receives a service activation request sent from the portal interface module, converts it into a service policy message corresponding to the service, and sends the service policy message to the CCG via the device interface. If the policy is executed successfully, the CCG will periodically report the user service consumption information (mainly including time length and traffic flow information), and the central control module invokes the charging engine module for performing rating after receiving the original charging information from the device interface module.

[0065] The portal interface is responsible for interconnecting with the Portal Server, sending the service activation request or the service deactivation request to the central control module, and returning the service request execution result to the Portal Server.

[0066] The device interface module is responsible for interconnecting with the CCG, forwarding the policy information delivered by the central control module to the CCG, and reporting the policy execution information and service usage information to the central control module.

[0067] The charging engine is the charging component of the Policy Server. The central control module invokes the charging engine for performing rating and accounting according to the user service consumption record.

[0068] The database interface enables other subsystems to access the database and the memory database.

[0069] The memory database is an optional component, which may be regarded as a buffer for the external database. The memory database is mainly adapted to store policy data, charging data, configuration data and user session data. By using the memory database, the performance of the system may be improved greatly. The central control module periodically sends an instruction to the memory database for reading the policy data, charging data, configuration data from the external database and refreshing the local memory data.

[0070] The CCG is adapted to control the access to the Content Server of the user, count the service consumption information, and periodically report related data to the Policy Server for performing charging. As shown in Figure 3, the internal structure of the CCG includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0071] The central control module is responsible for receiving the policy sent from the Policy Server and interpreting and executing the policy. During the execution of the policy, the central control module needs to interact with and control the flow classification module, the content filtration module and the charging collection module.

[0072] The flow classification module checks, classifies and controls the information such as the source IP, the destination IP, the destination port of the network packet, on the IP layer. The network flow that conforms to the policy may pass.

[0073] The content filtration module checks, classifies and controls the resources to be accessed by the network packet, such as the URL address applied by the HTTP,

the file path applied by the FTP (File Transfer Protocol) and the RTICP (Real-Time Streaming Protocol) path applied by the stream media, on the application layer. The network flow that conforms to the policy may pass.

[0074] The charging collection module collects the time length and the traffic flow information of the network flow, and reports the original charging data to the central control module. The central control module reports the original charging data to the Policy Server.

[0075] In the method according to an embodiment of the invention, Portal Server receives a service request from a user, and sends a service activation request to Policy Server. The Policy Server determines the corresponding service policy message according to the service after receiving the service activation request, and delivers the service policy message to CCG. The CCG executes the policy message, permits the user to use the service, and periodically reports the user service consumption information to the Policy Server. The Policy Server performs rating and charging according to the consumption information.

[0076] Specifically, as shown in Figure 4, the method includes following steps.

[0077] (1) A user sends a login request to the Portal Server, and the Portal Server authenticates the identity of the user.

[0078] (2) If the authentication is passed, the Portal Server receives the service selection data input by the user.

[0079] (3) The Portal Server sends a service activation request, which carries information such as the user IP, destination IP, service resources, to the Policy Server.

[0080] (4) The Policy Server determines the corresponding service policy message according to the service after receiving the service activation request, and delivers the service policy message to the CCG. Each service and its corresponding service policy are stored in the form of a correlation table between the service and the service policy. This table may be stored on the Policy Server or on a third party device. The Policy Server determines the policy corresponding to the service by querying the correlation table according to the activation request, extracts the parameters needed by the policy according to the activation request and the service policy, fills the parameters in the policy message and delivers the policy message. For example, for a game service, the content of the corresponding service policy message may include the following information: the source IP address (which may be the IP address of the user), the IP address of the game server, the port of the game server (which may refer to the TCP/UDP port), the upstream bandwidth, the downstream bandwidth and the URL.

[0081] (5) The CCG receives the service policy message, executes the service policy according to the instruction of the message, releases the access right from the user IP (which may be a source IP) to the destination IP, destination port or destination URL, and controls the network flow according to the bandwidth parameters in the policy. The CCG sends the policy execution result to the Policy Server after executing the policy.

[0082] (6) The Policy server informs the Portal Server of the service activation result.

[0083] (7) The Portal Server displays the service activation result to the user.

[0084] (8) If the service is activated, the user starts an application client end and performs content consumption, after knowing from the Portal Server that the service is available.

[0085] (9) The CCG periodically reports the service consumption information to the Policy Server during the content service used by the user.

[0086] (10) The Policy Server processes the service consumption information reported by the CCG in real time, and performs rating for the user content consumption.

[0087] (11) The Portal Server receives a request for stopping the service from the user when the user wants to logout the Content Server.

[0088] (12) The Portal Server sends a service deactivation request to the Policy Server.

[0089] (13) The Policy Server delivers a policy cancellation request to the CCG.

[0090] (14) The CCG cancels the policy and returns the policy cancellation result to the Policy server.

[0091] (15) The Policy server informs the Portal Server of the service cancellation result.

[0092] (16) The Portal Server displays the service cancellation result to the user.

[0093] (17) The CCG reports the last service consumption information of the user to the Policy Server.

[0094] (18) The Policy Server processes the service consumption information, performs rating, and settles accounts on the current content consumption according to each rating information.

[0095] In another embodiment of the invention, the content control gateway does not need to periodically report the user service consumption information to the Policy Server. Instead, the content control gateway reports the total service consumption information of the user to the Policy Server at a time after receiving the policy cancellation request delivered by the Policy Server. The Policy Server performs rating and accounting according to the consumption information.

[0096] The invention provides a novel content charging solution, by means of which the interconnection difficulty and the interconnection cost between the ICP Content Server and the content platform of the service provider may be lowered greatly, and the ICP may be effectively prevented from falsifying data, and accurate charging data may be provided. In the meanwhile, the corresponding network QoS may be ensured according to the requirements of a certain content service.

Claims

1. A method for content charging, comprising:

   sending, by a Portal Server, a service activation request to a Policy Server based on a service request from a user;
   responding to the service activation request, determining a service policy corresponding to the service request, and delivering a service policy activation message to a content control gateway, by the Policy Server;
   executing the service policy and reporting user service consumption information to the Policy Server by the content control gateway; and
   permitting the user to use the service, and charging according to the user service consumption information reported by the content control gateway, by the Policy Server.

2. The method according to claim 1, wherein the method further comprises:

   sending, by the Portal Server, a service deactivation request to the Policy Server, when a request for stopping the service from the user is received; and
   responding to the service deactivation request, delivering a service policy cancellation message, performing rating and accounting according to the consumption information, by the Policy Server.

3. The method according to claim 1 or 2, wherein the method further comprises:

   reporting, by the content control gateway, the user service consumption information to the Policy Server periodically during the use of the service;
   rating according to the user service consumption information, and accounting on the service consumption of the user according to each rating information after the user stops using the service, by the Policy Server.

4. The method according to claim 1, wherein the method further comprises:

   after responding to the service activation request, querying a preset correlation table between the service and the service policy according to the service activation request, determining the service policy corresponding to the service, extracting the parameters needed for executing the service policy, filling the parameters in the service policy activation message and delivering the service policy activation message to the content control gateway by the Policy Server.

5. The method according to claim 1, 2 or 4, wherein: the service policy activation message comprises the information of the source IP address, destination IP address, destination port, destination service resource and traffic flow information of the network packet.

6. The method according to claim 5, wherein the method further comprises:

   granting the source IP address of the user network packet a right to access the destination IP address, destination port and destination service resource, and controlling the network flow according to the traffic flow information in the service policy message, by the content control gateway.

7. The method according to claim 1, wherein the method further comprises:

   obtaining the content data flows according to the Content Server or the service port of the content, controlling the content data flow and collecting the consumption information, by the content control gateway.

8. A system for content charging, comprising a Portal Server and a Content Server, wherein the system further comprises a Policy Server and a content control gateway, the Policy Server is connected with the Portal Server and the content control gateway and is adapted to deliver a service policy activation message and a service policy cancellation message, perform rating and charging according to user service consumption information reported by the content control gateway;
   the content control gateway is connected with the Content Server and is adapted to control access to the Content Server of the user according to the access right, count the service consumption information and report the user service consumption information to the Policy Server for charging.

9. The system according to claim 8, wherein the Policy Server comprises a central control module, a charging engine module, a portal interface module and a device interface module, wherein:

   the central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to respond to a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver a

service policy activation message via the device interface module, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating;
the portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request;
the device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module;
the charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

10. The system according to claim 8, wherein the content control gateway comprises a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module, wherein:

the central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy;
the flow classification module is adapted to check, classify, control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and permit a network flow that conforms to the policy to pass;
the content filtration module is adapted to check, classify, control resources to be accessed by the network packet on the application layer, and permit the network flow that conforms to the policy to pass;
the charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module;
the interface module is adapted to provide an interface between the central control module and the Policy Server.

11. A Policy Server, for realizing the charging method according to claim 1, wherein the Policy Server comprises a central control module, a charging engine module, a portal interface module and a device interface module, wherein:

the central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to receive a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver the service policy activation message via the device interface, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating;
the portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request;
the device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module;
the charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

12. The server according to claim 11, wherein the server further comprises a database interface and a memory database, through the database interface, an external database and the memory database is accessed; the memory database is adapted to store policy data, charging data, configuration data and user session data, and receive an instruction from the central control module for updating the data.

13. A content control gateway, for implementing the charging method according to claim 1, comprising a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module, wherein:

the central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy;
the flow classification module is adapted to check, classify and control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and only permit a network flow that conforms to the policy to pass;
the content filtration module is adapted to check, classify and control resources to be accessed by the network packet on the application layer, and only permit the network flow that conforms to the policy to pass;

the charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module;
the interface module is adapted to provide an interface between the central control module and the Policy Server.

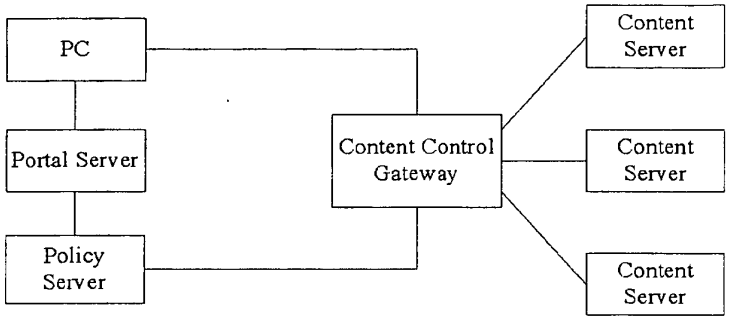

PC
Portal Server
Policy Server
Content Control Gateway
Content Server
Content Server
Content Server

Fig.1

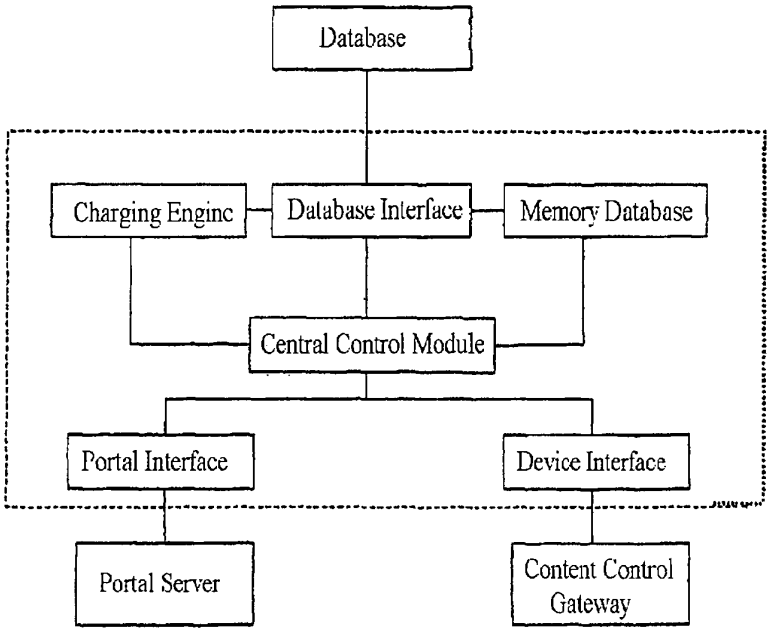

Database
Charging Enginc
Database Interface
Memory Database
Central Control Module
Portal Interface
Device Interface
Portal Server
Content Control Gateway

Fig.2

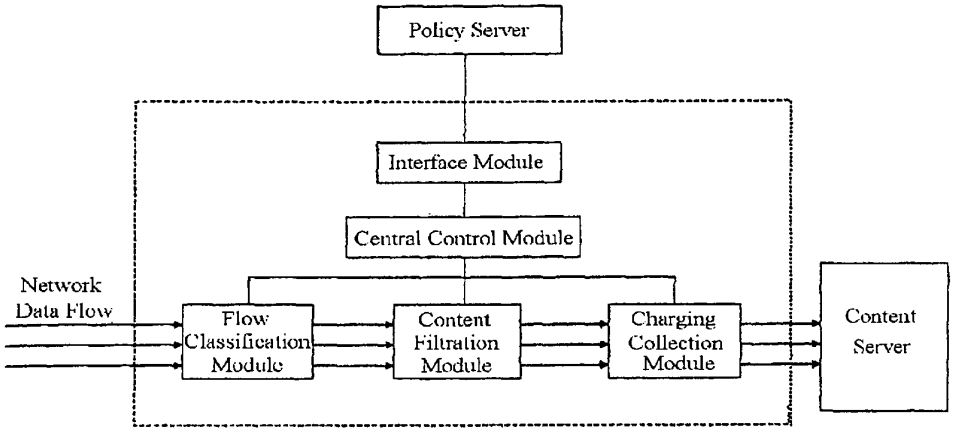

Policy Server
Interface Module
Central Control Module
Network
Data Flow
Flow
Classification
Module
Content
Filtration
Module
Charging
Collection
Module
Content
Server

Fig.3

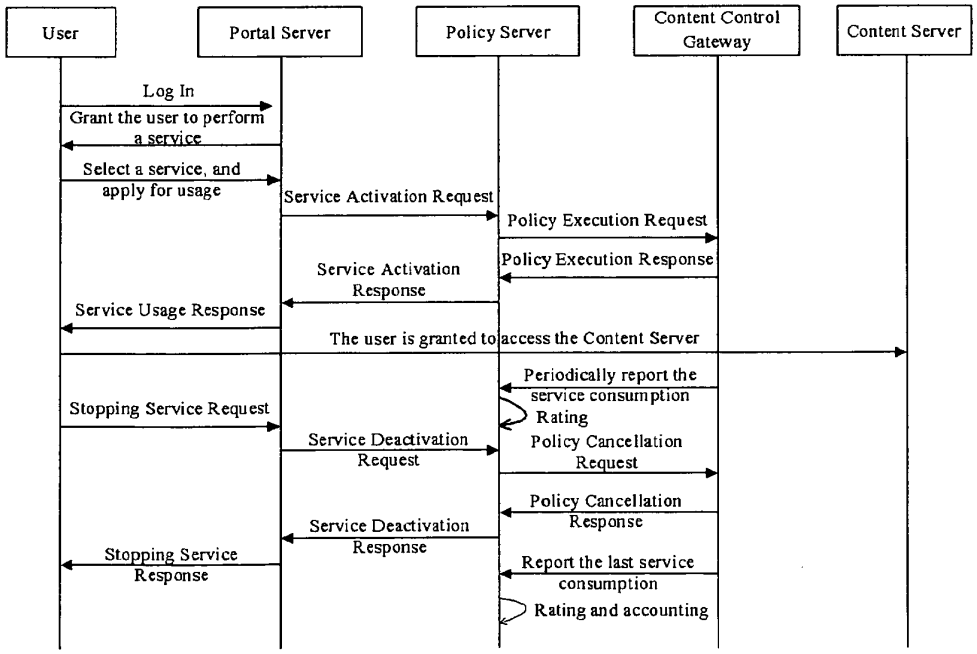

User
Portal Server
Policy Server
Content Control
Gateway
Content Server
Log In
Grant the user to perform
a service
Select a service, and
apply for usage
Service Activation Request
Policy Execution Request
Policy Execution Response
Service Activation
Response
Service Usage Response
The user is granted to access the Content Server
Periodically report the
service consumption
Rating
Stopping Service Request
Service Deactivation
Request
Policy Cancellation
Request
Policy Cancellation
Response
Service Deactivation
Response
Stopping Service
Response
Report the last service
consumption
Rating and accounting

Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/001156

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/14 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L (2006.01), G07F (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, PAJ: bill+, charg+, account, content, policy, strategy, request, gateway, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, A1, 0159990 (FUTURE TECH INC) 16.AUG. 2001 (16.08.2001), the whole document.	1-13
A	EP, A1, 1400934 (OPENWAVE SYSTEMS INC) 24.MAR. 2004 (24.03.2004), the whole document.	1-13
A	CN, A, 1556634 (ZHONGXING COMMUNICATION CO LTD SHENZHEN) 22.DEC. 2004 (22.12.2004), the whole document.	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance.

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29. AUG. 2006 (29. 08. 2006)	21 · SEP 2006 (21 · 09 · 2006)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer WANG,Hongli Telephone No. (86-10) 62084525

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/001156

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO0159990A1	16.08.2001	JP2003523031T	29.07.2003
		KR2000024368 A	06.05.2000
		AU200136124 A	20.08.2001
		KR331219 B	06.04.2002
		US2003023550 A1	30.01.2003
		CN1397125 A	12.02.2003
EP1400934A1	24.03.2004	NONE	
CN1556634A	22.12.2004	NONE	

Form PCT/ISA /210 (patent family annex) (April 2005)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 007 065 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 153(4) EPC

(43) Date of publication:
24.12.2008 Bulletin 2008/52

(21) Application number: **07720622.5**

(22) Date of filing: **30.03.2007**

(51) Int Cl.:
H04L 12/14 *(2006.01)*

(86) International application number:
PCT/CN2007/001048

(87) International publication number:
WO 2007/112685 (11.10.2007 Gazette 2007/41)

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

(30) Priority: **31.03.2006 CN 200610067080**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District, Shenzhen
Guangdong 518129 (CN)

(72) Inventors:
- **WU, Yajuan**
  Shenzhen Guangdong 518129 (CN)
- **LUO, Long**
  Shenzhen Guangdong 518129 (CN)

(74) Representative: **Haley, Stephen**
Gill Jennings & Every LLP
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) CHARGING ASSOCIATING METHOD, SYSTEM, CHARGING CENTER, AND DEVICE FOR APPLICATION SERVICE

(57) A method for charging correlation for an application or service is provided. The method may include: receiving a service identifier assigned for an application or service; and correlating Charging Data Records CDRs generated for the application or service based on the service identifier. A system for charging correlation, a billing center and an apparatus for charging correlation are also provided. These method and apparatus may provide a simple charging correlation process for an application or service.

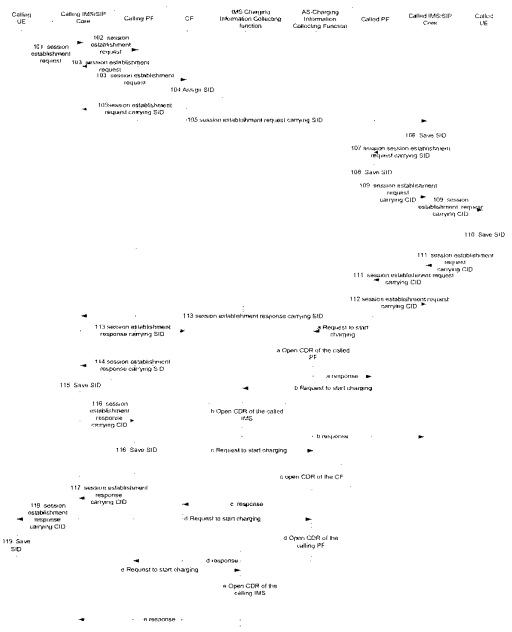


Fig. 1

EP 2 007 065 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to applications and services, and particularly, to a method and system for charging correlation of applications and services, a billing center and an apparatus for generating charging data record.

Background of the Invention

[0002] At present, communication systems have provided applications and services for individual user and/or group users, and communication media employed in these applications and services may include text, audio, video, and varieties combinations of multimedia. A general application or service is mainly oriented to individuals, and there usually is only one or two User Equipments (UEs) communicating with an Application Server or with each other. However, in an application or service in which group users take part, users of one or more groups usually communicate with other users at the same time. In other words, this kind of communication is not a two-party communication including one calling user and one called user, but a communication including a plurality of calling users and a plurality of called users. Such an application or service in which group users take part is also called a multi-party service.

[0003] In a session-based service, a Charging Identifier (CID) is allocated each time when an Application Server (AS) establishes a session with a UE, and all CIDs allocated are saved in the AS and a service bearer network. A billing center retrieves Charging Data Records (CDRs) corresponding to the CIDs from the service bearer network and the AS via a charging function collecting entity, and combines CDRs that correspond to the same CID in order to perform a charging. For applications and services employing an IP Multi-media Subsystem (IMS) as a service bearer network, the CIDs allocated are also called IMS Charging Identifiers (ICIDs). However, the applicant finds out that the CID-based charging method described above has some disadvantages in practical applications and services.

[0004] For example, in a service communication, when a UE establishes a session with an AS for a first time, the UE is given a CID. For some reasons, the UE may exit the service communication temporarily before the service communication is end. Later, the UE re-enters the service communication. In such a case the UE is given a new CID for a session established after re-entering the service communication. From a perspective of a user using the UE, the two sessions, established for the first entering and established for the re-entering, respectively, are two related sessions, and need to be combined for a charging. However, from a perspective of the billing center, the two sessions correspond to different CIDs, thus the two sessions are considered as unrelated sessions. If the two sessions need to be correlated, the billing center needs to analyze CDRs of the two sessions and perform complicated calculation based on user information recorded in the CDRs, yet it is still difficult to guarantee an accurate correlation of the two sessions. Such problem becomes more apparent in multi-party services.

[0005] In a multi-party service, UEs used by users of various parties of this service access a center control server via respective access servers. The center control server provides centralized session handling, which includes session signaling controls, media transmission authorization to communication parties, media data duplication and distribution, etc. One multi-party service has one center control server and at least one access server. The center control server performs controlling function (CF) and the access server performs participating function (PF). Logically, a CF corresponds to a multi-party service. In a multi-party service, the CF establishes one session for each UE, and the sessions of each UE correspond to a PF. Therefore, the center control server is looked as a CF while the access server is looked as at least one PF corresponding to at least one UE connected to the access server.

[0006] Therefore, multi-party services have a common feature that, a multi-party service has at least one session and each session corresponds to a UE of one user and corresponds to its CID. Due to such feature of multi-party services, the billing center needs to correlate a great number of CIDs when performing charging, which leads to poor charging accuracy and difficult implementation. Moreover, for a multi-party service, there is also a need to charge a user by correlating a plurality of sessions of the user in one multi-party service. However, according to the charging technique in the prior art, the billing center needs to generate CDRs based on ICIDs first and make further calculations based on group information in the CDRs, which is still complicated and tends to be inaccurate.

[0007] As discussed above, CID-based charging method in the prior art cannot correlate different sessions of a user in one service communication, but only can correlate actions of the user in one session. Such charging method may easily result in a repeated charging for one action and may omit an action which needs to be charged, thereby threatening security and reliability of charging operations and reducing user satisfaction.

[0008] Furthermore, as new demands emerge, it is becoming more and more difficult to use a single AS to handle a plurality of applications or services. In order to provide more flexible and richer services, operators or service providers are developing multi-services which includes a plurality of sub-services. For a perspective of a multi-service, the above application or service provided by the AS can be called single-service. In a multi-service, each sub-service has a sub-service server e.g. an AS, and an entire multi-service also has a service control function adapted to perform a centralized control of all the sub-service servers. For example, the service control

function controls initiation procedures of the respective sub-services and controls assignment of session identifiers of the respective sub-services, etc. A current typical multi-service has a structure that one of the sub-services is considered as the primary service, and all other sub-services of the multi-service are considered as supplementary services. The sub-service server serves the primary service can be called a primary service server and the sub-service servers serve the supplementary services can be called supplementary service servers. The implementation of the supplementary services depends on the implementation of the primary service in certain degree and provides supplementary functions for the implementation of the primary service. For example, a Presence Server may be configured in a PoC service network and be used to display group status to users during a PoC service session. For another example, a Location Service Server (LCS Server) may also be used in a PoC service network to provide location information of participating users.

[0009] As the development of multi-services, operators or service providers may develop correlating charging policies for multi-services. However, as discussed above, the conventional charging method is based on CIDs corresponding to separate sessions. Therefore the billing center needs to correlate CDRs of a plurality of services in a multi-service charging to perform a charging. Because a CID corresponds to only one session of a sub-service of a user, the billing center needs to analyze each CDR and performs comprehensive calculation by using complicated processes, thereby resulting in low charging accuracy and low feasibility.

[0010] Therefore, the conventional CID-based charging method is only applicable to correlate a plurality of actions of a user in one session, but is not applicable to correlate a plurality of sessions of a user in a single-service and says nothing of correlating a plurality of sessions of a user in a plurality of sub-services of a multi-service.

Summary of the Invention

[0011] Embodiments of a method and a system for charging correlation, a billing center and an apparatus for generating charging data record for implementing a charging correlation for an application or service are provided, which enables a charging correlation process to be easily performed and to greatly improve charging accuracy.

[0012] A method for charging correlation for an application or service may include:

assigning a service identifier by a service control function to an application or service;
sending the service identifier to a charging system; and
correlating, by the charging system, at least one Charging Data Record CDR generated for the application or service based on the service identifier.

[0013] A system for charging correlation for an application or service may include:

a service control function, adapted to assign a service identifier for an application or service; and
a charging system, adapted to correlate Data Records CDRs generated for the application or service based on the service identifier.

[0014] A billing center may include:

a first module, adapted to receive a service identifier assigned to an application or service and CDRs generated for the application or service; and
a second module, adapted to correlate the CDRs based on the service identifier from the first module.

[0015] An apparatus for generating charging data record may include:

a first module, adapted to receive a service identifier assigned to an application or service; and
a second module, adapted to generate Charging Data Records CDRs carrying the service identifier from the first module for the application or service.

[0016] The method for charging correlation, the system for charging correlation, the billing center and the apparatus for generating charging data record for implementing a charging correlation for an application or service provided in accordance with embodiments of the present invention are able to correlate a plurality of CDRs generated during an application or service, thereby implementing a correlated charging of a plurality of users participating in the application or service in a simple way. A plurality of CDRs generated for one user in the application or service may be correlated and the user can be accurately charged. Furthermore, correlated charging for multi-services can also be implemented. The technical solution provided in embodiments of the present invention is easy to be implemented and does not need to make many modifications to the existing networks, and therefore is highly feasible.

Brief description of the drawings

[0017]

Figure 1 is a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention.
Figure 2 is a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention.
Figure 3 is a flowchart of a charging correlation process in a session modification in accordance with an embodiment of the present invention.
Figure 4 is a flowchart of a charging correlation proc-

ess when a new user is added in accordance with an embodiment of the present invention.

Figure 5 is a flowchart of a charging correlation process of an on-demand session in accordance with an embodiment of the present invention.

Figure 6 is a flowchart of a charging correlation process of a pre-established session in accordance with an embodiment of the present invention.

Figure 7 is a flowchart of a charging correlation process when a user who established an on-demand session re-enters the session in accordance with an embodiment of the present invention.

Figure 8 is a flowchart of a charging correlation process when a user who established a pre-established session re-enters the session in accordance with an embodiment of the present invention.

Figure 9 is a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention.

Figure 10 is a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention.

Figure 11 is a structure diagram of a system for implementing a charging correlation of an application or service in accordance with an embodiment of the present invention.

Detailed Description of the Embodiments

[0018] This invention will hereinafter be described in detail with reference to accompanying drawings and embodiments.

[0019] A charging method for an application or service according to an embodiment of the present invention may include: assigning a service identifier to an application or service session, sending the service identifier to a charging system, and correlating, by the charging system, the CDRs generated in this service based on the service identifier. The charging method is described in detail in the following embodiments.

[0020] The charging system may include a charging information collecting function used to receive CDRs from ASs and bearer control layer entities, a charging gateway, and a billing center used to correlate the CDRs and perform other operations for charging. The charging information collecting function functions as an interface of the charging system, receives CDRs from network nodes e.g., ASs or bearer control layer entities connected to the charging information collecting function, and sends the CDRs to the billing center via the charging gateway. ASs and the bearer control layer entities have respective charging information collecting functions. A charging information collecting function corresponding to ASs is usually called an AS-charging information collecting function and a charging information collecting function corresponding to bearer control layer entities is usually called a bearer control layer-charging information collecting function. For bearer control layer in an IMS network, the bearer control layer-charging information collecting function is also called an IMS charging information collecting function. Embodiments of the present invention mainly concerns about transmission of service identifiers among ASs, bearer control layer entities and charging information collecting functions, therefore the figures and illustrations of the embodiments of the present invention omit the processes that the charging information collecting functions send CDRs and service identifiers to the billing center. In the figures and illustrations of the embodiments of the present invention, the AS-charging information collecting function entities and IMS charging information collecting function entities are referred to as AS-charging information collecting functions and IMS charging information collecting functions.

[0021] A first charging correlation scheme given in an embodiment of the present invention implements charging with a plurality of CDRs generated for one user in a single-service. In this embodiment, a service control function, e.g. an AS of a single-service session, assigns a uniform service identifier for the single-service, generates CDRs of participating users and sends the service identifier and the CDRs to a charging system. The charging system correlates the CDRs of a user in this single-service session.

[0022] In practical applications, a user may establish one or a plurality of sessions in one service and a CDR corresponds to one session of the user. Different ways may be adapted to correlate CDRs based on the service identifier. The CDRs to be correlated may be CDRs corresponding to a plurality of sessions established for one user in one service, or may be CDRs corresponding to a plurality of sessions established for a part of users or all users in one service. The specific way of correlating CDRs is chosen in accordance with an applied correlation policy and will not be described further herein.

[0023] The AS sends the service identifier and the CDRs to a charging information collecting function of a charging system. The charging information collecting function sends the CDRs collected and the service identifier to a billing center which performs charging correlation operations. When this charging correlation scheme is applied to application service layer, the charging information collecting function includes an AS-charging information collecting function corresponding to the service control function entity. The charging correlation scheme may also be applied to bearer control layer, and in such a case the charging information collecting function includes a bearer control layer-charging information collecting function corresponding to a bearer control layer entity that the service control function entity corresponds to, wherein the bearer control layer entity that the service control function corresponds to is used to bear the service control function. At this time, the bearer control layer entity corresponding to the service control function records the service identifier and generates CDRs for the current application or service, and sends the service identifier and the CDRs to the bearer control layer-charging infor-

mation collecting function of the bearer control layer entity. The AS-charging information collecting function and the bearer control layer-charging information collecting function respectively send the CDRs and service identifiers to the billing center. The billing center correlates the CDRs received from the AS-charging information collecting function and correlates the CDRs received from the bearer control layer-charging information collecting function, respectively. Or the billing center may correlates the CDRs received from the AS-charging information collecting function with the CDRs received from the bearer control layer-charging information collecting function. This charging correlation scheme in an embodiment of the present invention may be applied to both the application service layer and the bearer control layer in the embodiments shown in Figures 1 to 8. When the charging correlation scheme is applied only to the application service layer, the charging correlation process involves UE, AS, AS-charging information collecting function and billing center, without involving the bearer control layer entity and the bearer control layer-charging information collecting function. The charging correlation process in which the charging correlation scheme is applied only to the application service layer will not be described in detail herein, yet such process is still covered by the protection scope of the present invention.

[0024] The embodiments of the present invention are mainly oriented to session-based applications or services such as multi-party services. In conventional session-based services, session IDs (SIDs) corresponding to different service sessions are already employed. The existing SIDs may be used as service identifiers to correlate a plurality of CDRs. Also new identifiers may be defined as the service identifiers. Usually information exchanged among entities on the application service layer is sent via corresponding bearer control layer entities. For example, servers that perform PF of the multi-party service, a server performing CF, and UEs are used to exchange information via corresponding bearer control layer entities such as an IMS/SIP Core network (IMS/SIP Core). At the same time, network functions in the IMS/SIP Core may also generate CDRs for the current application or service in order to implement a charging process on the bearer control layer. In such process the AS of each application or service corresponds to a bearer control layer entity that is adapted to bear the AS.

[0025] At present, the mainstream multi-party services include Push-to-Talk over Cellular network (PoC) service, Conference service, etc. In a PoC service session, a server performing CF is a PoC server that performs CF, also called Controlling PoC Server; and the server performing PF is the PoC server that performs PF, also called Participating PoC Server. In a Conference service session, the server that performs CF is the Conference server that performs CF, also called a Controlling Conference Server; and the server performing PF is the Conference server that performs PF, also called a Participating Conference Server. The server performing PF and the server performing CF are logical functions of multi-party service servers, and the server performing PF and the server performing CF may be physically located in different ASs or in one AS. The server performing CF is referred to as the CF and the server performing PF is referred to as PF herein for the sake of simplicity. The embodiments of the present invention are described in detail herein taken a SIP based multi-party service as an example.

[0026] Figure 1 shows a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention. The entities involved in this embodiment include a calling UE and a calling PF of the calling UE, a calling IMS/SIP Core corresponding to the calling PF and the calling UE, a CF of a present multi-party service, a called UE and a called PF of the called UE, a called IMS/SIP Core corresponding to the called PF and the called UE. The entities involved in this embodiment also include an AS-charging information collecting function corresponding to the calling PF, CF, and the called PF, and an IMS charging information collecting function corresponding to the calling IMS/SIP Core and the called IMS/SIP Core. The calling UE, the calling PF and the CF correspond to a same bearer control layer entity i.e., the calling IMS/SIP Core, the called UE and the called PF correspond to a same bearer control layer entity i.e., the called IMS/SIP Core. The service control function of the current application or service performs CF of the multi-party service.

[0027] When the calling/called PF and CF are provided by servers in a network of one service provider, the calling/called PF and the CF may correspond to a same AS-charging information collecting function. In this embodiment, suppose that the calling/called PF and the CF correspond to a same AS-charging information collecting function. However, when the calling/called PF and the CF are provided by servers in different networks of different service providers, the calling/called PF and the CF may correspond to different AS-charging information collecting functions respectively, and accordingly, the calling/called PF and the CF send service identifiers and the CDRs to different AS-charging information collecting functions respectively. Similarly, when IMS/SIP Cores of the calling UE and the called UE are provided in a same network of a same operator, the calling/called IMS/SIP Cores may correspond to one IMS charging information collecting function. When the IMS/SIP Cores of the calling UE and the called UE are in different networks provided by different operators, the calling/called IMS/SIP Cores may correspond to different IMS charging information collecting functions and send service identifiers and the CDRs to different IMS charging information collecting functions respectively. In this embodiment, suppose that the calling/called IMS/SIP Cores correspond to one IMS charging information collecting function.

[0028] As shown in Figure 1, the process includes as follows.

[0029] 101-102: The calling UE sends a session es-

tablishment request to the calling PF via a corresponding calling IMS/SIP Core. The session establishment request may be carried in an SIP INVITE message in this embodiment; however, the present invention is not limited to this.

[0030] The application service layer entities such as the UE, PF, CF, etc., and the corresponding bearer control layer entities such as the IMS/SIP Core, etc., may be in a same network or in different networks. The present invention is not limited to this.

[0031] 103: The calling PF sends the session establishment request to the CF via the calling IMS/SIP Core.

[0032] 104: The CF assigns a service identifier (SID) for the current multi-party service session and the followings shall be performed once for each of the called UEs.

[0033] 105: The CF sends the session establishment request to the called IMS/SIP Core corresponding to the called PF via the calling IMS/SIP Core of the CF. The session establishment request carries the SID assigned in 104.

[0034] 106-107: The called IMS/SIP Core saves the received SID and sends the session establishment request carrying the SID to the called PF.

[0035] 108-109: The called PF saves the received SID and sends the session establishment request carrying the SID to the called UE via the called IMS/SIP Core.

[0036] 110-111: The called UE saves the received SID and returns a session establishment response carrying the SID to the called PF via the called IMS/SIP Core. The session establishment response is carried in an SIP 2000K message in this embodiment, however, the present invention does not limit to this.

[0037] 112-113: The called PF sends the session establishment response carrying the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0038] 114: The CF returns the session establishment response carrying the SID to the calling IMS/SIP Core.

[0039] 115-116: The calling IMS/SIP Core saves the received SID and returns the session establishment response carrying the SID to the calling PF, the calling PF also saves the received SID.

[0040] 117-119: The calling PF returns the session establishment response carrying the SID to the calling UE via the calling IMS/SIP Core, and the calling UE saves the received SID. By now, a session establishment process is completed.

[0041] In this embodiment, after receiving the SID, the service layer entities and bearer control layer entities related to the charging correlation process may insert the SID into or with the CDRs generated for the current application or service and send the CDRs to the corresponding charging information collecting functions. Specifically, the application service layer entities and bearer control layer entities generate CDRs after receiving a session establishment response indicating a successful session set-up or after sending the session establishment request, and the SID is included in the CDRs and the CDRs are sent to the charging information collecting functions. This embodiment describes a process in which the session is successfully established; hence it is supposed that the session establishment response always indicates a successful session set-up. In Figure 1, the application service layer entities related to the charging correlation process include a calling PF, a called PF and a CF; the bearer control layer entities related to the charging correlation process include a calling IMS/SIP Core and a called IMS/SIP Core. The procedure of sending the SID and the CDRs by the application service layer entities and bearer control layer entities related to the charging correlation process includes the followings.

[0042] The called PF may perform step ***a*** after sending the session establishment request in 109 or after receiving the session establishment response in 111. Step ***a*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing ***a*** and the steps following 111. Step ***a*** may include followings. The called PF requests the AS-charging information collecting function to start charging and sends the CDR of the called UE carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called PF during a current multi-party service.

[0043] The called IMS/SIP Core may save the SID when sending the session establishment request or when sending session establishment response that carries the SID. The called IMS/SIP Core may further perform step ***b*** after receiving the session establishment response in 112. Step ***b*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***b*** and the steps following 112. Step ***b*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start charging, and sends the CDR of the called UE carrying the SID to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called IMS/SIP Core during the current multi-party service.

[0044] The CF may perform step c after receiving the session establishment response in 113. Step c is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***c*** and the steps following 113. Step c may include followings. The CF requests the AS-charging information collecting function to start charging and sends CDRs of the calling and called UEs carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDRs and starts to record actions performed by the calling and called UE with the CF during the current multi-party service.

[0045] The calling PF may perform step ***d*** after receiving the session establishment response in 116. Step ***d*** is independent of other following steps and this embodiment of the present invention does not limit the sequence

order of performing step ***d*** and the steps following 116. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start charging and sends the CDR of the calling UE carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling PF during the current multi-party service.

[0046] The calling IMS/SIP Core may save the SID after sending the session establishment response that carries the SID. The calling IMS/SIP Core may further perform step ***e*** after receiving the session establishment response in 117. Step ***e*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***e*** and the steps following 117. Step ***e*** may include followings. The calling IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the calling UE that carries the SID to the IMS charging information collecting function. the IMS charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling IMS/SIP Core during the current multi-party service.

[0047] When the calling UE and the called UE establish a session and start a multi-party service communication, the AS-charging information collecting function or the IMS charging information collecting function starts to record the actions of the calling and called UEs that are performed on the entities during the multi-party service in real-time.

[0048] In the embodiment shown in Figure 1, the calling and the called PFs send the received SID to the calling and the called UEs, respectively. As such, when it needs to modify the session, or to add a new user into a session, or to make a user re-enter into a session, or to make a user exit the session, it is possible for the UEs to send the SID to a server performing PF or a server performing CF, in order to generate partial CDRs corresponding to the SID, or to generate a new CDR corresponding to the SID, or to update the CDR corresponding to the SID, or to close the CDR corresponding to the SID, respectively. However, sending the SID to the calling and the called UEs is not essential. Only when the above factors are taking into consideration, it is necessary to send the SID to the calling and the called UEs. In Figure 1, the calling and called UEs do not negotiate media parameters before establishing a session i.e., the calling and the called UEs establish an on-demand session. When the calling and called UEs negotiate media parameters before establishing a session i.e., the calling and the called UEs establish a pre-established session, the charging correlation process will be different from the process shown in Figure 1, as shown in Figure 2.

[0049] Figure 2 shows a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention. In this embodiment, media parameters have been negotiated between the calling UEs and the calling PF that servers the calling UEs before establishing a session, and media parameters have been negotiated also between the called UEs and the called PF that servers the called UEs. The entities involved in the process are the same as the entities in Figure 1. A brief description of the pre-established session is given as follows. Before establishing a session, the UE negotiates session parameters with the server performing PF for the UE. The UE initiates a session establishment process by a session modify request such as a parameter message (REFER message). Therefore in the session establishment process, session parameters negotiation may be omitted and the UE does not need to upload session parameters. The UE just needs to indicate the server performing PF which service is to be joined by the UE. As such, SIP signaling that is exchanged with the UE has fewer bits, and air interface resources may be saved. The server performing PF then initiates a normal session establishment process with the server performing CF according to the indication from the UE, and informs the UE of a successful set-up by sending a media data control protocol message to the UE after the session between the PF and the CF is established. The media data control protocol may be the Talk Burst Control Protocol (TBCP) or the Media Burst Control Protocol (MBCP).

[0050] Figure 2 mainly includes followings.

[0051] 201-202: The calling UE sends a session modify request to the calling PF via the calling IMS/SIP Core corresponding to the calling UE. The calling PF returns a session modify response to the calling UE. The session modify request may be carried in an SIP parameter message (SIP REFER message) and the session modify response may be carried in an SIP accepted message (SIP ACCEPTED message), however, the present invention is not limited to this.

[0052] 203: The calling PF sends a session establishment request to the CF via the calling IMS/SIP Core corresponding to the calling PF.

[0053] 204: The CF assigns a service identifier SID for a current multi-party service and the followings is performed once for each of the called UEs.

[0054] 205: The CF sends the session establishment request to the called IMS/SIP Core via the calling IMS/SIP Core. The session establishment request carries the SID assigned in 204.

[0055] 206-207: The called IMS/SIP Core saves the received SID and sends the session establishment request that carries the SID to the called PF.

[0056] 208-210: The called PF saves the received SID and returns a session establishment response carrying the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0057] While returning the session establishment response to the CF, the called PF also performs 210'. 210' may include followings. The called PF sends to the called IMS/SIP Core a media data control protocol message

carrying the SID, such as a TBCP Connect message used to notify the called UE to join the current service. The called UE saves the SID and returns an acknowledgment e.g. a TBCP Talk Burst Acknowledge message to the called PF via the called IMS/SIP Core. The called PF sends a confirmation e.g. a TBCP Talk Burst Confirm message to the called UE and then media data streams may be transmitted to the called UE.

[0058] In this embodiment, suppose that the called UE has negotiated parameters with the called PF and an auto-answer mode Has been set. That is, the called PF may send the media data control protocol message to the called UE, and return a session establishment response to the CF, without requesting the called UE in advance. The media data control protocol message, such as a TBCP Connect message or a Talk Burst Confirm message that is sent to the called UE, carries the SID. In another example, the called UE may also be configured to a manual response mode. That is, the called PF first sends a session establishment request e.g. an INVITE message to the called UE and then sends the media data control protocol message to the called UE. The called PF sends a session establishment response to the CF after the called user agrees to join the current service. In such a case, the media data control protocol message such as a TBCP Connect message or Talk Burst Confirm message, or the session establishment request such as an INVITE message that is sent to the called UE, may carry the SID.

[0059] 211-214: The CF returns a session establishment response carrying the SID to the calling IMS/SIP Core. The calling IMS/SIP Core saves the received SID and returns a session establishment response carrying the SID to the calling PF. The calling PF also saves the received SID.

[0060] 215-217: The calling PF sends a media data control protocol message, such as a TBCP Connect message, to the calling UE via the calling IMS/SIP Core to inform the calling UE that it is ready for a service session setup. The calling UE returns an acknowledgment, such as a TBCP Talk Burst Acknowledge message, to the calling PF via the calling IMS/SIP Core. The calling PF sends a confirmation such as a TBCP Talk Burst Confirm message to the called UE and is ready to receive media data streams from the calling UE. After that, the calling PF sends a session setup notification such as a NOTIFY message carrying the SID to the calling UE via the calling IMS/SIP Core. The calling UE saves the received SID and a whole session establishment process is completed.

[0061] In this process, the calling PF sends the SID to the calling UE by carrying the SID in a session setup notification or in a media data control protocol message such as a TBCP Connect message or a Talk Burst Confirm message.

[0062] The procedure of sending the SID and the CDRs received from the application service layer entities and bearer control layer entities that are related to the charging correlation process may include the followings.

[0063] The called IMS/SIP Core may save the SID after sending the session establishment request that carries the SID, the media data control protocol message that carries the SID, or the session establishment response that carries the SID. The called IMS/SIP Core may perform Step ***a*** after receiving the session establishment response, e.g., the response to the session establishment request or the response to the media data control protocol message, from the called UE. Step ***a*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***a*** and other steps. Step ***a*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start charging, and sends the CDR of the called UE to the IMS charging information collecting function, wherein the CDR of the called UE carries the SID. The IMS charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called IMS/SIP Core during the current multi-party service.

[0064] The called PF may perform step ***b*** after sending the session establishment request or media data control protocol message to the called UE, or after receiving the session establishment response e.g., a response to the session establishment request or a response to the media data control protocol message from the called UE. Step ***b*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***b*** and other steps. Step ***b*** may include followings. The called PF requests the AS-charging information collecting function to start charging and sends the CDR of the called UE that carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called PF during the current multi-party service.

[0065] The CF may perform step c after receiving the session establishment response in 210. Step c is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step c and the steps following 210. Step c may include followings. The CF requests the AS-charging information collecting function to start charging and sends CDRs of the calling and called UEs that carry the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDRs and starts to record actions performed by the calling and called UE with the CF during the current multi-party service.

[0066] The calling PF may perform step ***d*** after receiving the session establishment response in 213. Step ***d*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***d*** and the steps following 213. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start

charging and sends the CDR of the calling UE that carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling PF during the current multi-party service.

[0067] The calling IMS/SIP Core may save the SID after sending the session establishment response carrying the SID. The calling IMS/SIP Core may further perform step e after receiving the session establishment response in 211. Step e is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step e and the steps following 211. Step e may include followings. The calling IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the calling UE that carries the SID to the IMS charging information collecting function. the IMS charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling IMS/SIP Core during the current multi-party service.

[0068] During a multi-party service, a UE may modify the session, for example, the UE may modify the session media parameters, which may result that the AS-charging information collecting function or IMS charging information collecting function may generate a partial CDR. The partial CDR and original CDRs belong to the same multi-party service and need to be correlated in the charging correlation process. Therefore, in a session modification process, the UE needs to send the SID saved during the session establishment process to entities such as the server performing PF and the server performing CF which are related to the charging correlation process, so that the entities can generate partial CDRs corresponding to the SID. In this way the partial CDR may be correlated with other CDRs generated for the multi-party service.

[0069] Figure 3 shows a flowchart of a charging correlation process in a session modification process in accordance with an embodiment of the present invention. The entities involved in this embodiment may include: a calling UE and a calling PF of the calling UE, a calling IMS/SIP Core corresponding to the calling PF and the calling UE, a CF of a current multi-party service, a called UE and a called PF of the called UE, and a called IMS/SIP Core corresponding to the called PF and the called UE. This embodiment also involves: a AS-charging information collecting function corresponding to the calling PF, the called PF and the CF, and an IMS charging information collecting function corresponding to the calling IMS/SIP Core and the called IMS/SIP Core. Figure 3 includes the following processes.

[0070] 301: The calling UE sends a session modify request that carries the SID to the calling PF via the calling IMS/SIP Core. The session modify request is carried in an SIP UPDATE message or in an SIP Re-INVITE message in this embodiment, however, the present invention is not limited to this.

[0071] 302: The calling PF sends the session modify request that carries the SID to the calling IMS/SIP Core.

[0072] 303: The calling IMS/SIP Core sends the session modify request that carries the SID to the CF, and the followings is performed once for each of the called UEs.

[0073] 304-305: The CF sends the session modify request that carries the SID to the called IMS/SIP Core via the calling IMS/SIP Core.

[0074] 306: The called IMS/SIP Core sends the session modify request that carries the SID to the called PF.

[0075] 307-308: The called PF sends the session modify request that carries the SID to the called UE via the called IMS/SIP Core.

[0076] 309-310: The called UE returns a session modify response that carries the SID to the called PF via the called IMS/SIP Core. The session modify response may be carried in an SIP 2000K message in this embodiment, however, the present invention is not limited to this.

[0077] 311-313: The called PF sends the session modify response that carries the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0078] 314-315: The CF returns the session modify response that carries the SID to the calling IMS/SIP Core, the calling IMS/SIP Core returns the session modify response that carries the SID to the calling PF.

[0079] 316-317: The calling PF returns the session modify response that carries the SID to the calling UE via the calling IMS/SIP Core and the session modify process is completed.

[0080] In the above process, the procedure of sending the SID and the CDRs by the application service layer entities and bearer control layer entities that are related to the charging correlation process includes the followings.

[0081] The called PF may perform step ***a*** after sending the session modify request to the called UE or after receiving the session modify response from the called UE. Step ***a*** is independent from steps following 307 and the present invention does not limit the sequence order of performing step ***a*** and the steps following 307. Step ***a*** may include followings. The called PF requests the AS-charging information collecting function to start an intermediate charging and sends a partial CDR of the called UE, that is generated by the called PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the called PF, saves the partial CDR, and starts to record actions that may affect an accounting and are performed by the called UE on the called PF after the session is modified in the current multi-party service.

[0082] The called IMS/SIP Core may save the SID after sending the session modify request or the session modify request response carrying the SID. The called IMS/SIP Core may further perform step ***b*** after receiving the session modify response from the called UE. Step ***b*** is independent from steps following 309 and the present inven-

tion does not limit the sequence order of performing step ***b*** and the steps following 309. Step ***b*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start an intermediate charging and sends a partial CDR of the called UE, that is generated by the called IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function updates CDR of the called IMS/SIP Core, saves the partial CDR and starts to record actions that may affect an accounting and are performed by the called UE on the called IMS/SIP Core after the session is modified in the current multi-party service.

[0083] The CF may perform step c after receiving the session modify response in 313. Step c is independent from steps following 313 and the present invention does not limit the sequence order of performing step ***c*** and the steps following 313. Step ***c*** may include followings. The CF requests the AS-charging information collecting function to start an intermediate charging and sends the partial CDRs of the calling UEs and the called UEs, that is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the CF, saves the partial CDRs of the calling and the called UEs and starts to record actions that may affect an accounting and are performed by the calling and called UE on the CF after the session is modified in the current multi-party service.

[0084] The calling PF may perform step ***d*** after receiving the session modify response in 315. Step ***d*** is independent from steps following 315 and the present invention does not limit the sequence order of performing step ***d*** and the steps following 315. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start an intermediate charging and sends the partial CDR of the calling UE, which is generated by the calling PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the calling PF, saves the partial CDR of the calling UE and starts to record actions that may affect an accounting and are performed by the calling UE on the calling PF after the session is modified in the current multi-party service.

[0085] The calling IMS/SIP Core may save the SID while sending the session modify response carrying the SID. The calling IMS/SIP Core may further perform step ***e*** after receiving the session modify response in 314. Step e is independent from steps following 314 and the present invention does not limit the sequence order of performing step e and the steps following 314. Step e may include followings, the calling IMS/SIP Core requests the IMS charging information collecting function to start an intermediate charging and sends the partial CDR of the calling user, which is generated by the calling IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function updates CDR of the calling IMS/SIP Core, saves the partial CDR of the calling user and starts to record actions that may affect an accounting and are performed by the calling UE on the calling IMS/SIP Core after the session is modified in the current multi-party service.

[0086] In the embodiments shown in Figures 1 to 3, the calling PF, the CF and the called PF are separated entities. In practical applications, any one or any combination of the calling PF, the CF and the called PF may be provided by one entity, in which case the basic processes are the same as the embodiments shown in Figures 1 to 3, and will not be described in detail herein but are still covered by the protection scope of the present invention.

[0087] In Figures 1 and 2, the calling PF and the CF correspond to a same IMS/SIP Core and the called PF corresponds to another IMS/SIP Core. In practical applications, the calling PF, the CF and the called PF may correspond to different IMS/SIP Cores. When the calling UE and a called UE are in one network provided by an operator, the calling PF and the called PF of the called UE may correspond to the same IMS/SIP Core. When the calling UE and a called UE are in different networks provided by different operators, the calling PF and the called PF correspond to different IMS/SIP Cores. When the calling PF and the CF are in one network provided by the same operator, the calling PF and the CF correspond to the same IMS/SIP Core. When the called PF and the CF are in different networks provided by different operators, the called PF and the CF correspond to different IMS/SIP Cores. However, no matter the calling PF, the CF and the called PF correspond to the same IMS/SIP Core or to different IMS/SIP Cores, the processes in embodiments of the present invention are essentially the same. In one word, the application service layer entities such as the calling PF, the CF and the called PF send/receive session establishment/modify requests or session establishment/modify responses via corresponding IMS/SIP Cores, and the detailed processes thereof will not be described herein, but are still covered by the protection scope of the present invention.

[0088] During an existing multi-party service, when adding a new user, the control function entity (e.g., the CF) of the multi-party service generates a new CDR for a session of the new user. A service identifier will be adapted to correlate the CDRs of the new user when adding the new user.

[0089] Figure 4 shows a flowchart of a charging correlation process when adding a new user to an existing multi-party service in accordance with an embodiment of the present invention. A process of adding a new user includes: requesting by a UE to add another user (a third party user) into a current multi-party service. The third party user is shown as an added UE in Figure 4. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, an added UE, a CF of the current multi-party service, an

AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, suppose that the UE and the new user added to the current service (the added UE) are served by the same PF, and the UE, the added UE, the PF and the CF correspond to the same IMS/SIP Core.

[0090] As shown in Figure 4, the process includes followings.

[0091] 401-402: The UE sends an adding request that carries an SID to the PF via the IMS/SIP Core. The adding request may be carried in an SIP REFER message in this embodiment, however, the present invention is not limited to this.

[0092] 403-404: The PF sends the adding request that carries the SID to the CF via the IMS/SIP Core.

[0093] 405-406: The CF sends the adding request that carries the SID to the PF of the added UE via the IMS/SIP Core, and the PF sends the adding request that carries the SID to the added UE. The added UE returns an adding response that carries the SID to the PF via the IMS/SIP Core after receiving the adding request. The PF returns the adding response that carries the SID to the CF via the IMS/SIP Core. As such, the new UE is added to the current service.

[0094] The adding request may be carried in an SIP INVITE message and the adding response may be carried in an SIP 2000K message, however, the present invention is not limited to this.

[0095] 407: The CF returns the adding response that carries the SID to the PF of the UE via the IMS/SIP Core. The PF informs the UE that the new user has been added to the current service by returning the adding response that carries the SID to the UE via the IMS/SIP Core. The adding response may be carried in an SIP ACCEPTED message in this embodiment; however, the present invention is not limited to this.

[0096] In Figure 4, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the adding response in 406. Step ***a*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***a*** and the follow-up steps. The PF may perform step ***b*** after receiving the adding response in 406 and step ***b*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***b*** and the follow-up steps.

[0097] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to start charging and sends the CDR of the new user (the added UE) that is generated by the CF and carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the new user from the CF and starts to record actions performed by the new user on the CF during the current multi-party service.

[0098] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the new user that is generated by the PF and carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the new user from the PF and starts to record actions performed by the new user on the PF during the current multi-party service.

[0099] The bearer control layer entity related to the charging correlation process in Figure 4 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the adding response in 406, and step c is independent of other following steps and the present invention does not limit the sequence order of performing step c and the follow-up steps. Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the new user that is generated by the IMS/SIP Core and carries the SID to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the new user from the IMS/SIP Core and starts to record actions performed by the new user on the IMS/SIP Core during the current multi-party service.

[0100] In embodiments shown in Figures 3 and 4, the UE may establish an on-demand session or have a pre-established session, the processes in Figures 3 and 4 may be applied to both cases.

[0101] If a UE exits a session, the AS-charging information collecting function and the IMS charging information collecting function need to close the CDRs of the multi-party service of the UE. In such a case, the SID of the current multi-party service needs to be sent to the AS-charging information collecting function and the IMS charging information collecting function so that the CDRs corresponding to the same SID among all CDRs of the UE may be closed based on the same SID.

[0102] Figure 5 shows a flowchart of a charging correlation process when a UE that has established a pre-established session exits a session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core.

[0103] As shown in Figure 5, the process includes followings.

[0104] 501-502: The UE sends a release session request that carries an SID to the PF via the IMS/SIP Core. The release session request is carried in an SIP BYE message in this embodiment, however, the present invention is not limited to this.

[0105] 503: The PF sends the release session request that carries the SID to the CF via the IMS/SIP Core.

[0106] 504: The CF returns a release session response that carries the SID to the PF via the IMS/SIP Core. The release session response may be carried in

an SIP 200OK message in this embodiment, however, the present invention is not limited to this.

[0107] 505-506: The PF sends the release session response that carries the SID to the UE via the IMS/SIP Core.

[0108] In Figure 5, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the release session response in 503. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 503. The PF may perform step ***b*** after receiving the release session response in 504 and step ***b*** is independent of following steps and the present invention does not limit the sequence order of performing step ***b*** and the steps following 504.

[0109] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the CF and stops recording charging data of the UE.

[0110] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the PF and stops recording the charging data of the UE.

[0111] The bearer control layer entity related to the charging correlation process in Figure 5 is the IMS/SIP Core. The IMS/SIP Core may perform step ***c*** after receiving the release session response in 505, and step ***c*** is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 505.

[0112] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to stop charging and sends the SID to the IMS charging information collecting function. The IMS charging information collecting function closes CDR of the UE from the PF.

[0113] The release session process shown in Figure 5 is suitable to be used for a user who establishes an on-demand session. For a user who establishes a pre-established session, a different release session process shall be used. Figure 6 shows a flowchart of a charging correlation process for a user who establishes a pre-established session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core.

[0114] A whole session establishment process for a user who establishes a pre-established session includes two parts: firstly, the UE and the PF negotiate session parameters before establishing a session; then, the PF establishes a session with the CF for the UE when the UE is ready for establishing the session. Therefore this kind of session establishment process shall be ended in two steps: firstly, the session that is pre-established between the UE and the PF is modified; then, the session between the PF and the CF is released. As shown in Figure 6, the process includes followings.

[0115] 601-602: The UE sends a session modify and release request that carries an SID to the PF via the IMS/SIP Core in order to release the session. The session modify and release request may be carried in an SIP REFER BYE message in this embodiment, however, the present invention is not limited to this.

[0116] 603: The PF returns a session modify response to the UE via the IMS/SIP Core. The session modify response may be carried in an SIP ACCEPTED message in this embodiment, however, the present invention is not limited to this.

[0117] 604: The PF sends a release session request carrying the SID to the CF via the IMS/SIP Core. The release session request may be carried in a BYE message, however, the present invention is not limited to this.

[0118] 605: The CF returns a release session response to the PF via the IMS/SIP Core. The release session response may be carried in an SIP 2000K message in this embodiment, however, the present invention is not limited to this.

[0119] 606-607: The PF sends a release session notification to the UE via the IMS/SIP Core to notify the UE of a successful release of the session between the UE and the CF. The UE returns a release session response to the PF. The release session response may be carried in a NOTIFY message, and the release session response may be carried in an OK message, however, the present invention is not limited to this.

[0120] In Figure 6, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the release session request in 604 and after successful releasing the session. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 604. The PF may perform step ***a*** after receiving the release session response in 607.

[0121] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the CF and stops recording the charging data of the UE.

[0122] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the PF and stops recording the charging data of the UE.

[0123] The bearer control layer entity related to the

charging correlation process in Figure 6 is the IMS/SIP Core. The IMS/SIP Core may perform step ***c*** after receiving the release session response in 605, and step ***c*** is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 605.

[0124] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to stop charging and sends the SID to the IMS charging information collecting function. The IMS charging information collecting function closes CDR of the UE from the PF.

[0125] Besides the situations described above, new CDRs may be generated by the entities related to the charging correlation process in two other situation. The charging correlation processes in accordance with the embodiments of the present invention are suitable in such two situations. In the first situation, a user who establishes an on-demand session exits a current multi-party service session temporarily while the current multi-party service proceeds, then the user re-enters the multi-party service. In the other of the two situations, a user who establishes a pre-established session exits a current multi-party service session temporarily while the current multi-party service proceeds, then the user re-enters the multi-party service. The charging correlation processes in the two situations are described with reference to Figures 7 and 8.

[0126] Figure 7 shows a flowchart of a charging correlation process in a case that a user who establishes an on-demand session re-enters a session after the user exits the session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to a same IMS/SIP Core. As shown in Figure 7, the process includes followings.

[0127] 701-702: The UE sends a session joining request carrying an SID to the PF via the IMS/SIP Core. The session joining request may be carried in an SIP REFER message or an SIP INVITE message in this embodiment, however, the present invention is not limited to this.

[0128] 703: The PF sends the session joining request carrying the SID to the CF via the IMS/SIP Core.

[0129] 704: The CF returns a session joining response carrying the SID to the PF via the IMS/SIP Core. The session joining response may be carried in an SIP 2000K message or an SIP ACCEPTED message in this embodiment, however, the present invention is not limited to this.

[0130] 705-706: The PF sends the session joining response carrying the SID to the UE via the IMS/SIP Core.

[0131] In Figure 7, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the session joining response in 703. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 703. The PF may perform step ***b*** after receiving the session joining response in 704 and step ***b*** is independent of following steps and the present invention does not limit the sequence order of performing step ***b*** and the steps following 704.

[0132] Step ***a*** may include followings, the CF requests the AS-charging information collecting function to start charging and sends the CDR of the user who requests to re-enter the session (the UE), which is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the CF and starts to record actions that affect an accounting and are performed by the UE on the CF during the current multi-party service. It need to be noted that when the user re-enters the session, the opened CDR of the UE is a new CDR instead of the CDR of the UE generated before the UE dropped out of the session. However, the two CDRs have the same SID and can be correlated based on the SID.

[0133] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the UE, which is generated by the PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the PF and starts to record actions that affect the accounting and are performed by the UE on the PF during the current multi-party service.

[0134] The bearer control layer entity related to the charging correlation process in Figure 7 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the session joining response in 705, and step c is independent of following steps and the present invention does not limit the sequence order of performing step ***c*** and the steps following 705.

[0135] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the UE, which is generated by the IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the UE from the IMS/SIP Core and starts to record actions that affect the accounting and are performed by the UE on the IMS/SIP Core during the current multi-party service.

[0136] Figure 8 shows a flowchart of a charging correlation process in a case where a user who establishes a pre-established session re-enters a session after the user exits the session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of the current multi-party service, an AS-charging information collecting function and an IMS charging information collecting func-

tion. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core. As shown in Figure 8, the process includes followings.

[0137] 801-802: The UE and the PF negotiate session parameters before establishing a session. Then the UE sends a session modify request carrying an SID to the PF via the IMS/SIP Core. The session modify request may be carried in an SIP REFER message in this embodiment, however, the present invention is not limited to this.

[0138] 803: The PF returns a session modify response carrying the SID to the UE via the IMS/SIP Core. The session modify response may be carried in an SIP ACCEPTED message in this embodiment. However, the present invention is not limited to this.

[0139] 804: The PF sends a session joining request carrying the SID to the CF via the IMS/SIP Core to establish a session between the UE and the CF. The session joining request may be carried in an SIP INVITE message. However, the present invention is not limited to this.

[0140] 805-806: The CF returns a session joining response carrying the SID to the PF via the IMS/SIP Core. The session joining response may be carried in an SIP 200OK or an OK message. However, the present invention is not limited to this.

[0141] 807-809: The PF sends to the UE a session joining notification (e.g., a NOTIFY message) carrying a result of the session setup via the IMS/SIP Core. The UE returns a session joining response (e.g., an OK response) to the PF via the IMS/SIP Core. As such, the session re-entering process is completed.

[0142] In Figure 8, the service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the session joining request in 804 and after successful adding the UE into the session. Step ***a*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 804. The PF may perform step b after receiving the session joining response in 809 and similarly, the bearer control layer entity related to the charging correlation process, i.e., the IMS/SIP Core, may perform step c after receiving the response in 809.

[0143] Step ***a*** may include followings, the CF requests the AS-charging information collecting function to start charging and sends the CDR of the user (the UE) who requests to re-enter the session, which is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE from the CF and starts to record actions that affect an accounting and are performed by the UE on the CF during the current multi-party service. It need to be noted that when the user re-enters the session, the opened CDR of the UE is a new CDR instead of the CDR of the UE that is generated before the UE dropped out of the session. However, the two CDRs have the same SID and can be correlated based on the SID.

[0144] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the UE, which is generated by the PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the PF and starts to record actions that affect the accounting and are performed by the UE on the PF during the current multi-party service.

[0145] The bearer control layer entity related to the charging correlation process in Figure 8 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the session joining response in 805, and step c is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 805.

[0146] Step c may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the UE, which is generated by the IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the UE from the IMS/SIP Core and starts to record actions that affect the accounting and are performed by the UE on the IMS/SIP Core during the current multi-party service.

[0147] In embodiments shown in Figures 4 to 8, the PF and the CF are performed by two separated entities. In practical applications, the PF and the CF may be performed by one entity. In such a case, the essential processes of the embodiments in which the PF and the CF are performed by one entity are similar to the processes shown in Figures 4 to 8 and will not be described in detail herein, but are still covered by the protection scope of the invention.

[0148] Moreover, the PF and the CF correspond to the same bearer control layer entity e.g., the IMS/SIP Core in Figures 4 to 8. In practical applications, the PF and the CF may correspond to different bearer control layer entities. When the PF and the CF are in the same network of an operator, the PF and the CF correspond to the same IMS/SIP Core. When the PF and the CF are in different networks of different operators, the PF and the CF correspond to different IMS/SIP Cores. No matter the PF and the CF correspond to the same IMS/SIP Core or to different IMS/SIP Cores, the method in accordance with embodiments of the present invention is applicable. No matter the PF and the CF correspond to the same bearer control layer entity or to different bearer control layer entities, the method in accordance with embodiments of the present invention is applicable. In one word, the application service layer entities such as the PF and the CF send/receive messages comprising session modify requests/responses, session joining requests/responses, release session requests/responses, session modify requests/responses and session modify and release requests via corresponding IMS/SIP Cores. Detailed proc-

esses will not be described herein, but are still covered by the protection scope of the present invention.

[0149] In the flowcharts of the above embodiments, the responses returned by the called UE to the CF carry the SID. However, since the CF has learnt the SID of the current service, the responses from the called UE to the CF may not carry the SID.

[0150] In the above embodiments, the SID is sent to the AS-charging information collecting function and IMS charging information collecting function, thus the application service layer of the AS and the bearer control layer of the IMS can perform a function in accordance with the charging correlation scheme provided by embodiments of the present invention. In practical applications, it may be unnecessary for the application service layer or the bearer control layer to implement the charging correlation process, and in such a case the SID and CRDs needs not to be sent to the AS-charging information collecting function or the IMS charging information collecting function.

[0151] The embodiments of the present invention adopt SIDs as service identifiers, and a description of the SID used in a PoC service is given herein. In a PoC service, SID is assigned by a service control function to a calling/called PoC client. The SID is used to identify a PoC group session in an SIP communication, but is not used in charging data generation processes. A PoC Session Identity (PoC SID) is constructed in a format of a SIP Uniform Resource Identifier (URI) and is sent during a PoC session establishment process to a PoC client in a Contact header field and/or a TBCP CONNECT message. The PoC SID may be assigned and available for a long period, or be assigned temporarily. A long term PoC SID is adapted to a pre-arranged PoC group session. A temporary PoC SID is assigned by a server performing CF in the network to a PoC client when the PoC client establishes a PoC session for a PoC service for a first time, and is remained valid as long as the PoC service is in progress. When the PoC client establishes a session for another PoC service, the new PoC service is assigned a different PoC SID. However, if the PoC client exits a session of a PoC service temporarily and re-enters the same PoC service later, the PoC SID to used in the session will remain the same. It can be seen that the PoC SID may be used to identify a PoC service, therefore the PoC SID can also be used to charge correlation information of the service. Such PoC SID cannot be modified easily in transmission and the PoC client cannot modify the PoC SID after receiving the PoC SID, hence it is safe and reliable to use the PoC SID in a charging correlation process.

[0152] Embodiments of the present invention also propose a second charging correlation scheme to implement a charging correlation for a plurality of CDRs generated for one user in a multi-service that comprises a plurality of sub-services. The charging correlation scheme provides two ways to implement this charging correlation.

[0153] According to a first method, a service control function assigns a multi-service identifier for a current multi-service and assigns a sub-service identifier to each of the sub-services included in the current multi-service. The multi-service identifier and the sub-service identifiers are sent to a charging system. The charging system correlates CDRs of a sub-service based on the sub-service identifier of the sub-service, and correlates CDRs of the plurality of sub-services based on the multi-service identifier.

[0154] According to a second method, a service control function just assigns a multi-service identifier for a current multi-service. The multi-service identifier is sent to a charging system which correlates the CDRs of a plurality of sub-services of the current multi-service based on the multi-service identifier.

[0155] In a multi-service, a user may establish one or a plurality of sessions in each of the sub-services and a CDR is generated for each of the sessions of the user. Different methods may be used to correlate the CDRs based on the multi-service identifier. The CDRs to be correlated based on the multi-service identifier may be: CDRs corresponding to a plurality of sub-services (or a plurality of sessions of a plurality of sub-services) establish for one user in the current multi-service, or CDRs corresponding to a plurality of sub-services (or a plurality of sessions of a plurality of sub-services) established for a part of users or all users in the current multi-service. The method of correlating CDRs may be chosen based on special correlation policy applied. The contents and forms of correlation policies are not the technical problem to be solved by the present invention and will not be described further herein.

[0156] In a multi-service, a sub-service corresponds to a sub-service server. A service control function controls the sub-service servers to initiate, modify and terminate sub-services in order to initiate, modify and terminate the multi-service. According to the first method described above, for a sub-service, after the service control function assigns the multi-service identifier and the sub-service identifiers corresponding to the sub-services, the service control function sends the multi-service identifier and a sub-service identifier corresponding to a sub-service to a sub-service server corresponding to the sub-service. The sub-service server generates CDRs for the sub-service and sends the CDRs, the received multi-service identifier and the sub-service identifier to an AS-charging information collecting function of the sub-service server. The AS-charging information collecting function sends the received multi-service identifier, the sub-service identifier and the CDRs to a billing center. The billing center correlates the CDRs generated by one sub-service server based on the sub-service identifier, and further correlates CDRs generated by the sub-service servers based on the multi-service identifier. According to the second method described above, after assigning the multi-service identifier, the service control function sends the multi-service identifier to each sub-service server corresponding to each sub-service. A sub-service

server generates CDRs for each corresponding sub-service and sends the received multi-service identifier and the CDRs generated to the AS-charging information collecting function of the sub-service server. The AS-charging information collecting function sends the received multi-service identifier and the CDRs to the billing center. The billing center correlates the CDRs from different sub-service servers based on the multi-service identifier.

[0157] When the charging correlation scheme is applied to the application service layer, the charging information collecting function includes the AS-charging information collecting functions corresponding to the sub-service servers. The scheme can further be applied to the bearer control layer, and in such a case the charging information collecting function includes bearer control layer-charging information collecting functions of the bearer control layer entities corresponding to the sub-service servers. The bearer control layer entities corresponding to the sub-service servers are used to implement the service control functions. The bearer control layer entities corresponding to the sub-service servers are further used to record the multi-service identifier or a combination of the multi-service identifier and a sub-service identifier, and generate CDRs for corresponding sub-services. The bearer control layer entities send the multi-service identifier or the combination of the multi-service identifier and a sub-service identifier, and the CDRs to the bearer control layer-charging information collecting function of the bearer control layer entities. The AS-charging information collecting function and the bearer control layer-charging information collecting function send the received CDRs, and the multi-service identifier or the combination of the multi-service identifier and a sub-service identifier to the billing center. In Figures 9 and 10, the application service layer is taken as an example. When the present invention is applied only to the bearer control layer, charging correlation process involves UEs, service control functions, bearer control layer entities corresponding to sub-service servers, bearer control layer-charging information collecting functions and a billing center, without involving sub-service servers and AS-charging information collecting functions. Embodiments that the bearer control layer is employed are not described in detailed herein, but are still covered by the protection scope of the present invention. When the multi-service identifier or the combination of the multi-service identifier and the sub-service identifier is sent to an AS-charging information collecting function or to bearer control layer-charging information collecting function, the multi-service identifier or the combination of the multi-service identifier and the sub-service identifiers may be carried in CDRs.

[0158] Moreover, a multi-service usually includes a primary service and one or more supplementary services. That is, a multi-service includes a sub-service as the primary service and at least one sub-service as the supplementary service. The sub-service server and sub-service identifier corresponding to the primary service are called primary server and primary service identifier respectively, and the sub-service server and sub-service identifier corresponding to a supplementary service are called supplementary server and supplementary service identifier respectively. The service control function may be performed by a separated entity or be performed by the primary server. The multi-service identifier assigned to the multi-service may be identical with or different from the sub-service identifiers. When the multi-service includes a primary service and at least one supplementary service, the multi-service identifier may be identical with the primary service identifier.

[0159] The embodiments of the present invention are mainly applied to session-based applications or services such as multi-party services, the session IDs (SIDs) corresponding to different service sessions are already applied to conventional session-based services. The existing SIDs may be used as service identifiers to correlate a plurality of CDRs. Also new identifiers may be defined as the service identifiers. Usually information exchanged among entities on the application service layer is sent via corresponding bearer control layer entities. For example, servers performing PF of the multi-party service, the server performing CF, and the UEs may exchange information via corresponding bearer control layer entities such as an IMS/SIP Core network (IMS/SIP Core). At the same time, the network functions in the IMS/SIP Core may also generate CDRs for the current application or service in order to implement the charging correlation process on the bearer control layer. Each sub-service server of a sub-service corresponds to a bearer control layer entity, and the bearer control layer entity is adapted to bear the sub-service server.

[0160] At present, mainstream multi-services include: combinations of a plurality of multi-party services, a combination of a multi-party service and a Location Service or a combination of a multi-party service and a Presence Service. The second charging correlation scheme of the present invention is described hereinafter with reference to a multi-service comprising two multi-party services, e.g. a PoC service and a Conference service. A server performing CF and a server performing PF in the multi-party service are used to provide the services, yet the second charging correlation scheme focuses on the charging correlation of the sub-services, not internal flows of the sub-services. Therefore, for the sake of simplicity, the service processes between the server performing CF and the server performing PF in the multi-party service are omitted, and the server performing CF and the server performing PF are considered as sub-service servers of the multi-party service. A sub-service server corresponding to the PoC service is called a PoC server, and a sub-service server corresponding to the Conference service is called a Conference server. In embodiments of the present invention, the service control function is implemented by a PoC server.

[0161] Figure 9 shows a flowchart of a charging cor-

relation process for a multi-service in accordance with an embodiment of the present invention. In this embodiment, the service control function assigns a multi-service identifier. In this embodiment, the SID adapted to an individual PoC service in a conventional PoC service is used as the multi-service identifier. The entities involved in the embodiment include: PoC Client 1, PoC Client 2, a PoC server, a Conference server and a charging information collecting function. In this embodiment, PoC Client 1 initiates a multi-service and adds PoC Client 2 into the multi-service. As shown in Figure 9, the process includes followings.

[0162] 901: PoC Client 1 sends a session establishment request to the PoC server to initiate a PoC service. The session establishment request carries information of PoC Client 2, and is used to instruct to establish a multi-service comprising a Conference service and to add PoC Client 2 into the multi-service. The PoC server implements PoC service logic. A service control function in the PoC server assigns a multi-service identifier to the current multi-service. The multi-service identifier is the SID assigned to the PoC service. The session establishment request may be carried in an SIP INVITE message. However, the present invention is not limited to this.

[0163] 902: The service control function in the PoC server sends the session establishment request (e.g., an INVITE message) carrying the SID to the Conference server to initiate a Conference service. The Conference server returns a session establishment response (e.g., a 200OK message). The session establishment request carries the information of PoC Client 2 to indicate that PoC Client 2 need to be added into the Conference service.

[0164] After 902, both the PoC service and the Conference service are originated and the PoC server and the Conference server will perform steps ***b*** and ***a*** respectively to generate CDRs of the PoC service and CDRs of the Conference service on the AS-charging information collecting function.

[0165] Step ***a*** may include the followings. The Conference server generates CDRs for the present Conference service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that are generated by the Conference server and carries the SID. The AS-charging information collecting function opens the CDR received from the Conference server, starts to record actions which affect the accountings and, are performed on the Conference server by users of the Conference service, and returns a response to the Conference server.

[0166] Step ***b*** may include the followings. The PoC server generates a CDR for the current PoC service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDR that is generated by the PoC server and carries the SID. The AS-charging information collecting function opens the CDR received from the PoC server, starts to record actions which affect the accountings and are performed on the PoC server by users of the PoC service, and returns a response to the PoC server.

[0167] 903: The PoC server sends a session joining request carrying the SID to PoC Client 2 in order to add PoC Client 2 into the current PoC service session. PoC Client 2 returns a session joining response to the PoC server in order to indicate that PoC Client 2 has successfully joined the current PoC service session.

[0168] After the PoC server has successfully added PoC Client 2 into the current PoC service, the information of PoC Client 2 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step c needs to be performed. Step c may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDR carrying the SID of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDR of PoC Client 2 that carries the SID and is received from the PoC server, records the information of PoC Client 2 in the CDR, starts to record actions that affect the accounting and are performed by PoC Client 2 on the PoC server during the current multi-service, and returns a response to the PoC server.

[0169] 904: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 2 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 2 into the service session. The Conference server performs operations similar to the operations in 903 to add PoC Client 2 into the current Conference service session.

[0170] The information of PoC Client 2 needs to be recorded in the CDRs of the current Conference service session on the AS-charging information collecting function, therefore step ***d*** needs to be performed. Step ***d*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, sends the CDRs that carries the SID of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carries the SID and is received from the Conference server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0171] 905-906: The PoC server sends a session joining request (e.g., an INVITE message) carrying the SID to the Conference server, and the Conference server returns a session joining response (e.g., a 200OK message). The session joining request carries information of PoC Client 1 to indicate that PoC Client 1 need to be added into the Conference service. At the same time, the

PoC server adds PoC Client 1 into the current PoC service session and returns a session joining response (e.g., a 2000K message) to PoC Client 1.

[0172] After the PoC server has successfully added PoC Client 1 into the current PoC service session, the information of PoC Client 1 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step e needs to be performed. Step e may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID of PoC Client 1 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carries the SID and is received from the PoC server, records the information of PoC Client 1 in the CDR, starts to record actions that are performed by PoC Client 1 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0173] 907: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 1 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 1 into the service session. The Conference server performs operations similar to the operations in 903 to add PoC Client 1 into the current Conference service session.

[0174] The information of PoC Client 1 needs to be recorded in the CDRs of the current Conference service session on the AS-charging information collecting function, therefore step ***f*** needs to be performed. Step ***f*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID of PoC Client I to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carries the SID and is received from the Conference server, records the information of PoC Client 1 in the CDR, starts to record actions that are performed by PoC Client 1 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0175] After the processes described above, the CDRs of the sub-services, which are saved in the AS-charging information collecting function, carry the multi-service identifier, therefore, the CDRs of the sub-services can be correlated based on the multi-service identifier.

[0176] Figure 10 shows a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention. In this embodiment, the service control function assigns a multi-service identifier for the multi-service and assigns a sub-service identifier to each sub-service. In this embodiment, the sub-service identifier of the PoC service adopts the SID assigned for an individual PoC service in the conventional PoC service, called SID1. The sub-service identifier of the Conference service adopts the SID assigned for an individual Conference service in the conventional Conference service, called SID2. The entities involved in this embodiment include: PoC Client 1, PoC Client 2, a PoC server, a Conference server and a charging information collecting function. In this embodiment, PoC Client 1 initiates a multi-service and adds PoC Client 2 into the multi-service. As shown in Figure 10, the process includes followings.

[0177] 1001: PoC Client 1 sends a session establishment request to the PoC server to initiate a PoC service. The session establishment request carries information of PoC Client 2 and is used to instruct to establish a multi-service comprising a Conference service and to add PoC Client 2 into the multi-service. The PoC server implements PoC service logic. A service control function in the PoC server assigns a multi-service identifier for the current multi-service, assigns one or more sub-service identifiers to the PoC service and assigns one or more sub-service identifiers to the Conference service.

[0178] The sub-service identifier of the PoC service adopts the SID assigned to the PoC service, called SID1; the sub-service identifier of the Conference service adopts the SID assigned to the Conference service, called SID2; and the multi-service identifier adopts the SID assigned to the multi-service, called SID0. The session establishment request may be carried in an SIP INVITE message in this embodiment. However, the present invention is not limited to this.

[0179] 1002: The service control function in the PoC server sends the session establishment request (e.g., an INVITE message) carrying the SID0 and SID2 to the Conference server to initiate a Conference service. The Conference server returns a session establishment response (e.g., a 2000K message). The session establishment request carries information of PoC Client 2 to indicate that PoC Client 2 need to be added into the Conference service.

[0180] After 1002, both the PoC service and the Conference service are originated, and the PoC server and the Conference server will perform steps ***b*** and ***a*** respectively to generate CDRs of the PoC service session and CDRs of the Conference service session on the AS-charging information collecting function.

[0181] Step ***a*** may include the followings. The Conference server generates CDRs for the current Conference service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that is generated by the Conference server and carries the SID0 and SID2. The AS-charging information collecting function opens the CDRs received from the Conference server, starts to record actions of the Conference service which are performed on the Conference server by users and affect the accounting, and returns a response from the AS-charging information collecting function to the Conference server.

[0182] Step ***b*** may include the followings. The PoC

server generates CDRs for the current PoC service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that is generated by the PoC server and carries the SID0 and SID1. The AS-charging information collecting function opens the CDRs from the PoC server, starts to record actions of the PoC service which are performed on the PoC server by users and affect the accounting, and returns a response to the PoC server.

[0183] 1003: The PoC server sends a session joining request carrying the SID0 and SID1 to PoC Client 2 in order to add PoC Client 2 into the current PoC service session. PoC Client 2 returns a session joining response to the PoC server in order to indicate that PoC Client 2 has successfully joined the current PoC service session.

[0184] After the PoC server has successfully added PoC Client 2 into the current PoC service, the information of PoC Client 2 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step ***c*** needs to be performed. Step ***c*** may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID0 and SID1 of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carry the SID0 and SID1 and are received from the PoC server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0185] 1004: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 2 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 2 into the service session. The Conference server performs operations similar to the operations in 1003 in order to add PoC Client 2 into the current Conference service.

[0186] The information of PoC Client 2 needs to be recorded in the CDRs of the current Conference service on the AS-charging information collecting function, therefore step ***d*** needs to be performed. Step ***d*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID2 of PoC Client 2. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carry the SID0 and SID2 are received from the Conference server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0187] 1005-1006: The PoC server sends a session joining request (e.g., an INVITE message) carrying the SID0 and SID2 to the Conference server, and the Conference server returns a session joining response (e.g., a 2000K message). The session joining request carries information of PoC Client 1 to indicate that PoC Client 1 can be added into the Conference service session. At the same time, the PoC server adds PoC Client 1 into the current PoC service session and returns a session joining response (e.g., a 2000K message) to PoC Client 1.

[0188] After the PoC server has successfully added PoC Client 1 into the current PoC service session, the information of PoC Client 1 needs to be recorded in the CDRs of the current PoC service on the AS-charging information collecting function, therefore step ***e*** needs to be performed. Step e may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID1 of PoC Client 1. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carry the SID0 and SID1 are received from the PoC server, records the information of PoC Client 1 in the CDRs, starts to record actions that are performed by PoC Client 1 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0189] 1007: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 1 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 1 into the service session. The Conference server performs operations similar to the operations in 1003 to add PoC Client 1 into the current Conference service session.

[0190] The information of PoC Client 1 needs to be recorded in the CDRs of the current Conference service on the AS-charging information collecting function, therefore step ***f*** needs to be performed. Step ***f*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID2 of PoC Client 1. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carry the SID0 and SID2 are received from the Conference server, records the information of PoC Client 1 in the CDRs, starts to record actions that are performed by PoC Client 1 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0191] After the processes described above, CDRs of the sub-services in the AS-charging information collecting function have the multi-service identifier and the sub-service identifiers corresponding to the sub-services. Therefore the CDRs of a sub-service may be correlated based on the sub-service identifier of the sub-service, and the CDRs of different sub-services, which have al-

ready been correlated based on the sub-service identifiers, are then correlated based on the multi-service identifier.

[0192] Figures 9 and 10 illustrate the second charging correlation scheme of the present invention which is applied to the application service layer. When the charging correlation scheme is applied to the bearer control layer, the entities involved include: a bearer control layer entity corresponding to the sub-service servers, a bearer control layer-charging information collecting function, and UEs. The bearer control layer entities corresponding to the sub-service servers may record the multi-service identifier and/or sub-service identifiers when the multi-service identifier and/or sub-service identifiers are received by the sub-service servers, generate CDRs, and send the received multi-service identifier and/or sub-service identifiers and the CDRs to the corresponding bearer control layer-charging information collecting functions. The processes in which the charging correlation scheme is applied to the bearer control layer is similar to that in Figures 9 and 10 and will not be described in detail herein, but is covered by the protection scope of the present invention.

[0193] Moreover, the charging correlation process may be variable based on different multi-services to be charged for, yet the charging correlation process will always be in accordance with the two methods of implementing the second charging correlation scheme provided in the above embodiments of the present invention. Since different multi-services may include various sub-services, the charging flow may vary in different ways. For example, the service control function may send the multi-service identifier and the sub-service identifiers to the primary server and the supplementary servers in different ways: 1) the service control function may send a primary service identifier when initiating a primary service session, or when setting up the primary service session, or when setting up all supplementary service sessions, or when setting up the current multi-service session; 2) the service control function may send the multi-service identifier when initiating the primary service session, or when setting up the primary service session, or when setting up all supplementary service sessions, or when setting up the current multi-service session; 3) the service control function may send a supplementary service identifier when initiating corresponding supplementary service session, or when setting up corresponding supplementary service session, or when setting up the current multi-service session; 4) the service control function may send the multi-service identifier when initiating each of the supplementary service sessions, or when setting up each of the supplementary service sessions, or when setting up the current multi-service session. Various charging correlation processes for various multi-services will not be listed herein. However, any charging correlation process for multi-service that is in accordance with the principles of the current invention falls in the scope of the present invention.

[0194] In embodiments of the present invention, a sub-service included in a multi-service can be any application or service. A multi-service may include sub-services such as PoC service, Conference service, Location service, Presence service and any combination of the above applications and services.

[0195] A system for charging correlation for an application or service is further proposed. Figure 11 is a structure diagram of a system for implementing a charging correlation of an application or service in accordance with an embodiment of the present invention. In an embodiment of the present invention, the system includes a service identifier generating unit, a CDR generating unit and a CDR correlating unit.

[0196] The service identifier generating unit is adapted to assign a service identifier to a current application or service and send the service identifier to the CDR generating unit. The CDR generating unit is adapted to receive the service identifier from the service identifier generating unit, generate a plurality of CDRs for the current application or service and send the received service identifier and the CDRs generated to the CDR correlating unit. The CDR correlating unit is adapted to receive the CDRs and the service identifier from the CDR generating unit and correlate the CDRs of the current application or service based on the service identifier.

[0197] The service identifier generating unit may be a separated entity or be integrated into the service control function of the application or service. When the system is applied to a single-service, the service control function is an AS of the current application or service, e.g., a server performing CF for a multi-party service such as PoC service and Conference service. When the system is applied to a multi-service, the service control function is a service control function of the current multi-service. The service control function may be integrated into an AS of a sub-service (i.e., a sub-service server) of the multi-service or be integrated into a server performing CF for the multi-party service such as the PoC service and the Conference service. The CDR correlating unit may also be a separated entity or be integrated into a charging system.

[0198] Moreover, the CDR generating unit may further add the received service identifier into the CDRs generated so that the CDRs and the service identifier may be sent.

[0199] In the system provided by embodiments of the present invention, the units may function according to the processes described in the preceding embodiments, and detailed functions of the units are not described anymore.

[0200] A system for charging correlation is also proposed by embodiments of the present invention. The system for charging correlation includes a service control function entity and a charging system. The service control function entity is adapted to assign a service identifier to a current application or service and the charging system is adapted to correlate at least one set of CDRs generated for the application or service based on the service iden-

tifier that is assigned by the service control function entity. The charging system may further include a charging information collecting function entity and a billing center. The charging information collecting function entity is adapted to receive the service identifier from the service control function entity and collect at least one set of CDRs, and the billing center is adapted to correlate at least one set of CDRs based on the service identifier.

[0201] The service control function entity may be an AS adapted to generate at least one set of CDRs for the application or service. The system may further include a bearer control layer entity adapted to record the service identifier assigned by the service control function entity, and generate at least one set of CDRs. In such a case the charging information collecting function entity further includes an AS-charging information collecting function entity and a bearer control layer-charging information collecting function entity. The AS-charging information collecting function is adapted to receive the service identifier from the service control function entity (i.e., the AS) and the at least one set of CDRs generated by the service control function entity, and the bearer control layer-charging information collecting function entity is adapted to receive the service identifier from a bearer control entity and the at least one set of CDRs generated by the bearer control layer entity. Therefore the billing center can correlate the at least one set of CDRs received from the bearer control layer-charging information collecting function entity based on the service identifier, or correlate the at least one set of CDRs received from the AS-charging information collecting function entity based on the service identifier, or correlate the at least one set of CDRs from the bearer control layer-charging information collecting function entity and the at least one set of CDRs from the AS-charging information collecting function entity based on the service identifier.

[0202] When the application or service is a multi-party service, the service control function entity is a server performing CF. At least one server performing PF may further be included. The bearer control layer entity may include a bearer control layer entity corresponding to the server performing CF, and at least one bearer control layer entity corresponding to the server performing PF. The bearer control layer entity corresponding to the server performing CF is adapted to bear the server performing CF, and a bearer control layer entity corresponding to a server performing PF is adapted to bear the server performing PF. The AS-charging information collecting function entity may further include an AS-charging information collecting function entity of the server performing CF and at least one AS-charging information collecting function entity of the server performing PF. The bearer control layer-charging information collecting function entity may further include a bearing control layer charging information collecting function entity of the bearer control layer entity corresponding to the server performing CF, and at least one bearer control layer-charging information collecting function entity of a bearer control layer entity corresponding to a server performing PF.

[0203] When the application or service is a multi-service comprising a plurality of sub-services, the system may further include sub-service servers of a plurality of sub-services. The bearer control layer entity may further include at least one bearer control layer entity corresponding to a plurality of sub-service servers. The bearer control layer entity corresponding to the sub-service servers is adapted to bear the sub-service servers. The AS-charging information collecting function entity may further include AS-charging information collecting function entities of sub-service servers, and the bearer control layer-charging information collecting function entity may further include bearer control layer-charging information collecting function entities of bearer control layer entities of sub-service servers.

[0204] The functions of the components of the system in various cases have been given in the preceding description and will not be explained further herein, but are still covered by the protection scope of the present invention.

[0205] A billing center is also proposed in embodiments of the present invention. The billing center may include a first module adapted to receive a service identifier of the current application or service, and receive at least one set of CDRs generated for the application or service, and a second module adapted to correlate at least one set of CDRs based on the service identifier received by the first module and generate a bill. The CDRs received by the first module may be CDRs generated by an AS and CDRs generated by a bearer control layer entity. The second module may correlate the CDRs generated by the AS based on the service identifier, or correlate the CDRs generated by the bearer control layer entity based on the service identifier, or correlate the CDRs generated by the AS and the CDRs generated by the bearer control layer entity together based on the service identifier.

[0206] An apparatus for generating charging data record is also proposed in embodiments of the present invention. The an apparatus for generating charging data record may include a first module and a second module. The first module is adapted to receive a service identifier assigned to the current application or service, and the second module is adapted to generate for the application or service at least one set of CDRs carrying the service identifier that is received by the first module and adapted to export the at least one set of CDRs. The an apparatus for generating charging data record may be an AS or a bearer control layer entity in embodiments of the present invention.

[0207] In one word, in embodiments of the present invention, a plurality of CDRs generated for a user in a service session may be correlated for charging, and the CDRs of a plurality of sub-services in a multi-service of the user can also be correlated for charging. Furthermore, the embodiments of the present invention is easy to implement and can improve accuracy of correlated

charging. Therefore the methods and apparatus proposed in the embodiments of the present invention are beneficial in supplementing and improving the conventional application or service charging correlation process (especially the charging correlation process of a multi-party service).

[0208] The previous description of the disclosed embodiments is provided to enable those skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art and generic principles defined herein may be applied to other embodiments without departing from the scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

Claims

1. A method for charging correlation for an application or service, comprising:

   assigning a service identifier by a service control function to an application or service;
   sending the service identifier to a charging system; and
   correlating, by the charging system, at least one Charging Data Record CDR generated for the application or service based on the service identifier.

2. The method according to Claim 1, wherein the charging system comprises a charging information collecting function entity and a billing center; and the method further comprises:

   sending the service identifier to the billing center via the charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the service control function entity based on the service identifier.

3. The method according to Claim 2, wherein the application or service is a single-service, the service control function entity comprises an Application Server AS and the charging information collecting function entity comprises an AS charging information collecting function entity corresponding to the AS; and the method further comprises:

   assigning a service identifier by the AS to the single-service;
   sending the service identifier to the billing center via the AS charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the AS based on the service identifier.

4. The method according to Claim 3, wherein the charging information collecting function entity further comprises: a bearer control layer charging information collecting function entity corresponding to a bearer control layer entity that corresponds to the AS, and the method further comprises:

   assigning the service identifier by the AS to the single-service;
   sending the service identifier to the billing center via the AS charging information collecting function entity;
   recording the service identifier by the bearer control layer entity that corresponds to the AS;
   sending the service identifier to the billing center via the bearer control layer charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the AS based on the service identifier and correlating the at least one CDR generated by the bearer control layer entity based on the service identifier; or correlating the at least one CDR generated by the AS together with the at least one CDR generated by the bearer control layer entity based on the service identifier.

5. The method according to Claim 4, wherein the application or service is a multi-party service, the AS further comprises a server performing Control Function CF and at least one server performing Participating Function PF, and the service control function entity is the server performing CF; the AS charging information collecting function entity further comprises: at least one AS charging information collecting function entity covered by the server performing CF and at least one AS charging information collecting function entity covered by at least one server performing PF; the bearer control layer charging information collecting function entity further comprises at least one bearer control layer charging information collecting function entity covering the bearer control layer entities corresponding to the server performing CF and at least one server performing PF respectively, the bearer control layer entity corresponding to the server performing CF is used for bearing the server performing CF and the bearer control layer entity corresponding to a server performing PF is used for bearing the server performing PF;
   the server performing CF assigns the service identifier to the multi-party service and sends the service identifier to the at least one server performing PF, the server performing CF and the at least one server performing PF send the service identifier to the billing

center respectively via the AS charging information collecting function entity which corresponds to the server performing CF and the AS charging information collecting function entity which corresponds to the server performing PF;
the bearer control layer entities corresponding respectively to the server performing CF and the at least one server performing the PF record the service identifier, and send the server identifier to the billing center via the at least one bearer control layer charging information collecting function entity;
correlating, by the billing center, the CDRs generated by the server performing CF and generated by the at least server performing PF based on the service identifier, and correlating the CDRs generated by the bear control layer entities; or, correlating, by the billing center, the CDRs generated by the bear control layer entities, the CDRs generated by the server performing CF and generated by the at least server performing PF based on the service identifier.

6. The method according to any one of Claims 1 to 5, wherein sending the service identifier to the charging system comprises:

sending the at least CDR that carries the service identifier to the charging system.

7. The method according to any one of Claims 1 to 5, wherein in the application or service, one user is established at least one session, and one CDR corresponds to one session of one user; and
the at least CDR correlated for the application or service based on the service identifier comprises: CDRs corresponding to a plurality of sessions of one user in the application or service, or CDRs corresponding to a plurality of sessions of a part of or all users in the application or service.

8. The method according to Claim 2, wherein the application or service is a multi-service comprising a plurality of sub-services; the charging information collecting function entity comprises: at least one AS charging information collecting function entity which respectively corresponds to multiple sub-service server providing multiple sub-services; the service identifier assigned by the service control function entity for the application or service comprises: multi-service identifier of the multi-service and multiple sub-service identifiers of the multiple sub-services;
respectively receiving, by the multiple sub-service servers, the multi-service identifier and the respective sub-service identifier from the service control function entity, and sending the multi-service identifier and the respective sub-service identifier to the billing center via respective AS charging information collecting function entity; and
correlating, the billing center, the CDRs each sub-service server using the respective sub-service identifier, and correlating, the CDRs generated by all sub-service servers using the multi-service identifier.

9. The method according to Claim 8, wherein the charging information collecting function entity comprises: multiple bear control layer charging information collecting function entities of bear control layer entities that respectively correspond to the multiple sub-service servers; and the bear control layer entities that respectively correspond to the multiple sub-service servers are adapted to respectively bear the bear control layers;
recording, by the bear control layer entities that respectively correspond to the multiple sub-service servers, the corresponding sub-service identifier and the multi-service identifier, and sending the corresponding sub-service identifier and the multi-service identifier to the billing center via respective bear control layer charging information collecting function entities;
correlating, by the billing center, the CDRs generated by each bear control layer entity based on the corresponding sub-service identifier, and correlating CDRs generated by all the bear control layer entities based on the multi-service identifier.

10. The method according to Claim 8 or 9, wherein sending the multi-service identifier and the sub-service identifier comprises:

sending the CDRs that carry the multi-service identifier and the sub-service identifier.

11. The method according to Claim 8 or 9, wherein the multi-service identifier is identical to one of the sub-service identifiers, or is not identical to any one of the sub-service identifiers.

12. The method according to Claim 2, wherein the application or service is a multi-service comprising a plurality of sub-services; the service identifier assigned by the service control function entity for the application or service comprises: multi-service identifier of the multi-service; the charging information collecting function comprises: at least one AS charging information collecting function entity that respectively correspond to the multiple sub-service servers;
receiving, by the multiple sub-service servers, the multi-service identifier from the service charging information collecting function entity, and respectively sending the multi-service identifier to the billing center via respective AS charging information collecting function entity; correlating, by the billing center, the CDRs generated by the multiple sub-service servers based on the multi-service identifier.

13. The method according to Claim 12, wherein the

charging information collecting function entity comprises: multiple bear control layer charging information collecting function entities of bear control layer entities that respectively correspond to the multiple sub-service servers; and the bear control layer entities that respectively correspond to the multiple subservice servers are adapted to respectively bear the bear control layers;
the method further comprises:

recording, by the bear control layer entities that respectively correspond to the multiple subservice servers, the multi-service identifier, and sending the multi-service identifier to the billing center via respective bear control layer charging information collecting function entities; correlating, by the billing center, the CDRs generated by the bear control layer entities based on the the multi-service identifier.

14. The method according to Claim 12 or 13, wherein sending the multi-service identifier comprises: sending the CDRs that carry the multi-service identifier.

15. A system for charging correlation for an application or service, comprising:

a service control function, adapted to assign a service identifier for an application or service; and
a charging system, adapted to correlate at least one Charging Data Records CDR generated for the application or service based on the service identifier.

16. The system according to Claim 15, wherein the charging system comprises:

a charging information collecting function entity, adapted to receive the service identifier assigned by the service control function entity and collect the at least one CDR; and
a billing center, adapted to correlate the at least one CDR based on the service identifier received from the charging information collecting function entity.

17. The system according to Claim 16, wherein the service control function comprises an Application Server AS adapted to generate at least one CDR for the application or service; and the system further comprises a bearer control layer entity, adapted to record the service identifier and generate at least one CDR for the application or service.
wherein the charging information collecting function entity comprises:

an AS-charging information collecting function entity, adapted to receive the service identifier and the at least one CDR from the service control function entity;
a bearer control layer-charging information collecting function entity, adapted to receive the service identifier and the at least one CDR from the bearer control layer entity;

wherein
the billing center is further adapted to correlate the at least one CDR from the bearer control layer-charging information collecting function entity based on the service identifier, and correlate the at least one CDR from the AS-charging information collecting function entity based on the service identifier respectively, or adapted to correlate the at least one CDR from the bearer control layer-charging information collecting function entity with the at least one CDR from the AS-charging information collecting function entity based on the service identifier.

18. The system according to Claim 17, wherein the application or service is a multi-party service and the service control function entity is a server performing Controlling Function CF,
the system further comprises at least one server performing Participating Function PF,
wherein the bearer control layer entity comprises a bearer control layer entity corresponding to the server performing CF and at least one bearer control layer entity corresponding to the at least one server performing PF; the bearer control layer entity corresponding to the server performing CF is adapted to bear the server performing CF and the bearer control layer entity corresponding to the server performing PF is adapted to bear the server performing PF;
the AS-charging information collecting function entity comprises an AS-charging information collecting function entity corresponding to the server performing CF and at least one AS-charging information collecting function corresponding to the at least one server performing PF;
the bearer control layer-charging information collecting function comprises a bearer control layer-charging information collecting function entity of the bearer control layer entity corresponding to the server performing CF and at least a bearer control layer-charging information collecting function of the bearer control layer entity corresponding to the at least one server performing PF;
the server performing CF is adapted to assign the service identifier, send the service identifier to the at least one server performing PF, generate at least one set of CDR and send the service identifier and the CDRs to the AS-charging information collecting function entity of the server performing CF;
each server performing PF is adapted to record the service identifier, generate at least one set of CDR

and send the at least one set of CDR and the service identifier to the AS-charging information collecting function entity of the server performing PF;
the bearer control layer entity corresponding to the server performing CF is adapted to record the service identifier, generate the CDRs and send the CDRs and the service identifier to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
each bearer control layer entity corresponding to a server performing PF is adapted to record the service identifier, generate the CDRs and send the CDRs and the service identifier to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
the AS-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center; and
the bearer control layer-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center.

19. The system according to Claim 17, wherein the application or service is a multi-service comprising a plurality of sub-services, and
the system further comprises a plurality of sub-service servers providing the plurality of sub-services respectively; wherein
the bearer control layer entity comprises at least one bearer control layer entity corresponding to the sub-service servers and is adapted to bear the sub-service servers;
the AS-charging information collecting function entity comprises AS-charging information collecting function entities of respective sub-service servers;
the bearer control layer-charging information collecting function entity comprises bearer control layer-charging information collecting function entities of the bearer control layer entities corresponding to respective sub-service servers;
the service control function entity is further adapted to assign sub-service identifiers for the sub-services and send the service identifier and the sub-service identifiers to the sub-service servers;
each sub-service server is adapted to record the service identifier and the sub-service identifiers from the service control function entity, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier, the sub-service identifier and the at least one set of CDRs to the AS-charging information collecting function entity of the sub-service server;
the bearer control layer entity corresponding to the sub-service server is adapted to record the service identifier and the sub-service identifier from the sub-service server, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier, the sub-service identifier and the at least one set of CDRs to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
the AS-charging information collecting function entity is adapted to send the service identifier, sub-service identifiers and the CDRs to the billing center;
the bearer control layer-charging information collecting function entity is adapted to send the service identifier, sub-service identifiers and the CDRs to the billing center; and
the billing center is further adapted to correlate CDRs of each sub-service according to the sub-service identifier corresponding to the sub-service, and correlate CDRs of the plurality of sub-services according to the service identifier.

20. The system according to Claim 17, wherein the application or service is a multi-service comprising a plurality of sub-services, and
the system further comprises a plurality of sub-service servers providing the sub-services; wherein
the bearer control layer entity comprises at least one bearer control layer entity corresponding to the sub-service servers and is adapted to bear the sub-service servers;
the AS-charging information collecting function entity comprises AS-charging information collecting function entities corresponding to the sub-service servers; the bearer control layer-charging information collecting function entity comprises bearer control layer-charging information collecting function entities corresponding to the bearer control layer entities corresponding to the sub-service servers;
the service control function entity is adapted to send the service identifier to the sub-service servers;
the sub-service server is adapted to record the service identifier from the service control function entity, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the at least one set of CDRs and the service identifier to the AS-charging information collecting function entity of the sub-service server;
the bearer control layer entity corresponding to a sub-service server is adapted to record the service identifier from the sub-service server, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier and the at least one set of CDRs to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
an AS-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center;
a bearer control layer-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center; and
the billing center is adapted to correlate the CDRs of the sub-services based on the service identifier.

21. A billing center, comprising:

a first module, adapted to receive a service identifier assigned for an application or service and Charging Data Records CDRs generated for the application or service; and
a second module, adapted to correlate the CDRs based on the service identifier from the first module.

22. The billing center according to Claim 21, wherein the CDRs received by the first module comprise CDRs generated by an Application Server AS and CDRs generated by a bearer control layer entity; and
the second module is adapted to correlate the CDRs generated by the AS based on the service identifier and correlate the CDRs generated by the bearer control layer entity based on the service identifier respectively, or adapted to correlate the CDRs generated by the AS and the CDRs generated by the bearer control layer entity based on the service identifier.

23. The billing center according to any of Claim 21 or 22, wherein the application or service comprises at least one session and each set of the CDRs identified by ICID corresponds to one session; and
the second module is adapted to correlate a plurality of CDRs corresponding to a plurality of sessions of one user in the application or service based on the service identifier, or adapted to correlate a plurality of CDRs corresponding to a plurality of sessions of a part of or all users in the application or service based on the service identifier.

24. A apparatus for generating a charging data record, comprising:

a first module, adapted to receive a service identifier assigned for an application or service; and
a second module, adapted to generate Charging Data Records, CDRs, carrying the service identifier from the first module for the application or service.

25. The apparatus according to Claim 24, wherein the apparatus is an AS or a bearer control layer entity.

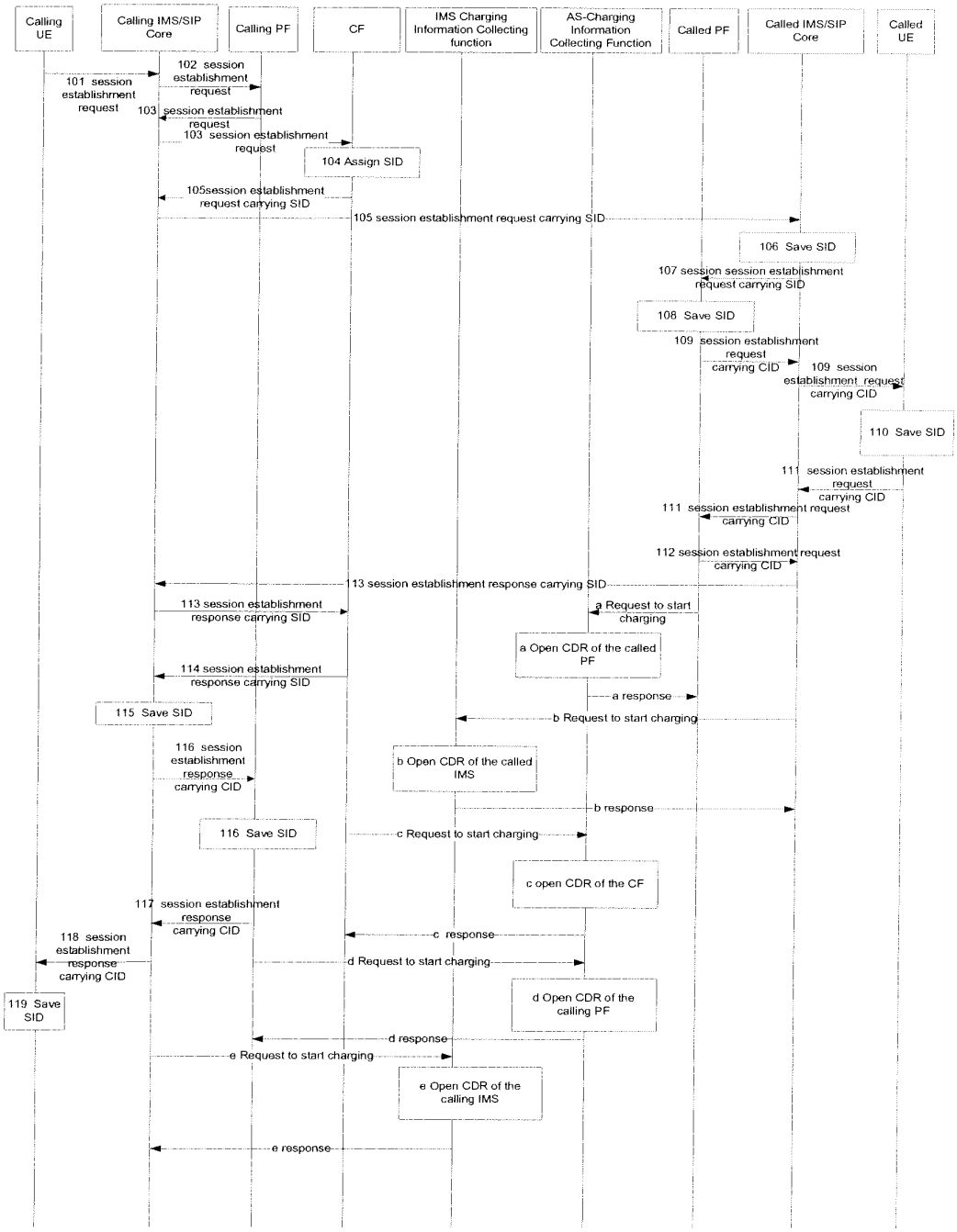

Calling UE
Calling IMS/SIP Core
Calling PF
CF
IMS Charging Information Collecting function
AS-Charging Information Collecting Function
Called PF
Called IMS/SIP Core
Called UE
101 session establishment request
102 session establishment request
103 session establishment request
103 session establishment request
104 Assign SID
105session establishment request carrying SID
105 session establishment request carrying SID
106 Save SID
107 session session establishment request carrying SID
108 Save SID
109 session establishment request carrying CID
109 session establishment request carrying CID
110 Save SID
111 session establishment request carrying CID
111 session establishment request carrying CID
112 session establishment request carrying CID
113 session establishment response carrying SID
113 session establishment response carrying SID
a Request to start charging
a Open CDR of the called PF
114 session establishment response carrying SID
a response
115 Save SID
b Request to start charging
116 session establishment response carrying CID
b Open CDR of the called IMS
b response
116 Save SID
c Request to start charging
c open CDR of the CF
117 session establishment response carrying CID
c response
118 session establishment response carrying CID
d Request to start charging
119 Save SID
d Open CDR of the calling PF
d response
e Request to start charging
e Open CDR of the calling IMS
e response

Fig. 1

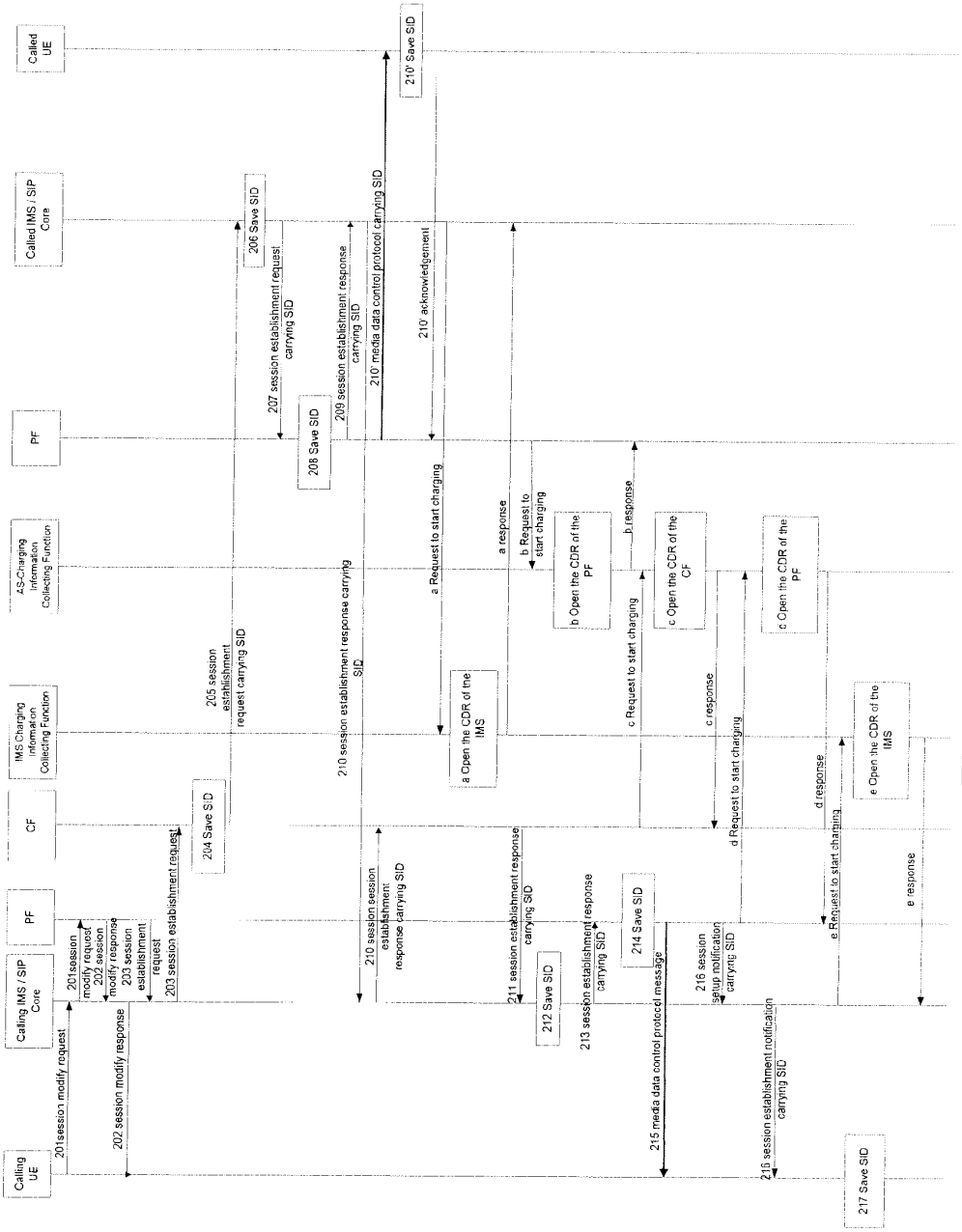

Calling UE
Calling IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
PF
Called IMS / SIP Core
Called UE
201 session modify request
202 session modify response
201 session modify request
202 session modify response
203 session establishment request
203 session establishment request
204 Save SID
205 session establishment request carrying SID
206 Save SID
207 session establishment request carrying SID
208 Save SID
209 session establishment response carrying SID
210' media data control protocol carrying SID
210' Save SID
210' acknowledgement
210 session establishment response carrying SID
210 session establishment response carrying SID
a Request to start charging
a response
a Open the CDR of the IMS
b Request to start charging
b response
b Open the CDR of the PF
c Request to start charging
c response
c Open the CDR of the CF
d Request to start charging
d response
c Open the CDR of the PF
e Request to start charging
e response
e Open the CDR of the IMS
211 session establishment response carrying SID
212 Save SID
213 session establishment response carrying SID
214 Save SID
215 media data control protocol message
216 session setup notification carrying SID
216 session establishment notification carrying SID
217 Save SID

Fig. 2

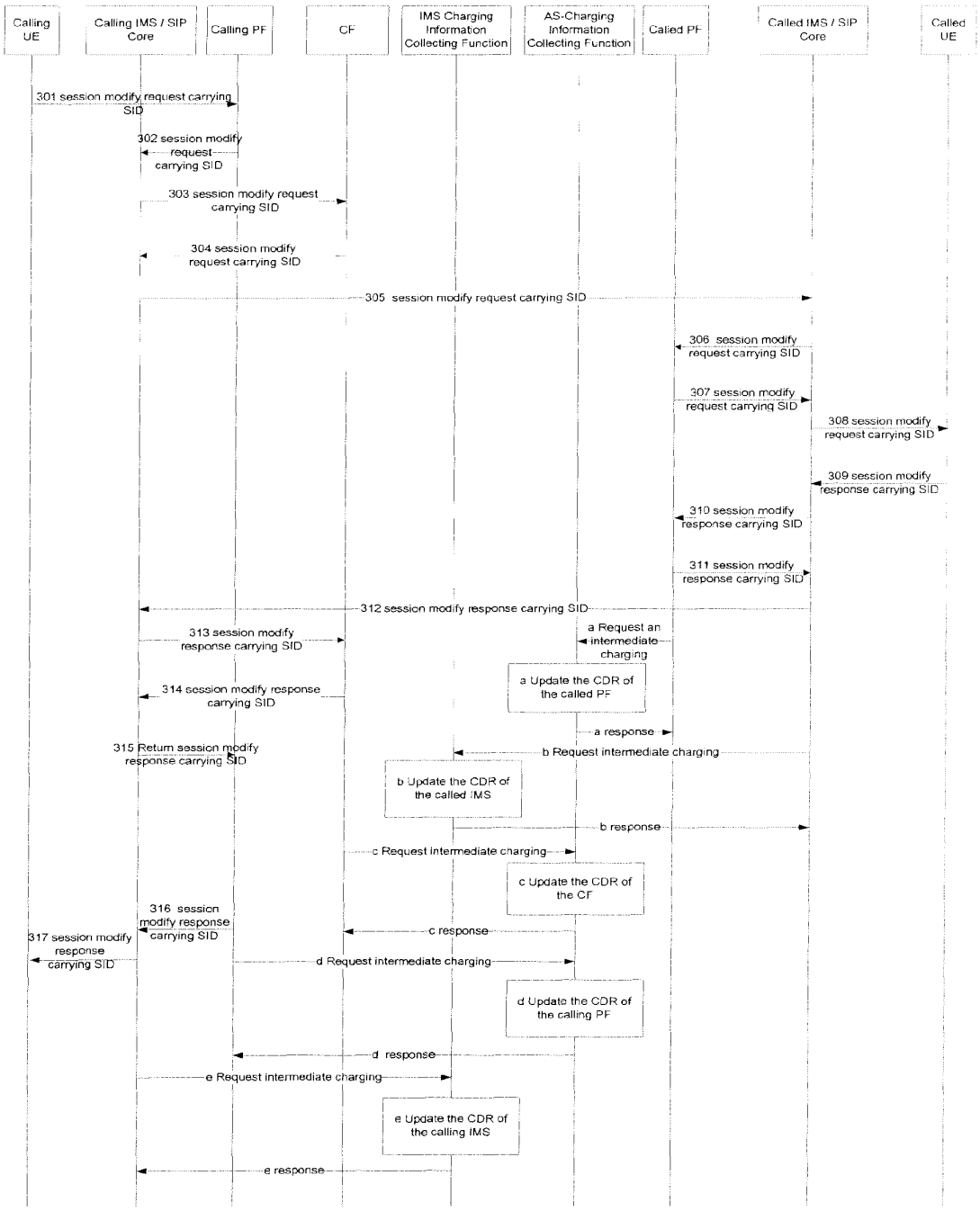

Calling UE
Calling IMS / SIP Core
Calling PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
Called PF
Called IMS / SIP Core
Called UE
301 session modify request carrying SID
302 session modify request carrying SID
303 session modify request carrying SID
304 session modify request carrying SID
305 session modify request carrying SID
306 session modify request carrying SID
307 session modify request carrying SID
308 session modify request carrying SID
309 session modify response carrying SID
310 session modify response carrying SID
311 session modify response carrying SID
312 session modify response carrying SID
313 session modify response carrying SID
a Request an intermediate charging
a Update the CDR of the called PF
314 session modify response carrying SID
a response
315 Return session modify response carrying SID
b Request intermediate charging
b Update the CDR of the called IMS
b response
c Request intermediate charging
c Update the CDR of the CF
316 session modify response carrying SID
c response
317 session modify response carrying SID
d Request intermediate charging
d Update the CDR of the calling PF
d response
e Request intermediate charging
e Update the CDR of the calling IMS
e response

Fig. 3

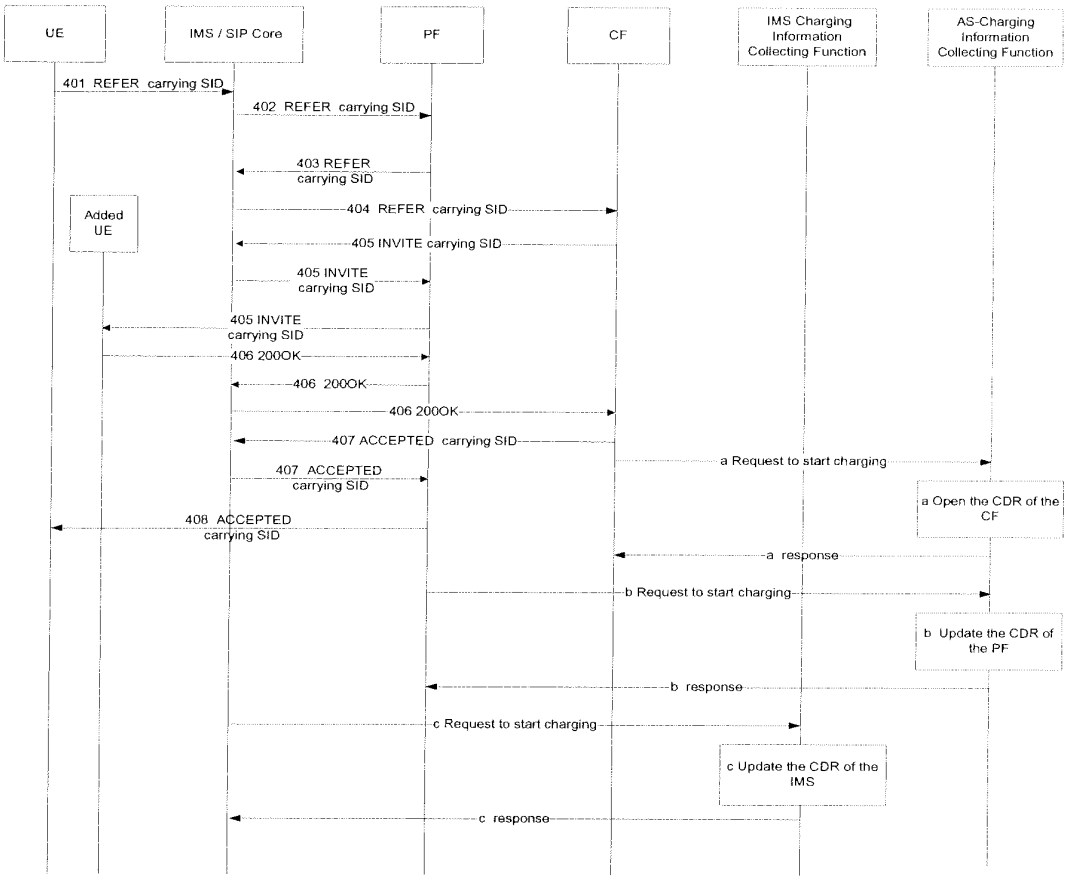

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
401 REFER carrying SID
402 REFER carrying SID
403 REFER carrying SID
404 REFER carrying SID
Added UE
405 INVITE carrying SID
405 INVITE carrying SID
405 INVITE carrying SID
406 200OK
406 200OK
406 200OK
407 ACCEPTED carrying SID
a Request to start charging
407 ACCEPTED carrying SID
a Open the CDR of the CF
408 ACCEPTED carrying SID
a response
b Request to start charging
b Update the CDR of the PF
b response
c Request to start charging
c Update the CDR of the IMS
c response

Fig. 4

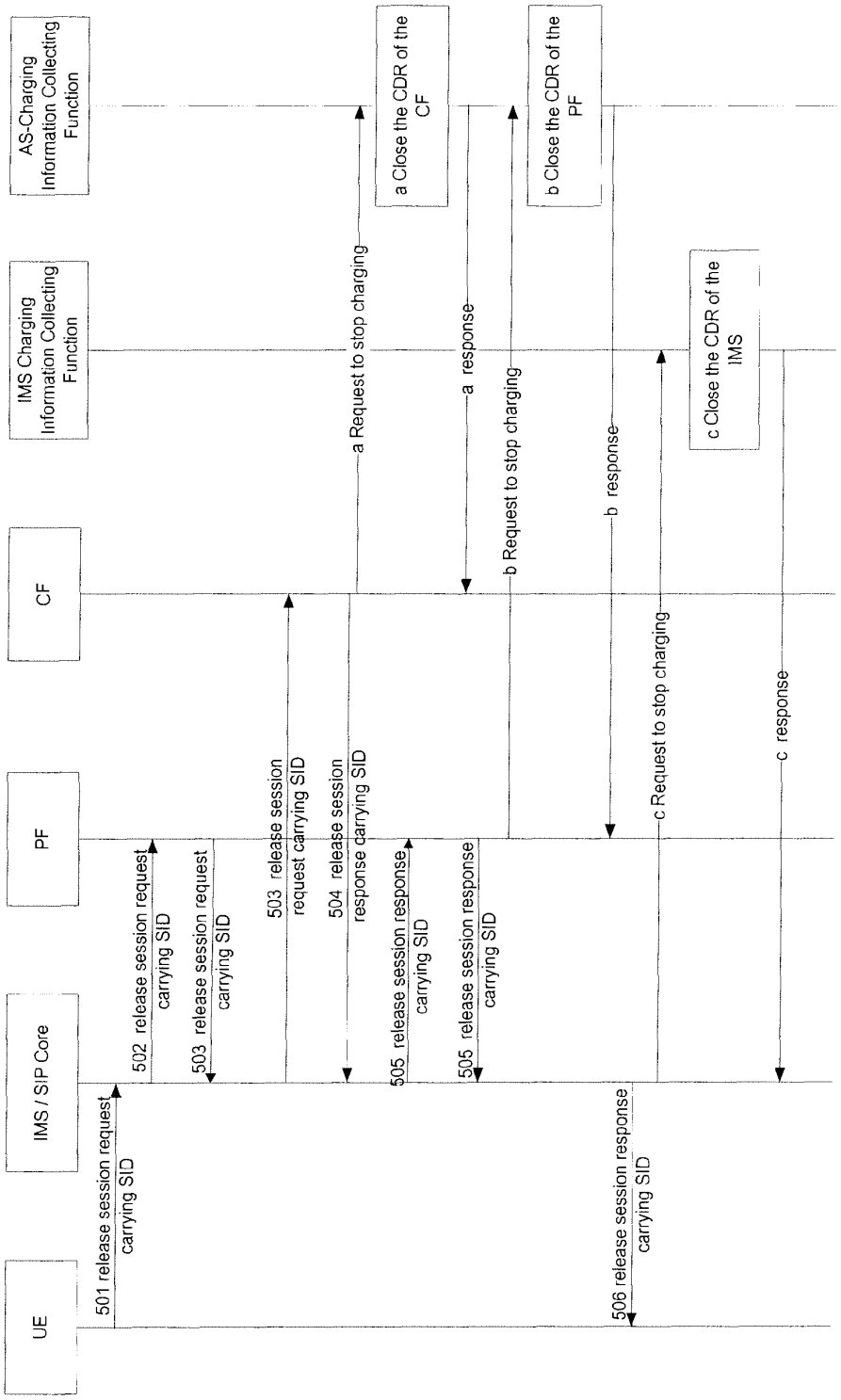

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
501 release session request carrying SID
502 release session request carrying SID
503 release session request carrying SID
503 release session request carrying SID
504 release session response carrying SID
505 release session response carrying SID
505 release session response carrying SID
506 release session response carrying SID
a Request to stop charging
a response
a Close the CDR of the CF
b Request to stop charging
b response
b Close the CDR of the PF
c Request to stop charging
c response
c Close the CDR of the IMS

Fig. 5

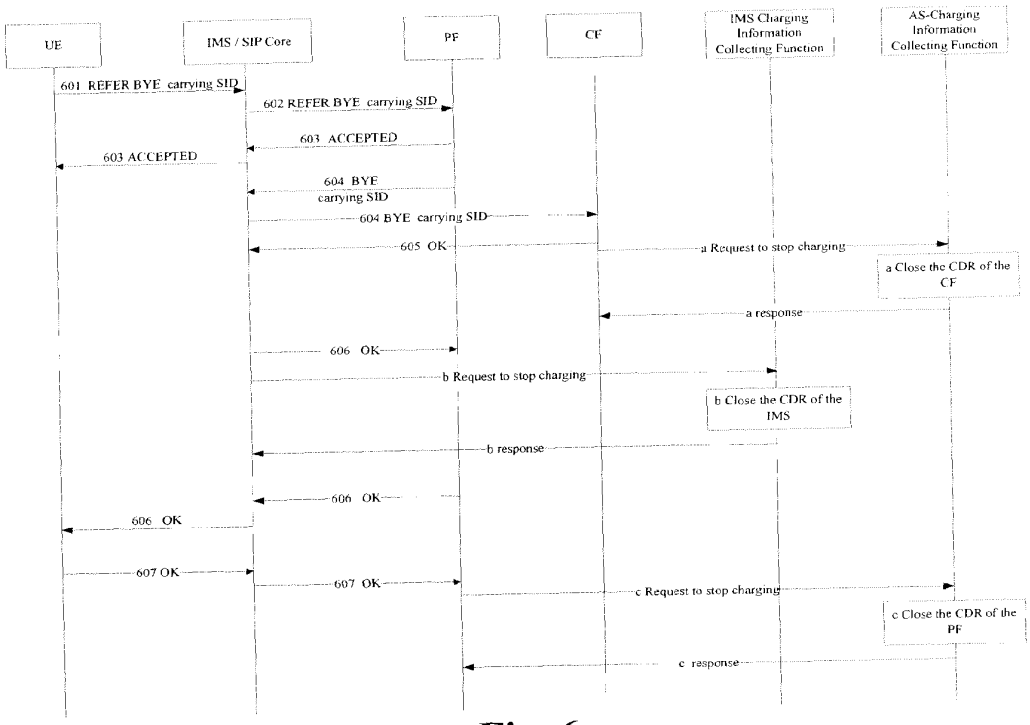

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
601 REFER BYE carrying SID
602 REFER BYE carrying SID
603 ACCEPTED
603 ACCEPTED
604 BYE carrying SID
604 BYE carrying SID
605 OK
a Request to stop charging
a Close the CDR of the CF
a response
606 OK
b Request to stop charging
b Close the CDR of the IMS
b response
606 OK
606 OK
607 OK
607 OK
c Request to stop charging
c Close the CDR of the PF
c response

Fig. 6

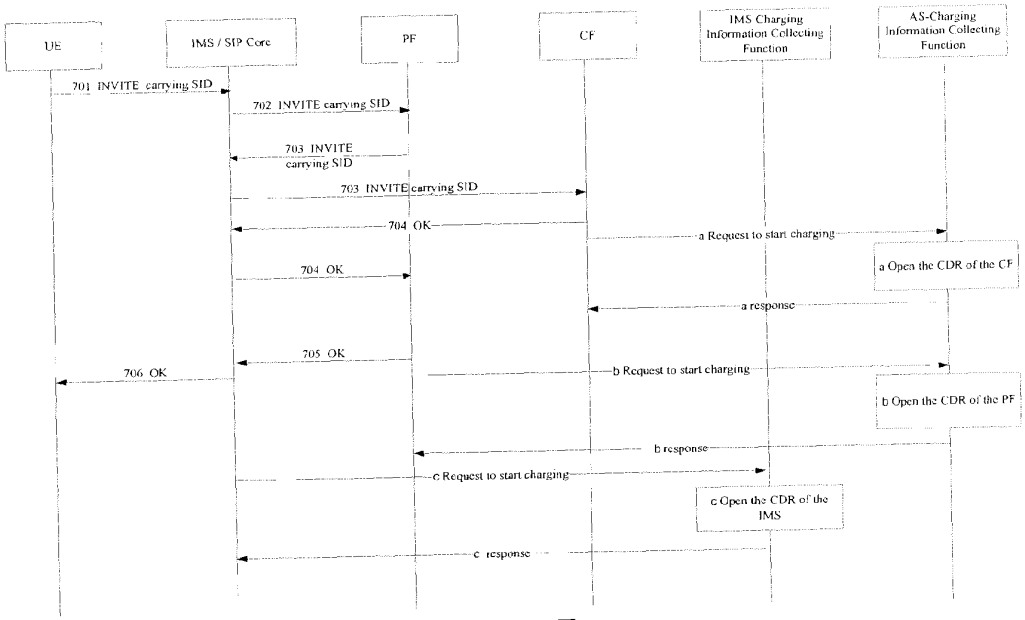

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
701 INVITE carrying SID
702 INVITE carrying SID
703 INVITE carrying SID
703 INVITE carrying SID
704 OK
a Request to start charging
a Open the CDR of the CF
704 OK
a response
705 OK
706 OK
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the IMS
c response

Fig. 7

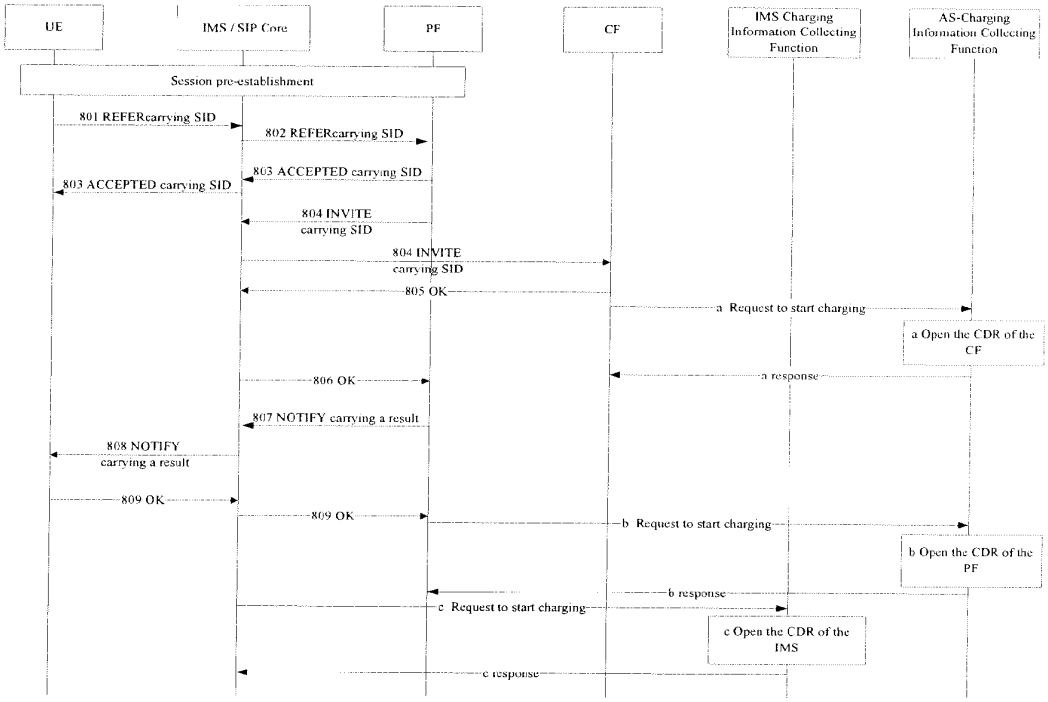

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
Session pre-establishment
801 REFERcarrying SID
802 REFERcarrying SID
803 ACCEPTED carrying SID
803 ACCEPTED carrying SID
804 INVITE carrying SID
804 INVITE carrying SID
805 OK
a Request to start charging
a Open the CDR of the CF
a response
806 OK
807 NOTIFY carrying a result
808 NOTIFY carrying a result
809 OK
809 OK
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the IMS
c response

Fig. 8

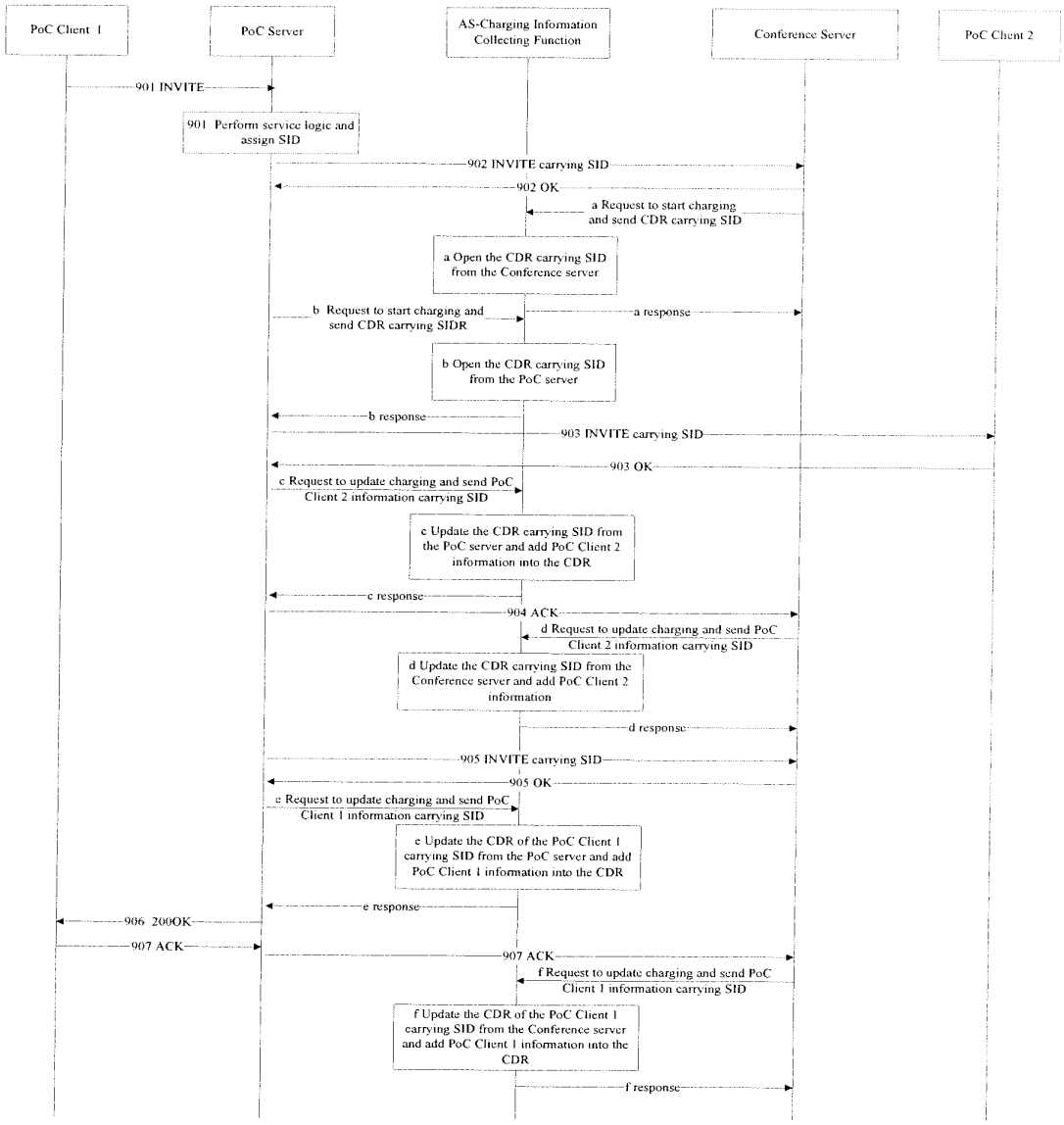

PoC Client 1
PoC Server
AS-Charging Information Collecting Function
Conference Server
PoC Client 2
901 INVITE
901 Perform service logic and assign SID
902 INVITE carrying SID
902 OK
a Request to start charging and send CDR carrying SID
a Open the CDR carrying SID from the Conference server
b Request to start charging and send CDR carrying SIDR
a response
b Open the CDR carrying SID from the PoC server
b response
903 INVITE carrying SID
903 OK
c Request to update charging and send PoC Client 2 information carrying SID
c Update the CDR carrying SID from the PoC server and add PoC Client 2 information into the CDR
c response
904 ACK
d Request to update charging and send PoC Client 2 information carrying SID
d Update the CDR carrying SID from the Conference server and add PoC Client 2 information
d response
905 INVITE carrying SID
905 OK
e Request to update charging and send PoC Client 1 information carrying SID
e Update the CDR of the PoC Client 1 carrying SID from the PoC server and add PoC Client 1 information into the CDR
e response
906 200OK
907 ACK
907 ACK
f Request to update charging and send PoC Client 1 information carrying SID
f Update the CDR of the PoC Client 1 carrying SID from the Conference server and add PoC Client 1 information into the CDR
f response

Fig. 9

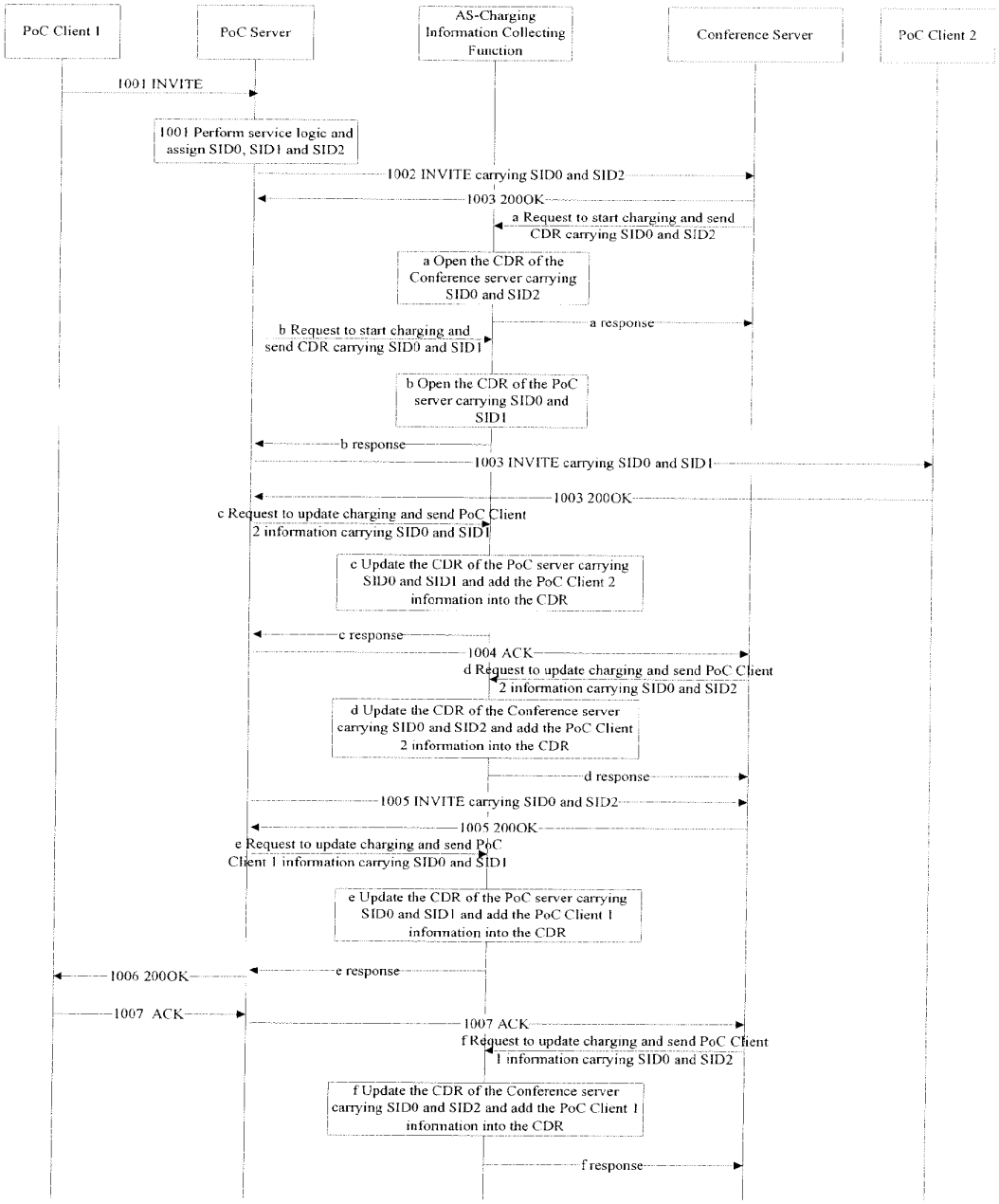

PoC Client 1
PoC Server
AS-Charging Information Collecting Function
Conference Server
PoC Client 2
1001 INVITE
1001 Perform service logic and assign SID0, SID1 and SID2
1002 INVITE carrying SID0 and SID2
1003 200OK
a Request to start charging and send CDR carrying SID0 and SID2
a Open the CDR of the Conference server carrying SID0 and SID2
a response
b Request to start charging and send CDR carrying SID0 and SID1
b Open the CDR of the PoC server carrying SID0 and SID1
b response
1003 INVITE carrying SID0 and SID1
1003 200OK
c Request to update charging and send PoC Client 2 information carrying SID0 and SID1
c Update the CDR of the PoC server carrying SID0 and SID1 and add the PoC Client 2 information into the CDR
c response
1004 ACK
d Request to update charging and send PoC Client 2 information carrying SID0 and SID2
d Update the CDR of the Conference server carrying SID0 and SID2 and add the PoC Client 2 information into the CDR
d response
1005 INVITE carrying SID0 and SID2
1005 200OK
e Request to update charging and send PoC Client 1 information carrying SID0 and SID1
e Update the CDR of the PoC server carrying SID0 and SID1 and add the PoC Client 1 information into the CDR
1006 200OK
e response
1007 ACK
1007 ACK
f Request to update charging and send PoC Client 1 information carrying SID0 and SID2
f Update the CDR of the Conference server carrying SID0 and SID2 and add the PoC Client 1 information into the CDR
f response

Fig. 10

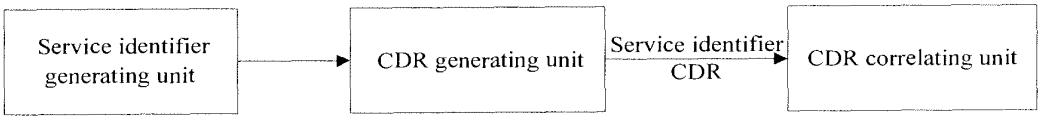

Service identifier generating unit
CDR generating unit
Service identifier
CDR
CDR correlating unit

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/001048

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/14(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC H04L 12/-; H04M 15/-; G06Q10/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT WPI EPODOC PAJ: service, charg+, money, bill, fee, cost, associat+, relat+, corresponding, flag, ID, identification, indicator, mark, identifier, identity, distribut+, assign, communicat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1267414A (NOKIA NETWORKS OY [FI]) 20 September 2000(20.09.2000) see claims 1,7and figure 3A	1-2, 15-16, 21, 24-25
A		3-14, 17-20, 22-23
A	CN1643888A (ERICSSON TELEFON AB L M [SE]) 20 July 2005(20.07.2005) see whole document	1-25
A	US2004255025A1 (RICAGNI GIUSEPPE [IT]) 16 December 2004(16.12.2004) see whole document	1-25

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 June 2007 (26.06.2007)	**12 Jul. 2007 (12.07.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer ZHAO,Weihua Telephone No. (86-10)62085024

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/001048

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1267414A	20.09.2000	FI981031A	15.01.1999
		WO9907108A2	11.02.1999
		AU8443398A	22.02.1999
		NO20000170A	13.03.2000
		EP1005737A2	07.06.2000
		US6240091B1	29.05.2001
		JP2001512926T	28.08.2001
CN1643888A	20.07.2005	EP1345402A1	17.09.2003
		WO03077528A1	18.09.2003
		AU2003210373A	22.09.2003
		EP1483893A1	08.12.2004
		JP2005520405T	07.07.2005
		US2005176404A1	11.08.2005
		AT311719T	15.12.2005
		DE60302559D	05.01.2006
		ES2252682T	16.05.2006
US2004255025A1	16.12.2004	None	

Form PCT/ISA /210 (patent family annex) (April 2007)

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) RALEP032C1
Application Number 14/082,040	Filed November 15, 2013
For Device-Assisted Services for Protecting Network Capacity	
Art Unit 3687	Examiner Rudy, Andrew J.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 700
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 505876.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 40013.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/James E. Harris/	December 1, 2016
Signature	Date
James E. Harris	903-201-6212
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	27671387
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	01-DEC-2016
Filing Date:	15-NOV-2013
Time Stamp:	19:02:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	3055.pdf	10370496 db66223e77b303b72c707b13a3bf1588e151bc42	no	20

Warnings:

Information:					
2	Non Patent Literature	3056.pdf	24448035 1be0315565d698a68e100c214709404b6b456701	no	85
Warnings:					
Information:					
3	Non Patent Literature	3057.pdf	1369098 4c887fb7b9fe8033365febea8b25f1275100a8cc	no	6
Warnings:					
Information:					
4	Non Patent Literature	3058.pdf	201178 0bdd69f18a3fd0292aa6cfb96076e8b9ccf310d5	no	4
Warnings:					
Information:					
5	Non Patent Literature	3059.pdf	984650 b3abbccb529e99d2c6635add88044e98852f41b7	no	20
Warnings:					
Information:					
6	Non Patent Literature	3060.pdf	2689325 2571b02a20421247b52538c8c218f2e3c8e6627f	no	336
Warnings:					
Information:					
7	Non Patent Literature	3061.pdf	868379 fd6eb4b7c7f13d4a778a1c80b64403253c0ae145	no	6
Warnings:					
Information:					
8	Non Patent Literature	3062.pdf	369346 69ebce04c86da14ea2d68c910afcd28d7fdf7e6d	no	2
Warnings:					
Information:					

9	Non Patent Literature	3063_Muntermann.pdf	400365 d732f8457b3d7b48773e6de195057acc9b18e201	no	36
Warnings:					
Information:					
10	Non Patent Literature	3064.pdf	944999 f03e4f3963258080c50536b168540d38a4b9eced	no	7
Warnings:					
Information:					
11	Non Patent Literature	3065_Fujitsu.pdf	158718 eee0e740dbe4d1b5db62cc52983988913c995e60	no	13
Warnings:					
Information:					
12	Non Patent Literature	3066.pdf	541057 5087e543fd3bcb9a11a377ef5db4f1c2ca88e720	no	15
Warnings:					
Information:					
13	Non Patent Literature	3067.pdf	2952523 18992a26a8917fcacb584769c943714abeee008d	no	14
Warnings:					
Information:					
14	Non Patent Literature	3068.pdf	749607 9e51f82ae6f112f5983929992b1d151a477fe5f9	no	5
Warnings:					
Information:					
15	Non Patent Literature	3069_OMA.pdf	469668 ea0fe39f7877344efbc29526eb097201b8731e98	no	21
Warnings:					
Information:					
			Total Files Size (in bytes):	47517444	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 06/01/2016

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
06/01/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com
krista@jacobseniplaw.com

Office Action Summary	Application No. 14/082,040	Applicant(s) RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-23* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-23 are pending. As noted from the November 27, 2015 communication, the November 17, 2015 Restriction requirement has been vacated.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 1-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed towards non-statutory subject matter because the claim(s) as a whole, considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea. The claim(s) is/are directed to a system/method which are clearly a machine/process under 35 USC 101 and thus are patent eligible concepts. However, one must further analyze the eligible concepts and determine whether the concepts, in this case, improve the functioning of the computer itself. Applicant's claim(s) is/are directed to the abstract idea of an apparatus that monitor network service usage activity. The additional elements or combination of

elements in the claim(s) amount(s) to no more than using a general purpose computing system, i.e. a processor and memory, to perform generic computer functions, e.g. provide instructions. It is noted that the method claim 22 requires no technology in addition to the recitations claimed. Viewed as a whole, these additional claim elements do not provide meaningful limitation(s) to transform the using computer technology, i.e. a processor and memory, to provide a common abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself. Therefore, the claims(s) are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. See, Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014).

The technology recited from the claims is deemed common knowledge technology and appears to add no additional technological improvement to the underlying invention. Viewed as a whole, these additional claim elements do not appear to provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself. Applicant's disclosure does not appear to lend support to anything other than the technology, e.g. a processor, memory, was commonly known. Therefore, the claims(s) are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. See, Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014).

Claim Rejections - 35 USC § 103

5. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-23 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Rados et al., US 8,484,568.

Rados discloses, e.g. Figs. 1-10 and related text, a network communication system comprising: a device e.g. 110 (see claim 18), memory, e.g. 210, 330, a processor, e.g. 200, the device configured to monitor e.g. Figs. 9, 10, the network for service usage activity, a traffic classification information, e.g. 720, and policy, e.g. 150.

Rados does not specifically disclose memory coupled to the processor and configured to provide the processor with instructions input of a user, nor a router.

Official Notice is taken that memory coupled to a processor and configured to provide the processor with instructions input of a user and a router has been common knowledge in the data monitoring art.

To have provided memory coupled to the processor and configured to provide the processor with instructions input of a user for Rados would have been obvious to one of ordinary skill in the art in view of Official Notice. Motivation for providing such would have been to incorporate common knowledge data aggregation used with telecommunication devices used in the data monitoring art.

It is noted Applicant's intended use claim language, e.g. claim 1, line 2, "configured to" does not further limit the positively recited claim language. As is, the claims that contain such language is deemed to be obvious variants of what Rados discloses and is configured to accomplish various policy intiatives for one of ordinary skill in the art in view of common knowledge.

7. Further pertinent references of interest are noted on the attached PTO-892.

8. Applicant's fourteen information disclosure statements (IDS's) have been reviewed. Note the attached IDS's.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/

Primary Examiner, Art Unit 3687

Notice of References Cited	Application/Control No. 14/082,040	Applicant(s)/Patent Under Reexamination RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,634,821 B2	01-2014	Raleigh; Gregory G.	H04L41/0806	455/419
*	B	US-8,503,455 B2	08-2013	Heikens; Heico	H04L47/10	370/395.21
*	C	US-8,484,568 B2	07-2013	Rados; Steven R.	H04L41/5032	715/745
*	D	US-8,023,425 B2	09-2011	Raleigh; Gregory G.	G06Q10/06375	370/252
*	E	US-7,987,496 B2	07-2011	Bryce; Duncan G.	H04L63/0227	726/1
*	F	US-7,849,477 B2	12-2010	Cristofalo; Michael	G06Q30/00	725/105
*	G	US-7,644,151 B2	01-2010	Jerrim; John	G06F21/552	709/212
*	H	US-7,457,870 B1	11-2008	Lownsbrough; Derek Leigh	H04L41/5058	709/217
*	I	US-7,395,244 B1	07-2008	Kingsford; Bryan	G06Q10/06	705/52
*	J	US-6,947,985 B2	09-2005	Hegli; Ronald Bjorn	H04L63/10	709/224
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAH, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAI et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2012-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	174	8064896		2011-11-22	BELL, Kris M. et al.	
	175	8160015		2012-04-17	RASHID, Mohammed H. et al.	
	176	8275830		2012-09-25	Raleigh, Gregory G.	
	177	7609700		2009-10-27	Ying, Wen-Ping et al.	
	178	8255515		2012-08-28	MELMAN, David et al.	
	179	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	180	7912056		2011-03-22	BRASSEM, Wayne	
	181	7920529		2011-04-05	MAHLER, Roger et al.	
	182	8184530		2012-05-22	SWAN, Tim L. et al.	
	183	8214536		2012-07-03	ZHAO, Wen	
	184	8213363		2012-07-03	Ying, Wen-Ping et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	185	8255689		2012-08-28	KIM, Eun Ah et al.	
	186	7746854		2010-06-29	AMBE, Shekhar et al.	
	187	7068600		2006-06-27	CAIN, Joseph Bibb	
	188	6876653		2005-04-05	AMBE, Shekhar et al.	
	189	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	190	7599288		2009-10-06	COLE, Raymond E. et al.	
	191	7546629		2009-06-09	ALBERT, Anthony et al.	
	192	7747730		2010-06-29	HARLOW, James D.	
	193	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	194	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	195	7283963		2007-10-16	FITZPATRICK, John E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	196	8271049		2012-09-18	SILVER, Andrew et al.	
	197	7644151		2010-01-05	JERRIM, John et al.	
	198	8291238		2012-10-16	GINTER, Karl L. et al.	
	199	8068824		2011-11-29	SHAN, Xueshan et al.	
	200	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	201	5283904		1994-02-01	CARSON, David G. et al.	
	202	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	203	8185152		2012-05-22	GOLDNER, Alla	
	204	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	205	7873344		2011-01-18	BOWSER, Robert et al.	
	206	7856226		2010-12-21	WONG, Ellis L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	207	7948952		2011-05-24	HURTTA, Tuija et al.	
	208	7957020		2011-06-07	MINE, Ryuta et al.	
	209	7346410		2008-03-18	UCHIYAMA, Kenji	
	210	7167078		2007-01-23	POURCHOT, Shawn C.	
	211	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	212	7970350		2011-06-28	SHEYNMAN, Arnold	
	213	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	214	8335161		2012-12-18	Foottit, Tom et al.	
	215	8315594		2012-11-20	Mauser, Edward Ronald et al.	
	216	8135388		2012-03-13	Gailloux, Michael A. et al.	
	217	6947723		2005-09-20	Gurnani, Roger et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	218	8353001		2013-01-08	Herrod, Allan	
	219	8195093		2013-06-05	Garrett, Darrin et al.	
	220	8036600		2011-10-11	Garrett, Darrin et al.	
	221	8301513		2012-10-30	Peng, Shih-Ta et al.	
	222	8230061		2012-07-24	Hassan, Amer A. et al.	
	223	8204794		2012-06-19	Peng, Shih-Ta et al.	
	224	8350700		2013-01-08	Fast, Raymond D. et al.	
	225	8204190		2012-06-19	Bang, Jung-Hee et al.	
	226	7865182		2011-01-04	Macaluso, Anthony G.	
	227	7962622		2011-06-14	Friend, John et al.	
	228	7583964		2009-09-01	Wong, Gregory A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	229	7565141		2009-06-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	240	7711848		2010-05-04	MAES, Stephane H.	
	241	6782412		2004-08-24	BROPHY, Kevin et al.	
	242	6081591		2000-06-27	SKOOG, Frederick H.	
	243	6064878		2000-05-16	DENKER, John Stewart et al.	
	244	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	245	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	246	8156206		2012-04-10	KILEY, Kevin J. et al.	
	247	8126722		2010-02-28	ROBB, Terence Alan et al.	
	248	8364089		2013-01-29	PHILLIPS, Derek	
	249	6754470		2004-06-22	Hendrickson, Keith et al.	
	250	8122128		2012-02-21	Burke, II, Robert M. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	251	8149823		2012-04-03	Turcan, Diane Brown et al.	
	252	8326359		2012-12-04	Kauffman, Donald C.	
	253	8131256		2012-03-06	MARTTI, Jyrki et al.	
	254	6381316		2002-04-30	JOYCE, Simon James et al.	
	255	7965983		2011-06-21	SWAN, Tim et al.	
	256	8284740		2012-10-09	O'CONNOR, Dennis M.	
	257	8116223		2012-02-14	TIAN, Dan et al.	
	258	6154738		2000-11-28	CALL, Charles Gainor	
	259	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	260	8306518		2012-11-06	GAILLOUX, Michael A.	
	261	8422988		2013-04-16	KESHAV, Srinivasan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	262	6035281		2000-03-07	Crosskey, James P. et al.	
	263	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	264	7760711		2010-07-20	Kung, Fen-Chung et al.	
	265	8000318		2011-08-16	Wiley, William L. et al.	
	266	8098579		2012-01-17	Ray, Amar N. et al.	
	267	8155670		2012-04-10	Fullam, Scott et al.	
	268	8374090		2013-02-12	Morrill, Robert J. et al.	
	269	7457265		2008-11-25	Julka, Vibhor et al.	
	270	7729326		2010-06-01	Sekhar, Ramesh	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7945945		2011-05-17	Graham, Richard et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	273	8059530		2011-11-15	Cole, Terry L.	
	274	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	275	8280354		2012-10-02	Smith, Christopher et al.	
	276	8331293		2012-12-11	Sood, Kapil	
	277	8019820		2011-09-13	Son, Giyeong et al.	
	278	8191116		2012-05-29	Gazzard, Daryl	
	279	6292828		2001-09-18	Williams, David L.	
	280	7043226		2006-05-09	Yamauchi, Toshiaki	
	281	7472189		2008-12-30	Mallya, Arvind R. et al.	
	282	7944948		2011-05-17	Chow, Albert T. et al.	
	283	7802724		2010-09-28	Nohr, Steven Paul	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	284	8155155		2012-04-10	Chow, Albert T. et al.	
	285	8447324		2013-05-21	Shuman, Mohammed Ataur et al.	
	286	8005009		2011-08-23	McKee, Neil et al.	
	287	7760861		2010-07-20	Croak, Marian et al.	
	288	8060463		2011-11-15	Spiegel, Joel R.	
	289	8224773		2012-07-17	Spiegel, Joel R.	
	290	8352980		2013-01-08	Howcroft, Jerald Robert	
	291	8386386		2013-02-26	Zhu, Kevin	
	292	8347362		2013-01-01	Cai, Yigang et al.	
	293	8340718		2012-12-25	Colonna, Massimo et al.	
	294	8385896		2013-02-26	Proctor Jr., James A. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	295	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	296	8279864		2012-10-02	Wood, Daniel M.	
	297	8271045		2012-09-18	Parolkar, Satish et al.	
	298	8233883		2012-07-31	De Froment, Eric	
	299	8224382		2012-07-17	Bultman, Michael J.	
	300	8184590		2012-05-22	Rosenblatt, Ariel	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	1	1463238	EP		2004-09-29	Alcatel		☐
	2	1739518	EP		2007-01-03	Research In Motion Limited		☐
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		☐
	6	2003014891	WO		2003-02-20	The Boeing Company		☐
	7	2003058880	WO		2003-07-17	Telia AB		☐
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		☐
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		☐
	10	2004095753	WO		2004-11-04	Motorola Inc.		☐
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		☐
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		☐
	14	2006077481	WO		2006-07-27	TrueContext Corporation		☐
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		☐
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		☐
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		☐
	18	2007018363	WO		2007-02-15	Upresto, Inc.		☐
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		☐
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		☐
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		☐
	22	2008017837	WO		2008-02-14	Symbian Software Limited		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		☐
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		☐
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		☐
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		☐
	27	2008099802	WO		2008-08-21	NEC Corporation		☐
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		☐
	29	2006120558	WO		2006-11-16	Nokia Corp.		☐
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		☐
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	34	2005008995	WO		2005-01-27	Starhub Ltd.		☐
	35	1998058505	WO		1998-12-23	Sonera Oy		☐
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS **Remove**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
	8	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
	9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm, December 20, 2008 [retrieved May 16, 2012]	☐
	10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
	11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
	12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
	13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
	14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
	15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
	16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐
	17	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐
	25	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐
	26	Ruckus Wireless – White Paper; "Smarter Wi-Fi for Mobile Operator Infrastructures" 2010	☐
	27	Accuris Networks, "The Business Value of Mobile Data Offload – a White Paper", 2010	☐
	28	Wireless Broadband Alliance, "WISPr 2.0, 08 April, 2010"; Doc. Ref. No.: WBA/RM/WISPr, Version 01.00	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	29	THURSTON, Richard, "WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi"; June 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/	☐
	30	Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 1) Technical Specification – Version 1.0.0"; 2012	☐
	31	Wi-Fi Alliance Hotspot 2.0 Technical Task Group, "Wi-Fi Certified Passpoint™ (Release 1) Deployment Guidelines – Version 1.0 – October 2012"	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	Raleigh, Gregory G.
Attorney Docket Number	RALEP032C1

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5774532	A	1998-06-30	Gottlieb et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040225898	A	2004-11-11	Frost, D. et al.	
	2	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	3	20060114832	A	2006-06-01	Hamilton et al.	
	4	20060156398	A	2006-07-13	Ross et al.	
	5	20060173959	A	2006-08-03	Mckelvie et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

	6	20070033194	A	2007-02-08	Srinivas et al.	
	7	20080070550	A	2008-03-20	Hose, David Alan	
	8	20080201266	A	2008-08-21	Chua et al.	
	9	20100284327	A	2010-11-11	Miklos, Gyorgy	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5633868	A	1997-05-27	Baldwin et al.	
	2	6061571	A	2000-05-09	Tamura, Hideo	
	3	6157636	A	2000-12-05	Voit et al.	
	4	6725256	B1	2004-04-20	Albal et al.	
	5	6751296	B1	2004-06-15	Albal et al.	
	6	6792461	B1	2004-09-14	Hericourt, Olivier	
	7	6934751	B2	2005-08-23	Jayapalan et al.	
	8	7027055	B2	2006-04-11	Anderson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7043225	B1	2006-05-09	Patel et al.	
	10	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	11	7174156	B1	2007-02-06	Mangal, Manish	
	12	7636626	B2	2009-12-22	Oesterling et al.	
	13	7680086	B2	2010-03-16	Eglin	
	14	7720206	B2	2010-05-18	Devolites et al.	
	15	7765294	B2	2010-07-27	Edwards et al.	
	16	7843831	B2	2010-11-30	Morrill et al.	
	17	8005913	B1	2011-08-23	Carlander, Carrie	
	18	8131858	B2	2012-03-06	Agulnik et al.	
	19	8160056	B2	2012-04-17	Van der Merwe et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	8180333	B1	2012-05-15	Wells et al.	
	21	8223655	B2	2012-07-17	Heinz et al.	
	22	8315198	B2	2012-11-20	Corneille et al.	
	23	8340678	B1	2012-12-25	Pandey, Vinod	
	24	8385199	B1	2013-02-26	Coward et al.	
	25	8520595	B2	2013-08-27	Yadav et al.	
	26	8523547	B2	2013-09-03	Pekrul, Merton W.	
	27	8621056	B2	2013-12-31	Coussemaeker et al.	
	28	8875042	B2	2014-10-28	LeJeune et al.	
	29	9135037	B1	2015-09-15	Petrescu-Prahova et al.	
	30	9172553	B2	2015-10-27	Dawes et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	9177455	B2	2015-11-03	Remer, David M.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030028623	A1	2003-02-06	Hennessey et al.	
	2	20050060525	A1	2005-03-17	Schwartz et al.	
	3	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	4	20070061800	A1	2007-03-15	Cheng et al.	
	5	20070255769	A1	2007-11-01	Agrawal et al.	
	6	20070299965	A1	2007-12-27	Nieh et al.	
	7	20080066181	A1	2008-03-13	Haveson et al.	
	8	20080126287	A1	2008-05-29	Cox et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	20080212751	A1	2008-09-04	Chung, Simon	
	10	20090203352	A1	2009-08-13	Fordon et al.	
	11	20100041365	A1	2010-02-18	Lott et al.	
	12	20100121744	A1	2010-05-13	Belz et al.	
	13	20140073291	A1	2014-03-13	Hildner et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2002045315	WO	A2	2002-06-06	Micromuse		
	2	2009008817	WO	A1	2009-01-15	Ericsson		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5131020	A	1992-07-14	Liebesny et al.	
	2	5325532	A	1994-06-28	Crosswy et al.	
	3	6640334	B	2003-10-28	Rasmussen, John H.	
	4	7409447	B	2008-08-05	Assadzadeh, Alireza	
	5	7614051	B	2009-11-03	Glaum et al.	
	6	7668612	B	2010-02-23	Okkonen, Harri	
	7	7756056	B2	2010-07-13	Kim et al.	
	8	8131281	B1	2012-03-06	Hildner et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	8160598	B2	2012-04-17	Savoor, Raghvendra	
	10	8223741	B	2012-07-17	Bartlett et al.	
	11	8370483	B	2013-02-05	Choong Jason et al.	
	12	8375136	B2	2013-02-12	Roman et al.	
	13	8396458	B	2013-03-12	Raleigh, Gregory G.	
	14	8645518	B	2014-02-04	David, Scott L.	
	15	8670334	B	2014-03-11	Keohane et al.	
	16	8676925	B	2014-03-18	Liu et al.	
	17	8693323		2014-04-08	McDysan, David E.	
	18	8725899	B	2014-05-13	Short et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040039792	A1	2004-02-26	Nakanishi, Tomoaki	
	2	20040137890	A1	2004-07-15	Kalke, Catherine	
	3	20040243992	A	2004-12-02	Gustafson et al.	
	4	20050075115	A1	2005-04-07	Corneille et al.	
	5	20050239447	A1	2005-10-27	Holzman et al.	
	6	20070143824	A1	2007-06-21	Shahbazi, Majid	
	7	20070213054	A1	2007-09-13	Han, Seung-Wook	
	8	20070226775	A	2007-09-27	Andreasen et al.	
	9	20070266422	A1	2007-11-15	Germano et al.	
	10	20080032715	A1	2008-02-07	Jia et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20080139210	A	2008-06-12	Gisby et al.		
	12	20080166993	A1	2008-07-10	Gautier et al.		
	13	20080293395	A1	2008-11-27	Mathews et al.		
	14	20090044185	A1	2009-02-12	Krivopaltsev, Eugene		
	15	20090163173	A1	2009-06-25	Williams, Timothy D.		
	16	20090254857	A	2009-10-08	Romine et al.		
	17	20100075666	A1	2010-03-25	Garner, Neil Robert		
	18	20100235329	A	2010-09-16	Koren et al.		

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101127988	CN	A	2008-02-20	ZTE Corporation		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8174970		2012-05-08	Adamczyk, Maria et al.	
	2	8165576		2012-04-24	Raju, Vishwanath et al.	
	3	8073721		2011-12-06	Lewis, Lundy	
	4	8032899		2011-10-04	Archer, Charles J. et al.	
	5	7974624		2011-07-05	Gallagher, Michael D. et al.	
	6	7907970		2011-03-15	Park, Vincent D. et al.	
	7	7778176		2010-08-17	Morford, Michael Robert	
	8	7725570		2010-05-25	Lewis, Lundy	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	7634388		2009-12-15	Archer, Charles J. et al.	
	10	7633438		2009-12-15	Tysowski, Piotr Konrad	
	11	7593417		2009-09-22	Wang, James et al.	
	12	7551922		2009-06-23	Roskowski, Steve et al.	
	13	7545782		2009-06-09	Rayment, Stephen G. et al.	
	14	7039037		2006-05-02	Wang, Jiwei R. et al.	
	15	6928280		2005-08-09	Xanthos, James et al.	
	16	6765925		2004-07-20	Sawyer, Wilson et al.	
	17	5889477		1999-03-30	Fastenrath, Ulrich	
	18	8332517		2012-12-11	Russell, Jesse E.	
	19	8315718		2012-11-20	Caffrey, Paul Oliver et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	20	8447980		2013-05-21	Godfrey, James A. et al.	
	21	8429403		2013-04-23	Moret, Eric et al.	
	22	8411587		2013-04-02	Curtis, William et al.	
	23	8396929		2013-03-12	Helfman, Nadav et al.	
	24	8363658		2013-01-29	Delker, Jason R. et al.	
	25	8265004		2012-09-11	Toutonghi, Michael J.	
	26	8233895		2012-07-31	Tysowski, Piotr Konrad	
	27	7685254		2010-03-23	Pandya, Ashish A.	
	28	7181017		2007-02-20	Nagel, Robert H. et al.	
	29	6965872		2005-11-15	Grdina, Jerome M.	
	30	8406427		2013-03-26	Chand, Naresh et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	31	8429409		2013-04-23	Wall, Jonathan et al.	
	32	8402540		2013-03-19	Kapoor, Harsh et al.	
	33	8135657		2013-03-13	Kapoor, Harsh et al.	
	34	8271992		2012-09-18	Chatley, Scott P. et al.	
	35	8315999		2012-11-20	Chatley, Scott P. et al.	
	36	8332375		2012-12-11	Chatley, Scott P. et al.	
	37	8468337		2013-06-18	Gaur, Santosh P. et al.	
	38	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	39	8352630		2013-01-08	Hart, Justin Scott	
	40	6640097		2003-10-28	Corrigan, Louis et al.	
	41	7039713		2006-05-02	Van Gunter, David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	42	5915008		1999-06-22	Dulman, Scott	
	43	8126476		2012-02-28	Vardi, Yosef et al.	
	44	8000276		2011-08-16	Scherzer, Shimon et al.	
	45	8358638		2013-01-22	Scherzer, Tamir et al.	
	46	8356336		2013-01-15	Johnston, Keith et al.	
	47	8307067		2012-11-06	Ryan, Nicholas M.	
	48	7286848		2007-10-23	Vireday, Richard P. et al.	
	49	7313237		2007-12-25	Bahl, Paramvir et al.	
	50	7444669		2008-10-28	Bahl, Paramvir et al.	
	51	7548976		2009-06-16	Bahl, Paramvir et al.	
	52	8027339		2011-09-27	Short, Joel E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	53	8095112		2012-01-10	Chow, Richard et al.	
	54	8369274		2013-02-05	Sawai, Ryo	
	55	7881697		2011-02-01	Baker, Matthew Donald et al.	
	56	7899438		2011-03-01	Baker, Matthew Donald et al.	
	57	7945238		2011-05-17	Baker, Matthew Donald et al.	
	58	8078140		2011-12-13	Baker, Matthew Donald et al.	
	59	8285249		2012-10-09	Baker, Matthew Donald et al.	
	60	7493659		2009-02-17	Wu, Handong et al.	
	61	7801985		2010-09-21	Pitkow, Jim et al.	
	62	8242959		2012-08-14	Mia, Rashidus S. et al.	
	63	8326319		2012-12-04	Davis, Richard W.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	64	8019886		2011-09-13	Harrang, Jeffrey Paul et al.	
	65	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	
	66	7139569		2006-11-21	Kato, Akira	
	67	7529204		2009-05-05	Bourlas, Yair et al.	
	68	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	69	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	70	8032409		2011-10-04	Mikurak, Michael G.	
	71	8045973		2011-10-25	Chambers, Michael D.	
	72	8116781		2012-02-14	Chen, Xixian et al.	
	73	8126396		2012-02-28	Bennett, James D.	
	74	8351898		2013-01-08	Raleigh, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	75	5630159		1997-05-13	Zancho, William F.	
	76	5633484		1997-05-27	Zancho, William F. et al.	
	77	5814798		1998-09-29	Zancho, William F.	
	78	7039403		2006-05-02	Wong, Gregory A.	
	79	7583964		2009-09-01	Wong, Gregory A.	
	80	7593730		2009-09-22	Khandelwal, Deepak et al.	
	81	7948953		2011-05-24	Melkote, Keerti G. et al.	
	82	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	83	8270972		2012-09-18	Otting, Marcia J. et al.	
	84	7929959		2011-04-19	DeAtley, Dallas et al.	
	85	7478420		2009-01-13	Wright, Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	86	7502672		2009-03-10	Kolls, H. Brock	
	87	7756757		2010-07-13	Oakes III, Charles Lee	
	88	7930446		2011-04-19	Kesselman, Alex et al.	
	89	8078163		2011-12-13	Lemond, Eric et al.	
	90	8068829		2011-11-29	Lemond, Eric et al.	
	91	8086497		2011-12-27	Oakes III, Charles Lee	
	92	8166040		2012-04-24	Brindisi, Richard G. et al.	
	93	6934249		2005-08-23	Bertin, Olivier et al.	
	94	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	95	8447607		2013-05-21	Weider, Chris et al.	
	96	8504729		2013-08-06	Pezzutti, David A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	97	8495227		2013-07-23	Kaminsky, David L. et al.	
	98	8472371		2013-06-25	Bari, Farooq et al.	
	99	8134954		2012-03-13	Godfrey, James A. et al.	
	100	7535880		2009-05-19	Hinman, Brian L. et al.	
	101	7499438		2009-03-03	Hinman, Brian L. et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	104	6654814		2003-11-25	Britton, Kathryn H. et al.	
	105	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	106	8325638		2012-12-04	Jin, Haipeng et al.	
	107	8116749		2012-02-14	Proctor Jr., James Arthur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	108	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	109	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	110	8150431		2012-04-03	Wolovitz, Lionel et al.	
	111	8483135		2013-07-09	Cai, Yigang et al.	
	112	6104700		2000-08-15	Haddock, Stephen R. et al.	
	113	8185127		2012-05-22	Cai, Zheng et al.	
	114	8521110		2013-08-27	Rofougaran, Ahmadreza	
	115	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7546460		2009-06-09	Maes, Stephane H.	
	118	7921463		2011-04-05	Sood, Kapil et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	119	7940751		2011-05-10	Hansen, Christopher J.	
	120	8122249		2012-02-21	Falk, Rainer et al.	
	121	8495360		2013-07-23	Falk, Rainer et al.	
	122	8520589		2013-08-27	Bhatt, Yogesh et al.	
	123	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	124	8379847		2013-02-19	Bell, Robert H. et al.	
	125	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	126	8296404		2012-10-23	McDysan, Dave et al.	
	127	8195163		2012-06-05	Gisby, Doug et al.	
	128	8437734		2013-05-07	Ray, Amar N. et al.	
	129	8280351		2012-10-02	Ahmed, Shahid et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	130	7460837		2008-12-02	Diener, Neil R.	
	131	7653394		2010-01-26	McMillin, Brian K.	
	132	8130793		2012-03-06	Edwards, Stephen K. et al.	
	133	8509082		2013-08-13	Heinz, John M. et al.	
	134	8526329		2013-09-03	Mahany, Ronald L. et al.	
	135	5983270		1999-11-09	Abraham, Dalen M. et al.	
	136	6598034		2003-07-22	Kloth, Axel K.	
	137	7032072		2006-04-18	Quinn, Michael J. et al.	
	138	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	139	7742406		2010-06-22	Muppala, Suresh	
	140	7953877		2011-05-31	Vemula, Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	141	7957381		2011-06-07	Clermidy, Fabien et al.	
	142	8031601		2011-10-04	Feroz, Azeem et al.	
	143	8255534		2012-08-28	Assadzadeh, Alireza	
	144	8489720		2013-06-16	Morford, Michael Robert et al.	
	145	7774323		2010-08-10	Helfman, Nadav	
	146	7043268		2006-05-09	Yukie, Satoru et al.	
	147	8391262		2013-03-05	Maki, Lasse et al.	
	148	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	149	8166554		2012-04-24	John, Pramod	
	150	7697540		2010-04-13	Haddad, Reda et al.	
	151	6748195		2004-06-08	Phillips, W. Garland	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	152	8583499		2013-11-12	De Judicibus, Dario et al.	
	153	8352360		2013-01-08	De Judicibus, Dario et al.	
	154	8463232		2013-06-11	Tuli, Amol et al.	
	155	7958029		2011-06-07	Bobich, Thomas et al.	
	156	7540408		2009-06-02	Levine, Judah Joseph et al.	
	157	7826427		2010-11-02	Sood, Kapil et al.	
	158	8185088		2012-05-22	Klein, Robert S. et al.	
	159	8548428		2013-10-01	Raleigh, Gregory G.	
	160	8483694		2013-07-09	Lewis, Allan D. et al.	
	161	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	162	8452858		2013-05-28	Wu, John et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	163	7610396		2009-10-27	Taglienti, Claudio et al.	
	164	7984511		2011-07-19	Kocher, Paul Carl et al.	
	165	7987510		2011-07-26	Kocher, Paul C. et al.	
	166	8571993		2013-10-29	Kocher, Paul C. et al.	
	167	8543265		2013-09-24	Ekhaguere, David E. et al.	
	168	8385975		2013-02-26	Forutanpour, Babak	
	169	6873988		2005-03-29	Hermann, Conrad K. et al.	
	170	7013469		2006-03-14	Smith, Adam W. et al.	
	171	7203169		2007-04-10	Okholm, Jon Eric et al.	
	172	7286834		2007-10-23	Walter, Edward	
	173	7555757		2009-06-30	Smith, Adam W. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	174	7574509		2009-08-11	Nixon, Mark J. et al.	
	175	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	176	7940685		2011-05-10	Breslau, Lee Michel et al.	
	177	8196199		2012-06-05	Hrastar, Scott E. et al.	
	178	8204505		2012-06-19	Jin, Haipeng et al.	
	179	8228818		2012-07-24	Chase, Christopher J. et al.	
	180	8320244		2012-11-27	Muqattash, Alaa et al.	
	181	8411691		2013-04-02	Aggarwal, Rahul	
	182	8461958		2013-06-11	Saenz, Jorge E. et al.	
	183	8484327		2013-07-09	Werner, Eran et al.	
	184	8522039		2013-08-27	Hyndman, Arn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	185	8544105		2013-09-24	Mclean, Ivan H. et al.	
	186	8571474		2013-10-29	Chavez, Timothy R. et al.	
	187	8194572		2012-06-05	Horvath, Robert et al.	
	188	8516552		2013-08-20	Raleigh, Gregory G.	
	189	8441955		2013-05-14	Wilkinson, Robert Todd et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		☐
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐
	5	1802839A	CN		2006-07-12	Motorola Inc.		☐
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6438575	B1	2002-08-20	Khan et al.	
	2	6578076	B1	2003-06-10	Putzolu, David Matthew	
	3	6697821	B2	2004-02-24	Ziff et al.	
	4	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	5	6982733	B1	2006-01-03	McNally et al.	
	6	6983370	B2	2006-01-03	Eaton et al.	
	7	7084775	B1	2006-08-01	Smith, Michael R.	
	8	7133695	B2	2006-11-07	Beyda, William J.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7222304	B2	2007-05-22	Beaton et al.	
	10	7260382	B1	2007-08-21	Lamb et al.	
	11	7271765	B2	2007-09-18	Stilp et al.	
	12	7318111	B2	2008-01-08	Zhao, Wen	
	13	7561899	B2	2009-07-14	Lee, Changseok	
	14	7627872	B2	2009-12-01	Hebeler et al.	
	15	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	16	7685530	B2	2010-03-23	Sherrard et al.	
	17	7760137	B2	2010-07-20	Martucci et al.	
	18	7843843	B1	2010-11-30	Papp III et al.	
	19	7925778	B1	2011-04-12	Wijnands et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	21	7937450	B2	2011-05-03	Janik, Craig M.	
	22	8010082	B2	2011-08-30	Sutaria et al.	
	23	8019846	B2	2011-09-13	Roelens et al.	
	24	8050705	B2	2011-11-01	Sicher et al.	
	25	8064418	B2	2011-11-22	Maki, Lasse	
	26	8086791	B2	2011-12-27	Caulkins, Jason	
	27	8103285	B2	2012-01-24	Kalhan, Amit	
	28	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
	29	8200200	B1	2012-06-12	Belser et al.	
	30	8229914	B2	2012-07-24	Ramer et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8233433	B2	2012-07-31	Kalhan, Amit	
	32	8249601	B2	2012-08-21	Emberson et al.	
	33	8259692	B2	2012-09-04	Bajko, Gabor	
	34	8406736	B2	2013-03-26	Das et al.	
	35	8489110	B2	2013-07-16	Frank et al.	
	36	8495181	B2	2013-07-23	Venkatraman et al.	
	37	8514927	B2	2013-08-20	Sundararajan et al.	
	38	8522249	B2	2013-08-27	Beaule, Stephane	
	39	8532610	B2	2013-09-10	Manning Cassett et al.	
	40	8571598	B2	2013-10-29	Valavi, John J.	
	41	8631428	B2	2014-01-14	Scott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8634425	B2	2014-01-21	Gorti et al.	
	43	8701015	B2	2014-04-15	Bonnat, Pierre	
	44	8739035	B2	2014-05-27	Trethewey, Jim	
	45	8804517	B2	2014-08-12	Oerton, Kevin John	
	46	8825109	B2	2014-09-02	Montemurro et al.	
	47	8831561	B2	2014-09-09	Sutaria et al.	
	48	8880047	B2	2014-11-04	Konicek et al.	
	49	8930238	B2	2015-01-06	Coffman et al.	
	50	8949597	B1	2015-02-03	Reeves et al.	
	51	8977284	B2	2015-03-10	Reed, Mark J.	
	52	9014973	B2	2015-04-21	Ruckart, John	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040259534	A1	2004-12-23	Chaudhari et al.	
	2	20060072451	A1	2006-04-06	Ross, Alan D.	
	3	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	4	20070192460	A1	2007-08-16	Choi et al.	
	5	20070293191	A1	2007-12-20	Mir et al.	
	6	20070294410	A1	2007-12-20	Pandya et al.	
	7	20080050715	A1	2008-02-28	Golczewski et al.	
	8	20080080457	A1	2008-04-03	Cole, Terry L.	
	9	20080282319	A1	2008-11-13	Fontijn et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	10	20090049518	A1	2009-02-19	Roman et al.	
	11	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	12	20100151866	A1	2010-06-17	Karpov et al.	
	13	20100248719	A1	2010-09-30	Scholaert, Hugh	
	14	20110145920	A1	2011-06-16	Mahaffey et al.	
	15	20130326356	A9	2013-12-05	Zheng et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	2	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	3	101815275A	CN	A	2010-08-25	Yang, Liu		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	4	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐
	5	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	6	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	2	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐
	3	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	4	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	5	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	2	7320029	B2	2008-01-15	Rinne et al.	
	3	7539132	B2	2009-05-26	Werner et al.	
	4	7805606	B2	2010-09-28	Birger et al.	
	5	8175574	B1	2012-05-08	Panda et al.	
	6	8180881	B2	2012-05-15	Seo et al.	
	7	8191124	B2	2012-05-29	Wynn et al.	
	8	8275415	B2	2012-09-25	Huslak, Nicholas S.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8300575	B2	2012-10-30	Willars, Per	
	10	8315593	B2	2012-11-20	Gallant et al.	
	11	8347378	B2	2013-01-01	Merkin et al.	
	12	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	13	8527410	B2	2013-09-03	Markki et al.	
	14	8539561	B2	2013-09-17	Gupta et al.	
	15	8554876	B2	2013-10-08	Winsor, Gerald W.	
	16	8666395	B2	2014-03-04	Silver, Andrew	
	17	8391834	B2	2013-03-05	Raleigh, Gregory G.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	1	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	2	20040170191	A	2004-09-02	Guo et al.	
	3	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	4	20050186948	A	2005-08-25	Gallagher et al.	
	5	20070147317	A	2007-06-28	Smith et al.	
	6	20080025230	A	2008-01-31	Patel et al.	
	7	20080056273	A	2008-03-06	Pelletier et al.	
	8	20080270212	A	2008-10-30	Blight et al.	
	9	20100030890	A	2010-02-04	Dutta et al.	
	10	20110110309	A	2011-05-12	Bennett, James D.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add
FOREIGN PATENT DOCUMENTS						Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1310401	CN	A	2001-08-29	Wang, Di Xing		☐
	2	2466831	EP	A1	2012-06-20	Openet Telecom Ltd. - Mcnamee et al.		☐
	3	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
	4	1999027723	WO	A1	1999-06-03	Telefonaktiebolaget LM Ericsson		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20120029718		2012-02-02	DAVIS, Edward L.	
	212	20110241624		2011-10-06	PARK, Jun-seok et al.	
	213	20090307746		2009-12-10	DI, Jinwen et al.	
	214	20050009499		2005-01-13	KOSTER, Karl	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	215	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	216	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	217	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	218	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	219	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	220	20080313730		2008-12-18	Iftimie, Sorin et al.	
	221	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	222	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	223	20080240373		2008-10-02	WILHELM, Robert D.	
	224	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	225	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	226	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	227	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	228	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	229	20090172077		2009-07-02	ROXBURGH, David et al.	
	230	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	231	20030171112		2003-09-11	Lupper, Alfred et al.	
	232	20070300252		2007-12-27	Acharya, Swarup et al.	
	233	20050007993		2005-01-13	Chambers, Mahdi et al.	
	234	20020164983		2002-11-07	Raviv, Li-On et al.	
	235	20070280453		2007-12-06	Kelley, Sean S.	
	236	20100241544		2010-09-23	Benson, Dan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	237	20090157792		2009-06-18	Fiatal, Trevor	
	238	20070109983		2007-05-17	Shankar, Rohit et al.	
	239	20020049074		2002-04-25	Eisinger, Bernd et al.	
	240	20020161601		2002-10-31	Nauer, Bernhard et al.	
	241	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	242	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	243	20010048738		2001-12-06	Baniak, Paul G. et al.	
	244	20070033197		2007-02-08	Scherzer, Shimon et al.	
	245	20110013569		2011-01-20	Scherzer, Shimon et al.	
	246	20110159818		2011-06-30	Scherzer, Shimon et al.	
	247	20120020296		2012-01-26	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	248	20120196644		2012-08-02	Scherzer, Shimon et al.	
	249	20120238287		2012-09-20	Scherzer, Shimon	
	250	20130058274		2013-03-07	Scherzer, Shimon et al.	
	251	20130084835		2013-04-04	Scherzer, Shimon et al.	
	252	20090005000		2009-01-01	Baker, Matthew et al.	
	253	20090006116		2009-01-01	Baker, Matthew et al.	
	254	20090006200		2009-01-01	Baker, Matthew et al.	
	255	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	256	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	257	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	258	20130065555		2013-03-14	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	259	20120155296		2012-06-21	Kashanian, Nematolah	
	260	20120330792		2012-12-27	Kashanian, Nematolah	
	261	20130030960		2013-01-31	Kashanian, Nematolah	
	262	20130095787		2013-04-18	Kashanian, Nematolah	
	263	20130117140		2013-05-09	Kashanian, Nematolah	
	264	20130183937		2013-07-18	Neal, Daniel John et al.	
	265	20060135144		2006-06-22	Jothipragasam, Premkumar	
	266	20080089295		2008-04-17	Keeler, James D. et al.	
	267	20080022354		2008-01-24	Grewal, Karanvir et al.	
	268	20040102182		2004-05-27	Reith, Lothar et al.	
	269	20030233332		2003-12-18	Keeler, James D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	270	20080250053		2008-10-09	Aaltonen, Janne et al.	
	271	20110195700		2011-08-11	Kukuchka, Robert et al.	
	272	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	273	20130144789		2013-06-06	Aaltonen, Janne et al.	
	274	20100131584		2010-05-27	Johnson, William J.	
	275	20100080202		2010-04-01	Hanson, Mark	
	276	20070147324		2007-06-28	McGary, Faith	
	277	20130024914		2013-01-24	Ahmed, Shahid et al.	
	278	20130103376		2013-04-25	Gaddam, Venkat et al.	
	279	20130111572		2013-05-02	Gaddam, Venkat et al.	
	280	20130117382		2013-05-09	Gaddam, Venkat et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	281	20130149994		2013-06-13	Gaddam, Venkat et al.	
	282	20070168499		2007-07-19	Chu, Jing-Long	
	283	20070025301		2007-02-01	Petersson, Justus et al.	
	284	20070140145		2007-06-21	Kumar, Surender et al.	
	285	20080120129		2008-05-22	Seubert, Michael et al.	
	286	20060174035		2006-08-03	Tufail, Mudassir	
	287	20110264923		2011-10-27	Kocher, Paul C. et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6119933	A	2000-09-19	Wong et al.	
	2	7149229	B1	2006-12-12	Leung, Kent K.	
	3	7242668	B2	2007-07-10	Kan et al.	
	4	8095640	B2	2012-01-10	Guingo et al.	
	5	8347104	B2	2013-01-01	Pathiyal, Krishna K.	
	6	8694772	B2	2014-04-08	Kao et al.	
	7	8705361	B2	2014-04-22	Venkataraman et al.	
	8	8719423	B2	2014-05-06	Wyld	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	8780857	B2	2014-07-15	Balasubramanian et al.	
	10	8811991	B2	2014-08-19	Jain et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050135264	A1	2005-06-23	Popoff et al.	
	2	20050245241	A1	2005-11-03	Durand et al.	
	3	20070165630	A1	2007-07-19	Rasanen et al.	
	4	20080125079	A1	2008-05-29	O'Neil et al.	
	5	20100287599	A1	2010-11-11	He et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1	1503548	EP	A1	2005-02-02	FG Microtec GmbH		☐
	2	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		☐
	3	2008301121	JP	A	2008-12-11	Kyocera Corp.		☐
	4	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		☐
	5	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐
	6	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	7	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.		☐
	8	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS **Remove**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5974439	A	1999-10-26	Bollella, Gregory	
	2	6038540	A	2000-03-14	Krist et al.	
	3	6058434	A	2000-05-02	Wilt et al.	
	4	6125391	A	2000-09-26	Meltzer et al.	
	5	6393014	B1	2002-05-21	Daly et al.	
	6	6397259	B1	2002-05-28	Lincke et al.	
	7	6735206	B1	2004-05-11	Oki et al.	
	8	6748437	B1	2004-06-08	Mankude et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6882718	B1	2005-04-19	Smith, Benjamin V.	
	10	7017189	B1	2006-03-21	DeMello et al.	
	11	7024460	B2	2006-04-04	Koopmas et al.	
	12	7047276	B2	2006-05-16	Liu et al.	
	13	7058022	B1	2006-06-06	Carolan et al.	
	14	7149521	B2	2006-12-12	Sundar et al.	
	15	7162237	B1	2007-01-09	Silver et al.	
	16	7200112	B2	2007-04-03	Sundar et al.	
	17	7248570	B2	2007-07-24	Bahl et al.	
	18	7266371	B1	2007-09-04	Amin et al.	
	19	7366654	B2	2008-04-29	Moore, Robert C.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7391724	B2	2008-06-24	Alakoski et al.	
	21	7395244	B1	2008-07-01	Kingsford, Bryan	
	22	7411930	B2	2008-08-12	Montojo et al.	
	23	7454191	B2	2008-11-18	Dawson et al.	
	24	7508799	B2	2009-03-24	Sumner et al.	
	25	7512128	B2	2009-03-31	DiMambro et al.	
	26	7554983	B1	2009-06-30	Muppala, Suresh	
	27	7564799	B2	2009-07-21	Holland et al.	
	28	7627767	B2	2009-12-01	Sherman et al.	
	29	7676673	B2	2010-03-09	Weller et al.	
	30	7817615	B1	2010-10-19	Breau et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7844034	B1	2010-11-30	Oh et al.	
	32	7849161	B2	2010-12-07	Koch et al.	
	33	7849477	B2	2010-12-07	Cristofalo et al.	
	34	7860088	B2	2010-12-28	Lioy, Marcello	
	35	7889384	B2	2011-02-15	Armentrout et al.	
	36	7894431	B2	2011-02-22	Goring et al.	
	37	7899039	B2	2011-03-01	Andreasen et al.	
	38	7966405	B2	2011-06-21	Sundaresan et al.	
	39	7978686	B2	2011-07-12	Goyal et al.	
	40	7987496	B2	2011-07-26	Bryce et al.	
	41	8032168	B2	2011-10-04	Ikaheimo, Jorma	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8073427	B2	2011-12-06	Koch et al.	
	43	8104080	B2	2012-01-24	Burns et al.	
	44	8131840	B1	2012-03-06	Denker, Richard E.	
	45	8150394	B2	2012-04-03	Bianconi et al.	
	46	8190122	B1	2012-05-29	Alexander et al.	
	47	8385964	B2	2013-02-26	Haney, Richard D.	
	48	8407763	B2	2013-03-26	Weller et al.	
	49	8484568	B2	2013-07-09	Rados et al.	
	50	8503455	B2	2013-08-06	Heikens, Heico	
	51	8504032	B2	2013-08-06	Lott et al.	
	52	8504687	B2	2013-08-06	Maffione et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8504690	B2	2013-08-06	Shah et al.	
	54	8522337	B2	2013-08-27	Adusumilli et al.	
	55	8527662	B2	2013-09-03	Biswas et al.	
	56	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	57	8644813	B1	2014-02-04	Gailloux et al.	
	58	8667542	B1	2014-03-04	Bertz et al.	
	59	8793304	B2	2014-07-29	Lu et al.	
	60	8812525	B1	2014-08-19	Taylor III, Buford Leonard	
	61	8863111	B2	2014-10-14	Selitser et al.	
	62	8948726	B2	2015-02-03	Smith et al.	
	63	8966018	B2	2015-02-24	Bugwadia et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	9002342	B2	2015-04-07	Tenhunen et al.	
	65	RE44412		2013-08-06	Naqvi et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030134650	A1	2003-07-17	Sundar et al.	
	2	20030159030	A1	2003-08-21	Evans, Junius A.	
	3	20040127208	A1	2004-07-01	Nair et al.	
	4	20040260766	A1	2004-12-23	Barros et al.	
	5	20050041617	A1	2005-02-24	Huotari et al.	
	6	20050096024	A1	2005-05-05	Bicker et al.	
	7	20060075506	A1	2006-04-06	Sanda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	8	20060095517	A1	2006-05-04	O'Connor et al.	
	9	20060126562	A1	2006-06-15	Liu, Huitao	
	10	20060277590	A1	2006-12-07	Limont et al.	
	11	20060291419	A1	2006-12-28	McConnell et al.	
	12	20070257767	A1	2007-11-08	Beeson, Curt	
	13	20080018494	A1	2008-01-24	Waite et al.	
	14	20080034063	A1	2008-02-07	Yee, Robert	
	15	20090036111	A1	2009-02-05	Danford et al.	
	16	20120108225	A1	2012-05-03	Luna et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5572528	A	1996-11-05	Shuen, Pauline	
	2	5754953	A	1998-05-19	Briancon et al.	
	3	6628934	A	2003-09-30	Rosenberg et al.	
	4	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	5	6757717	B1	2004-06-29	Goldstein, Leonid	
	6	6901440	B1	2005-05-31	Bimm et al.	
	7	6970692	B2	2005-11-29	Tysor, Arthur James	
	8	7007295	B1	2006-02-28	Rose et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7203752	B2	2007-04-10	Rice et al.	
	10	7222190	B2	2007-05-22	Klinker et al.	
	11	7224968	B2	2007-05-29	Dobson et al.	
	12	7379731	B2	2008-05-27	Natsuno et al.	
	13	7457870	B1	2008-11-25	Lownsbrough et al.	
	14	7515926	B2	2009-04-07	Bu et al.	
	15	7536695	B2	2009-05-19	Alam et al.	
	16	7586871	B2	2009-09-08	Hamilton et al.	
	17	7752330	B2	2010-07-06	Olsen et al.	
	18	7792257	B1	2010-09-07	Vanier et al.	
	19	7801783	B2	2010-09-21	Kende et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7865187	B2	2011-01-04	Ramer et al.	
	21	7933274	B2	2011-04-26	Verma et al.	
	22	8005726	B1	2011-08-23	Bao, Yulin	
	23	8050690	B2	2011-11-01	Neeraj, Chawla	
	24	8086398	B2	2011-12-27	Sanchez et al.	
	25	8107953	B2	2012-01-31	Zimmerman et al.	
	26	8112435	B2	2012-02-07	Epstein et al.	
	27	8174378	B2	2012-05-08	Richman et al.	
	28	8195661	B2	2012-06-05	Kalavade, Asawaree	
	29	8200163	B2	2012-06-12	Hoffman, George E.	
	30	8200818	B2	2012-06-12	Freund et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8208788	B2	2012-06-26	Ando et al.	
	32	8254880	B2	2012-08-28	Aaltonen et al.	
	33	8270955	B2	2012-09-18	Ramer et al.	
	34	8326828	B2	2012-12-04	Zhou et al.	
	35	8331223	B2	2012-12-11	Hill et al.	
	36	8358975	B2	2013-01-22	Bahl et al.	
	37	8533775	B2	2013-09-10	Alcorn et al.	
	38	8538394	B2	2013-09-17	Zimmerman et al.	
	39	8538458	B2	2013-09-17	Haney, Richard D.	
	40	8565746	B2	2013-10-22	Hoffman, George E.	
	41	8571501	B2	2013-10-29	Miller et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	43	8713535	B2	2014-04-29	Malhotra et al.	
	44	8713641	B1	2014-04-29	Pagan et al.	
	45	8730842	B2	2014-05-20	Collins et al.	
	46	8732808	B2	2014-05-20	Sewall et al.	
	47	8761711	B2	2014-06-24	Grignani et al.	
	48	9049010		2015-06-02	Jueneman et al.	
	49	6445777		2002-09-03	Clark, Curtis	
	50	7039027		2006-05-02	Bridgelall, Raj	
	51	7990049		2011-08-02	Shioya, Shunsuke	
	52	8180886		2012-05-15	Overcash et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8339991		2012-12-25	Biswas et al.	
	54	8630314		2014-01-14	York, Frederick John	
	55	8868725		2014-10-21	Samba, Augustine S.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020154751	A1	2002-10-24	Thompson et al.	
	2	20030084321	A1	2003-05-01	Tarquini et al.	
	3	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	4	20060136882	A1	2006-06-22	Noonan et al.	
	5	20060143066	A1	2006-06-29	Calabria	
	6	20070073899	A1	2007-03-29	Judge et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	7	20070174490	A1	2007-07-26	Choi et al.	
	8	20070234402	A1	2007-10-04	Khosravi et al.	
	9	20090048913	A1	2009-02-19	Shenfield et al.	
	10	20090181662	A1	2009-07-16	Fleischman et al.	
	11	20120166604	A1	2012-06-28	Fortier et al.	
	12	20020191573		2002-12-19	Whitehill et al.	
	13	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	14	20090070379		2009-03-12	Rappaport, Theodore R.	
	15	20100318652		2010-12-16	Samba, Augustine S.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐
	2	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	3	1850575	EP	A1	2007-10-31	Research In Motion		☐
	4	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐
	5	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	6	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	3	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	4	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	5	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
	6	Loopt User Guide, metroPCS, 7/17/2008	☐
	7	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
	8	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
	9	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	11	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Gart, Matthew S.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7805140	B2	2010-09-28	Friday et al.	
	2	8605691	B2	2013-12-10	Soomro et al.	
	3	8655357	B1	2014-02-18	Gazzard et al.	
	4	8706863		2014-04-22	Fadell, Anthony	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020188732	A1	2002-12-12	Buckman et al.	
	2	20080010379	A	2008-01-10	Zhao, Hang	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Gart, Matthew S.
	Attorney Docket Number	RALEP032C1

	3	20080034419	A	2008-02-07	Mullick et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1878160	CN	A	2006-12-13	Jiang, Yong		☐
	2	2011149532	WO	A1	2011-12-01	Raleigh et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	14/082,040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

SEARCHED			
Class	Subclass	Date	Examiner
709	203,217, 220,223, 224	5/26/2016	AJR
H 04L	29/08072	5/26/2016	AJR
H 04L	29/06	5/26/2016	AJR
H 04L	43/00	5/26/2016	AJR
H 04L	12/2602	5/26/2016	AJR
H 04L	41/22	5/26/2016	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	5/26/2016	AJR
Inventor name search conducted.	5/26/2016	AJR

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6885997	B1	2005-04-26	Roberts, David T.	
	2	7720464	B2	2010-05-18	Batta, Puneet	
	3	7797060	B2	2010-09-14	Grgic et al.	
	4	7853255	B2	2010-12-14	Karaoguz et al.	
	5	7930327	B2	2011-04-19	Craft David et al.	
	6	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
	7	8095124	B2	2012-01-10	Balia, Hinal K.	
	8	8229394	B2	2012-07-24	Karlberg, Johan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8264965	B2	2012-09-11	Dolganow et al.	
	10	8442015	B2	2013-05-14	Behzad et al.	
	11	8495700	B2	2013-07-23	Shahbazi, Majid	
	12	8528068	B1	2013-09-03	Weglein et al.	
	13	8548427	B2	2013-10-01	Chow et al.	
	14	8566236	B2	2013-10-22	Busch, James David	
	15	8572117	B2	2013-10-29	Rappaport, Theodore S.	
	16	8589955	B2	2013-11-19	Roundtree et al.	
	17	8601125	B2	2013-12-03	Huang et al.	
	18	8635164	B2	2014-01-21	Rosenhaft et al.	
	19	8660853	B2	2014-02-25	Robb et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030188006	A	2003-10-02	Bard, Steven R.	
	2	20030188117	A	2003-10-02	Yoshino et al.	
	3	20040255145	A	2004-12-16	Chow, Jerry	
	4	20050055595	A	2005-03-10	Frazer et al.	
	5	20060160536	A	2006-07-20	Chou, Joey	
	6	20060168128	A	2006-07-27	Sistla et al.	
	7	20070259656	A	2007-11-08	Jeong, Jong Woo	
	8	20080263348	A	2008-10-23	Zaltsman et al.	
	9	20080313315	A	2008-12-18	Karaoguz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	10	20090282127	A	2009-11-12	Leblanc et al.	
	11	20100167696	A	2010-07-01	Smith, Christopher David et al.	
	12	20110019574	A	2011-01-27	Malomsoky et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101123553A	CN		2007-09-11	Southeast University		☐
	2	1937511A	CN		2007-03-28	ZTE		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7809351	B1	2010-10-05	Panda et al.	
	2	8346210	B2	2013-01-01	Balsan et al.	
	3	8355696	B1	2013-01-15	Olding et al.	
	4	8488597		2013-07-16	Nie et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050250536	A1	2005-11-10	Deng et al.	
	2	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	20060035631	A1	2006-02-16	White et al.	
	4	20060206709	A1	2006-09-14	Labrou et al.	
	5	20070060200	A1	2007-03-15	Boris et al.	
	6	20090046707	A1	2009-02-19	Smires et al.	
	7	20100311402	A1	2010-12-09	Srinivasan et al.	
	8	20110277019	A1	2011-11-10	Pritchard Jr., John Russell	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	05/26/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5633868	A	1997-05-27	Baldwin et al.	
	2	6061571	A	2000-05-09	Tamura, Hideo	
	3	6157636	A	2000-12-05	Voit et al.	
	4	6725256	B1	2004-04-20	Albal et al.	
	5	6751296	B1	2004-06-15	Albal et al.	
	6	6792461	B1	2004-09-14	Hericourt, Olivier	
	7	6934751	B2	2005-08-23	Jayapalan et al.	
	8	7027055	B2	2006-04-11	Anderson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7043225	B1	2006-05-09	Patel et al.	
	10	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	11	7174156	B1	2007-02-06	Mangal, Manish	
	12	7636626	B2	2009-12-22	Oesterling et al.	
	13	7680086	B2	2010-03-16	Eglin	
	14	7720206	B2	2010-05-18	Devolites et al.	
	15	7765294	B2	2010-07-27	Edwards et al.	
	16	7843831	B2	2010-11-30	Morrill et al.	
	17	8005913	B1	2011-08-23	Carlander, Carrie	
	18	8131858	B2	2012-03-06	Agulnik et al.	
	19	8160056	B2	2012-04-17	Van der Merwe et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	8180333	B1	2012-05-15	Wells et al.	
	21	8223655	B2	2012-07-17	Heinz et al.	
	22	8315198	B2	2012-11-20	Corneille et al.	
	23	8340678	B1	2012-12-25	Pandey, Vinod	
	24	8385199	B1	2013-02-26	Coward et al.	
	25	8520595	B2	2013-08-27	Yadav et al.	
	26	8523547	B2	2013-09-03	Pekrul, Merton W.	
	27	8621056	B2	2013-12-31	Coussemaeker et al.	
	28	8875042	B2	2014-10-28	LeJeune et al.	
	29	9135037	B1	2015-09-15	Petrescu-Prahova et al.	
	30	9172553	B2	2015-10-27	Dawes et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	9177455	B2	2015-11-03	Remer, David M.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030028623	A1	2003-02-06	Hennessey et al.	
	2	20050060525	A1	2005-03-17	Schwartz et al.	
	3	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	4	20070061800	A1	2007-03-15	Cheng et al.	
	5	20070255769	A1	2007-11-01	Agrawal et al.	
	6	20070299965	A1	2007-12-27	Nieh et al.	
	7	20080066181	A1	2008-03-13	Haveson et al.	
	8	20080126287	A1	2008-05-29	Cox et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	20080212751	A1	2008-09-04	Chung, Simon	
	10	20090203352	A1	2009-08-13	Fordon et al.	
	11	20100041365	A1	2010-02-18	Lott et al.	
	12	20100121744	A1	2010-05-13	Belz et al.	
	13	20140073291	A1	2014-03-13	Hildner et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2002045315	WO	A2	2002-06-06	Micromuse		
	2	2009008817	WO	A1	2009-01-15	Ericsson		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-03-09
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2009 (15.01.2009)

PCT

(10) International Publication Number
WO 2009/008817 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04L 12/26* (2006.01)

(21) International Application Number:
PCT/SE2008/050830

(22) International Filing Date: 3 July 2008 (03.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/948,223 6 July 2007 (06.07.2007) US

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: **PELLETIER, Ghyslain**; Bondevägen 57A, S-961 39 Boden (SE). **WÄNSTEDT, Stefan**; Faktorsvägen 15, S-972 51 Luleå (SE). **ENSTRÖM, Daniel**; Hedenslundsvägen 7, S-954 33 Gammelstad (SE).

(74) Agent: **NILSSON, Charlotte**; Ericsson AB, Patent Unit 3G, S-164 80 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) Title: CONGESTION CONTROL IN A TRANSMISSION NODE

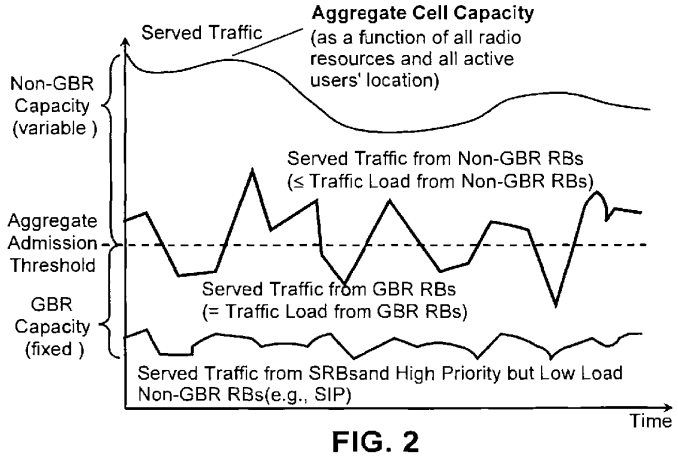


FIG. 2

(57) Abstract: Packets are selectively marked or dropped when congestion of the radio resources is experienced, the selective marking/dropping being related to or dependent on the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and fairness. For example, packets are marked or dropped based on a user's associated share of the total (or a subset of the) shared radio resources. This share may be expressed in terms of the costs of the resources in terms the user's level of utilization of the shared resources, or in terms of it's fairness with respect to other users sharing the same resources. Thus, the present technology takes into account the distribution of resources usage between receivers contributing to the congested state of the radio network.

WO 2009/008817 A1

CONGESTION CONTROL IN A TRANSMISSION NODE

[0001] This application claims the benefit and priority of United States provisional patent application 60/948,223, filed July 6, 2007, entitled "CONGESTION CONTROL ALGORITHM IN A TRANSMISSION NODE", which is incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] This invention pertains to telecommunications, and particularly to the control of congestion in wireless telecommunications.

BACKGROUND

[0003] It is a well-known fact that packet-switched networks utilizing resources shared between the users can experience congestion. Congestion will happen when the sum of traffic of the ingress nodes of the shared resource exceeds the sum of the traffic of the egress nodes of the same shared resource. The most typical example is a router with a specific number of connections. Even if the router has processing power enough to re-route the traffic according to the estimated link throughput, the current link throughput might restrict the amount of traffic the outgoing links from the router can cope with. Hence, the buffers of the router will build up and eventually overflow. The network then experiences congestion and the router is forced to drop packets.

[0004] **Radio resources and congestion**

[0005] Another example of congestion can be found when studying wireless networks with shared channels such as 802.11 a/b/g, High Speed Packet Access (HSPA), Long Term Evolution (LTE), and Worldwide Interoperability for Microwave Access (WiMAX). In these networks, at least the downlink is shared between the users and thus is a possible candidate to experience congestion. In e.g. the case of LTE, the enhanced NodeB (eNB) base station will manage re-transmissions on the Medium Access Control (MAC) layer to the mobile terminal (user equipment, UE) which will have impact on the amount of traffic for which the eNB can provide throughput at any given moment. The more re-transmissions (HARQ and RLC ARQ) required for

successful reception at the UE, the less are the available resources (e.g. transmission power, number of available transmission slots) to provide throughput for other users.

[0006] In, e.g., the case of LTE, the base station (eNB) will also manage how much redundancy is added to protect the data against transmission errors by selecting a proper Modulation and Coding Scheme (MCS) for the physical channel, and then matches the resulting bits to a number of resource blocks (RB). The more conservative the MCS selected for the transmission (e.g. for UEs in bad radio conditions), the less the available resource blocks to provide throughput for users.

[0007] **Congestion and IP transport protocols**

[0008] The normal behavior for any routing node is to provide buffers that can manage a certain amount of variation in input/output link capacity and hence absorb minor congestion occurrences. However, when the congestion is severe enough, the routing node will eventually drop packets.

[0009] Transmission Control Protocol (TCP) is a connection-oriented, congestion-controlled and reliable transport protocol. For TCP traffic, a dropped packet will be detected by the sender since no acknowledgment (ACK) is received for that particular packet and a re-transmission will occur. Further, the TCP protocol has a built in rate adaptive feature which will lower the transmission bit-rate when packet losses occur and re-transmissions happen on the Internet Protocol (IP) layer. Hence, TCP is well suited to respond to network congestion.

[0010] User Datagram Protocol (UDP) is a connectionless transport protocol that only provides a multiplexing service with an end-to-end checksum. UDP is not reliable or congestion-controlled. UDP traffic thus does not have similar mechanisms as TCP to respond to congestion. UDP traffic is by definition non-reliable in the sense that the delivery is not guaranteed. Missing UDP packets will not be re-transmitted unless the application layer using the transport service provided by UDP has some specialized feature which allows this. UDP by itself does not respond in any way to network congestion, although application layer mechanisms may implement some form of response to congestion.

[0011] **Explicit Congestion Notification (ECN)**

[0012] To further increase the performance of routing nodes, a mechanism called "Explicit Congestion Notification for IP" has been developed. See, e.g., RFC 3168, Proposed Standard, September 2001, incorporated herein by reference. This mechanism uses two bits in the IP header to signal the risk for congestion-related losses. The field has four code points, where two are used to signal ECN capability and the other two are used to signal congestion. The code point for congestion is set in, e.g., routers. When the receiver has encountered a congestion notification it propagates the information to the sender of the stream which then can adapt its transmission bit-rate. For TCP, this is done by using two bits in the TCP header. Prior to their definition for use with ECN, these bits were reserved and not used. When received, these bits trigger the sender to reduce its transmission bit-rate.

[0013] The benefit with TCP is dual in this case. As a first benefit, since TCP acknowledges the reception of the incoming packets, all TCP connections automatically have a back-channel (This is not the case with UDP). As a second benefit, TCP has a built-in back-off response to packet losses which also can be used in connection with ECN (This is not available for UDP).

[0014] To summarize, ECN with TCP has all the mechanisms available in standards to enable successful deployment. This is also seen in more modern routers and new PC operating systems.

[0015] The situation with ECN for UDP is quite different. ECN is defined for IP usage with any transport protocol. However, ECN is only explicitly specified in terms of use with TCP traffic. ECN for UDP needs the same generic mechanisms as ECN for TCP: a fast back-channel and some rate control algorithm.

[0016] Within the context of UDP-based real-time communication services such as IMS Multimedia Telephony (MTSI), there is a clear need to manage congestion. Such services are by definition quite sensitive to packet loss. Hence, any means available to avoid such losses should be used. ECN for UDP would be a suitable candidate to alleviate the impact of congestion. It turns out that both requirements for successful ECN usage, fast feedback and rate adaptation, are readily available in many such

services, the lacking part is the connection between the ECN bits and the response of the application.

[0017] Another aspect of the use of ECN is the congestion avoidance algorithm (described below) used in a congested node to either drop or mark packets to signal congestion.

[0018] **Congestion avoidance algorithms**

[0019] Congestion avoidance algorithms include three basic types: Tail Drop, Random Early Detection (RED), and Weighted Random Early Detection (WRED).

[0020] A tail drop congestion avoidance algorithm treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.

[0021] The Random Early Detection (RED) congestion avoidance algorithm addresses network congestion in a responsive rather than reactive manner. Underlying the RED mechanism is the premise that most traffic runs on data transport implementations which are sensitive to loss and will temporarily slow down when some of their traffic is dropped. TCP, which responds appropriately - even robustly - to traffic drop by slowing down its traffic transmission, effectively allows RED's traffic-drop behavior to work as a congestion-avoidance signaling mechanism. A typical RED implementation starts dropping or marking packets when the average queue depth is above a minimum threshold. The rate of dropping or marking packets is increased linearly as the average queue size increases, until the queue size reaches the maximum threshold. At this point, all packets are dropped. Whether a packet is ECN-marked or dropped depends on if the ECN bits shows that the mechanism is enabled. However, when applied to traffic that does not respond to congestion or is not robust against losses, RED induces negative impacts on the service.

[0022] A weighted Random Early Detection (WRED) congestion avoidance precedence between IP flows provides for preferential traffic handling of packets with higher priority. WRED can selectively discard or mark lower priority traffic when the average queue depth is above a minimum threshold. Differentiated performance characteristics

for different classes of service can be provided in this manner. By randomly dropping or marking packets prior to periods of high congestion, WRED tells the packet source to decrease its transmission rate.

[0023] Other variants of similar algorithms exist, where the decisional factor is based on queue sizes, traffic classes, resource reservation, and ECN capabilities. In this respect, network nodes interact with the transport protocols in an attempt to mitigate congestion while providing means to the sender to adapt its sending rate consequently and limit the impact of congestion to applications.

[0024] Algorithms to mark or drop packets when congestion is experienced in a network node, henceforth simply referred to as a "marking algorithm", have so far (i.e. in fixed networks) defined congestion as a function of a node's queue depth. The probability that a packet will be "congestion-marked or dropped" in a queue is derived as a function of the average depth of the queue where it lies. Traffic classes and resource reservation (e.g. RSVP) in this respect are essentially a mean to separate one interface's queue into multiple smaller ones, for the purpose of calculating this probability.

[0025] **Congestion in fixed packet data networks**

[0026] For fixed packet-switched networks, a link is typically said to be congested when the offered load on the link reaches a value close to the capacity of the link. In other words, congestion is defined as the state in which a network link is close to being completely utilized by the transmission of bytes. This is largely because the capacity of the link is constant over time, and because the physical characteristics of the ingress and of the egress links are similar.

[0027] **Congestion in wireless networks**

[0028] Defining congestion in wireless network is more complex than simply relating to capacity in terms of the number of bits that can be transmitted. Congestion in wireless networks can be defined as the state in which the transmission channel is close to being completely utilized.

[0029] The total capacity of the transmission channel is distributed between different receivers having different radio conditions. This means that the shared resources are consumed partly by varying levels of redundancy (retransmissions, channel coding) necessary to protect the data that is useful to the user (i.e. IP packets). This tradeoff is conceptually shown in Fig. 1.

[0030] **Managing radio resources and cell capacity**

[0031] The concept of radio bearers is used in LTE to, e.g., support user data services. End-to-end services (e.g. IP services) are multiplexed on different bearers. These different bearers represent different priority queues over the radio interface.

[0032] A bearer is referred to as a GBR bearer if dedicated network resources related to a Guaranteed Bit Rate (GBR) value that is associated with the bearer are permanently allocated (e.g. by an admission control function in the RAN) at bearer establishment / modification. Otherwise, a bearer is referred to as a Non-GBR bearer:

- GBR (Guaranteed Bit Rate – UL + DL)
- MBR (Maximum Bit Rate – UL + DL)

[0033] With respect to how resources are separated between different receivers, there can be a guarantee for some receivers about a specific bit rate, a guaranteed bit rate (GBR). There can also be a part of the cell capacity that is used for data for which no guarantee in terms of bit rate is applicable (non-GBR). Applications, such as real-time applications using codecs that can adapt their bit rate, may fill their allocated GBR and go to a higher rate to fill the non-GBR area, when possible, to increase the application bit rate and hence improve their performance. Fig. 2 shows capacity in terms whether bit rate is guaranteed or not.

[0034] **eNode B Measurements**

[0035] In E-UTRAN, certain types of measurements can be performed internally in the eNode B. These measurements do not need to be specified in the standard; rather they are implementation dependent. The possible measurements serve a number of procedures, such as handovers and other radio resource management.

[0036] In particular, the eNode B can perform measurement related to the amount of transmission power in the cell, antenna branch or per resource block (per UE), as well as received power in the UL per cell, per UE, or per resource block.

[0037] **Measurements and Handover decisions**

[0038] The serving eNode B performs UL measurements on (for instance) the signal-to-interference-ratio (SIR), received resource block power, and the received total wideband power. For a handover (HO) decision, it may also take into account other (downlink) measurements, such as the transmitted (total) carrier power and/or the transmitted carrier power per resource block.

[0039] **Problems with existing solutions**

[0040] When the network node that experiences congestion is at one edge of a wireless network, such as a base station transmitter, congestion can occur due to one or more of the following: (1) the ingress data rate is larger than the downlink available throughput for the entire cell; (2) the ingress data rate is larger than the downlink available throughput, for one receiver (UE); (3) a UE is in bad radio conditions; (4) the cell capacity becomes power limited.

[0041] In other words, the total bit rate exchanged over the air is distributed between user data and coding rate, where the coding rate is adjusted to the radio conditions the receiver is in.

[0042] To make it possible to signal congestion using, e.g., ECN in a manner that is most relevant to quickly efficiently decrease congestion in the radio resources, a mechanism is needed to mark the packets. Packets can (for example) be marked using ECN, even for real-time applications using RTP over UDP.

[0043] Using ECN with UDP traffic requires specialized application behavior: upon reception of a congestion notification, the receiver needs to transmit a request to the sender requiring the sender to reduce its bit-rate. When that request arrives at the sender, it should immediately reduce the transmitted bit-rate. The amount of the reduction is determined by the sender, which in turn can base its decision on a number of parameters.

[0044] In short, current foreseen mechanisms will not provide efficient marking or packet dropping mechanisms that efficiently address congestion of the radio resources.

SUMMARY

[0045] In accordance with an aspect of the technology described herein, packets are selectively marked or dropped when congestion of the radio resources is experienced, the selective marking/dropping being related to or dependent on the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and fairness. For example, packets are marked or dropped based on a user's associated share of the total (or a subset of the) shared radio resources. This share may be expressed in terms of the costs of the resources in terms the user's level of utilization of the shared resources, or in terms of it's fairness with respect to other users sharing the same resources. Thus, the present technology takes into account the distribution of resources usage between receivers contributing to the congested state of the radio network.

[0046] One aspect of the technology concerns a method of operating a communications network. The method comprises detecting congestion of a shared radio resource and, for a user of the shared radio resource, selectively dropping packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

[0047] In one example embodiment the user's share is expressed in terms of cost or amount of resources associated to a user. In one example implementation, the method further comprises determining the cost, or the amount of resources associated to the user, based on transmitter measurements. For example, the transmitter measurements include at least one of the following: downlink total transmit power; downlink resource block transmit power; downlink total transmit power per antenna branch; downlink resource block transmit power per antenna branch; downlink total resource block usage; uplink total resource block usage; downlink resource block activity; uplink resource block activity; uplink received resource block power; uplink signal to interference ratio (per user equipment unit); uplink UL HARQ block error rate. Another example implementation, comprises determining the cost, or the amount of resources associated to the user, based on at least one of receiver feedback and/or measurements. In an example implementation, the receiver feedback and/or measurements include channel quality indication/(CQI/HARQ) feedback.

[0048] An example embodiment further comprises determining the user's share in terms of one or more of the following: the user's fraction of total power; the user's fraction of total interference; the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost); channel quality indications; handover measurements; and, the type of modulation and coding scheme used for the user.

[0049] An example embodiment further comprises selectively dropping the packets in accordance with the user's share of radio resource usage and relative priority of the user relative to other users in periods of congestion of the shared radio resource.

[0050] In another of its aspects, the technology concerns a packet marker which marks or drops packet in accordance with the technique(s) described herein, e.g., selectively dropping packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

BRIEF DESCRIPTION OF THE DRAWINGS

[0051] The foregoing and other objects, features, and advantages of the invention will be apparent from the following more particular description of preferred embodiments as illustrated in the accompanying drawings in which reference characters refer to the same parts throughout the various views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

[0052] Fig. 1 is a diagrammatic view of tradeoff between "useful bits" and channel coding using the same amount of resource blocks.

[0053] Fig. 2 is a diagrammatic view showing operation-controlled partitioning of cell capacity.

[0054] Fig. 3 is a diagrammatic view showing layered functional view of functional components of an example LTE eNB node and a user equipment unit (UE).

[0055] Fig. 4 is a diagrammatic view showing downlink scheduler input, output and interactions according to an example embodiment.

DETAILED DESCRIPTION

[0056] In the following description, for purposes of explanation and not limitation, specific details are set forth such as particular architectures, interfaces, techniques, etc. in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced in other embodiments that depart from these specific details. That is, those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are included within its spirit and scope. In some instances, detailed descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description of the present invention with unnecessary detail. All statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

[0057] Thus, for example, it will be appreciated by those skilled in the art that block diagrams herein can represent conceptual views of illustrative circuitry embodying the principles of the technology. Similarly, it will be appreciated that any flow charts, state transition diagrams, pseudocode, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

[0058] The functions of the various elements including functional blocks labeled or described as "processors" or "controllers" may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared or distributed. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may include, without limitation, digital signal processor (DSP) hardware, read only memory (ROM) for storing software, random access memory (RAM), and non-volatile storage.

[0059] Fig. 3 shows various example functions involved in transmission (eNB) and reception (UE) in a Long Term Evolution (LTE) version of a telecommunications network 20. While LTE is used to exemplify concepts related to radio transmission such as the packet marking technique described herein, similar concepts apply also to other wireless technologies and the technology is thus equally applicable to systems other than LTE.

[0060] The telecommunications network 20 includes both base station node 28 (also known as a NodeB, eNodeB, or BNode) and wireless terminal 30 (also known as a user equipment unit [UE], mobile station, or mobile terminal). The wireless terminal 30 can take various forms, including (for example) a mobile terminal such as mobile telephones ("cellular" telephones) and laptops with mobile termination, and thus can be, for example, portable, pocket, hand-held, computer-included, or car-mounted mobile devices which communicate voice and/or data with radio access network. Alternatively, the wireless terminals can be fixed wireless devices, e.g., fixed cellular devices/terminals which are part of a wireless local loop or the like.

[0061] Typically base station node 28 communicates over wireless interface 32 (e.g., a radio interface) with plural wireless terminals, only one representative wireless terminal 30 being shown in Fig. 3. Each base station node 28 serves or covers a geographical area known as a cell. That is, a cell is a geographical area where radio coverage is provided by the radio base station equipment at a base station site. Each cell is identified by an identity, which is broadcast in the cell. The base stations communicate over the air interface (e.g., radio frequencies) with the user equipment units (UE) within range of the base stations.

[0001] The base station node 28 comprises a radio access network (RAN). If the radio access network is a "flat" type network as occurs in LTE, the base station node 28 essentially performs most of the radio access network functionality and connects to core networks. If, on the other hand, the radio access network is of a more conventional type (such as a Universal Mobile Telecommunications (UMTS) Terrestrial Radio Access Network (UTRAN), one or more base station nodes are connected to the core network through a controller node such as a radio network controller (RNC). The UMTS is a third generation system which in some respects builds upon the radio access technology known as Global System for Mobile communications (GSM) developed in

Europe. UTRAN is essentially a radio access network providing wideband code division multiple access (WCDMA) to user equipment units (UEs). The Third Generation Partnership Project (3GPP) has undertaken to evolve further the UTRAN and GSM-based radio access network technologies, the LTE being just one version of evolution.

[0062] As those skilled in the art appreciate, in W-CDMA technology a common frequency band allows simultaneous communication between a user equipment unit (UE) and plural base stations. Signals occupying the common frequency band are discriminated at the receiving station through spread spectrum CDMA waveform properties based on the use of a high speed, pseudo-noise (PN) code. These high speed PN codes are used to modulate signals transmitted from the base stations and the user equipment units (UEs). Transmitter stations using different PN codes (or a PN code offset in time) produce signals that can be separately demodulated at a receiving station. The high speed PN modulation also allows the receiving station to advantageously generate a received signal from a single transmitting station by combining several distinct propagation paths of the transmitted signal. In CDMA, therefore, a user equipment unit (UE) need not switch frequency when handoff of a connection is made from one cell to another. As a result, a destination cell can support a connection to a user equipment unit (UE) at the same time the origination cell continues to service the connection. Since the user equipment unit (UE) is always communicating through at least one cell during handover, there is no disruption to the call. Hence, the term "soft handover." In contrast to hard handover, soft handover is a "make-before-break" switching operation.

[0063] Fig. 3 shows an Internet Protocol (IP) packet 40_B received at base station node 28, e.g., from a core network or another base station node. Fig. 3 further shows various layer handlers or functionalities comprising base station node 28 and wireless terminal 30. In particular, for base station node 28 and wireless terminal 30, respectively, Fig. 3 shows: PDCP functionality 42_B and 42_W; radio link control functionality 44_B and 44_W; medium access control (MAC) functionality 46_B and 46_W; and physical layer functionality 48_B and 48_W.

[0064] Fig. 3 illustrates that IP packets for plural users are typically in-coming on SAE bearers to base station node 28 from other radio access network nodes or from the core

network. "SAE" stands for "System Architecture Evolution", and an SAE bearer supports a flow and provides Quality of Service (QoS) end-to-end (both over radio and core network). Typically there is a one-to-one mapping between an SAE Bearer and an SAE Radio Bearer. Furthermore there is a one-to-one mapping between a Radio Bearer and a logical channel. It then follows that an SAE Bearer, i.e. the corresponding SAE Radio Bearer and SAE Access Bearer, is the level of granularity for QoS control in an SAE/LTE access system. Packet flows mapped to the same SAE Bearer receive the same treatment. Fig. 3 further illustrates that an instance of each of the aforementioned functionalities can exist for each user (such as user #i depicted as one of the plural users in Fig. 3).

[0065] Fig. 3 further illustrates various sub-units of the layer handlers or functionalities for base station node 28 and wireless terminal 30. For example, in base station node 28 PDCP functionality 42_B comprises header compressors 50_B and ciphering units 52_B, and in wireless terminal 30 the PDCP functionality 42_W comprises header decompressors 50_W and deciphering units 52_W. In base station node 28, the radio link control functionality 44_B comprises segmentation/automatic repeat request (ARQ) unit 54_B, while in wireless terminal 30 the radio link control functionality 44_W comprises concatenation/automatic repeat request (ARQ) unit 54. In base station node 28 the medium access control (MAC) functionality 46_B comprises MAC scheduler 56; MAC multiplexing units 58_B; and Hybrid ARQ units 60_B. In wireless terminal 30 the medium access control (MAC) functionality 46_W comprises MAC demultiplexing units 58_W and Hybrid ARQ units 60_W. In base station node 28 the physical layer functionality 48_B comprises coding units 62_B; modulators 64_B; and antenna and resource mapping units 66_B which ultimately connect to or comprise transceivers 68_B. Conversely, in wireless terminal 30 the physical layer functionality 48_W comprises decoding units 62_W; demodulators 64_W; and antenna and resource mapping units 66_W (which connect to or comprise transceiver(s) 68_W).

[0066] The MAC scheduler 56 is connected to or interacts with various units of functionalities of base station node 28. For example, a payload selection signal is applied from MAC scheduler 56 to segmentation/automatic repeat request (ARQ) unit 54_B; priority handling and payload selection signals are applied from MAC scheduler 56 to MAC multiplexing units 58_B; retransmission control signals are applied from MAC scheduler 56 to Hybrid ARQ units 60_B; modulation scheme signals are applied

from MAC scheduler 56 to modulators 64_B; and, antenna and resource assignment signals are applied from MAC scheduler 56 to antenna and resource mapping units 66_B.

[0067] Fig. 3 thus shows how user data in an IP packet 40_B is processed by the various layers or functionalities of base station node 28, and is carried to PDCP functionality 42_B in a SAE bearer; from PDCP functionality 42_B to radio link control functionality 44_B by a radio bearer; from radio link control functionality 44_B to medium access control (MAC) functionality 46_B by a logical channel; and from medium access control (MAC) functionality 46_B to physical layer functionality 48_B by a transport channel; and is then transported over air interface 32 to wireless terminal 30.

[0068] On the side of wireless terminal 30, Fig. 3 also shows how the information received over air interface 32 is handled by physical layer functionality 48_W; and then handed over transport channels to medium access control (MAC) functionality 46_W, and then handed over logical channels to radio link control functionality 44_W; handed over radio bearers to PDCP functionality 42_W; and then realized over SAE bearers as a received packet 40_W.

[0069] In LTE, a shared channel (the DL-SCH) is used for downlink transmissions of user data. As can be seen in Fig. 3, MAC scheduler 56 is the process, functionality, or unit that determines what receiver will be served using the shared resources. The MAC scheduler 56 also determines what resource block (in time and frequency) will be used as well with the proper modulation and coding scheme. User and data rate on the DL-SCH is based on instantaneous channel quality. For the uplink and in other wireless channels where dedicated radio bearers are used, the shared resource in the amount of interface that can be generated for each UE; this is referred to as an interference limited system.

[0070] As indicated previously, congestion is typically experienced in a radio network when the shared resources become utilized beyond a certain threshold. For a fixed amount X of radio resources, the amount of user data that is transmitted varies based on radio link conditions.

[0071] The present technology marks or drops packets selectively when congestion of the radio resources is experienced. In the illustrated embodiment, the selective

marking/dropping of packets during congestion according to the criteria/techniques described herein can be implemented in or realized by in a suitable functionality in a node such as a base station (eNB). The functionality which makes the decision to mark or drop a packet according to the foregoing criteria is termed a "packet marker" and can be, for example, a downlink scheduler (e.g., MAC scheduler 56), or a separate process that monitors the queues of the scheduler, or separate process with its own queues prior to the scheduler.

[0072] The selective marking/dropping technique of the present technology is related to or dependent on the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and/or fairness. For example, packets are marked or dropped based on a user's associated share of the total (or a subset of the) shared radio resources. This share may be expressed in terms of the costs of the resources in terms the user's level of utilization of the shared resources, or in terms of it's fairness with respect to other users sharing the same resources. Thus, the packet marker and the techniques of the present technology take into account the distribution of resources usage between receivers contributing to the congested state of the radio network.

[0073] As used herein, the term "user" refers to a user of radio resources, and thus may be an IP flow (service) [even a packet itself], a radio bearer, a UE, or a group of UEs. Which of those is marked may be based on relative priority between each other, such as using QoS classes, UE subscription information, or the like.

[0074] The technology thus encompasses at least two ways of apportioning a user's share: the first way is based on the cost or amount of resources associated to a user; the second way is based on "fairness".

[0075] A user's share of the total costs can be derived in terms of radio resources. The cost, or the amount of resources associated to the user, may be determined based on different measurements, independently or not, such as transmitter measurements and receiver feedback and/or measurements.

[0076] As used herein, "fairness" means that both the share of radio resources and QoS and other guarantees provided by the system are used in the decision to mark or drop.

On the other hand, in a system with high congestion where QoS targets cannot be reached for several UEs, the eNB can use each UE's share of the resources and use the QoS agreements relative to each other to decide how to mark/drop packets, until congestion levels come back to normal. Thus, "fairness" encompasses a combination of radio resource usage and QoS agreements (bitrate, delay, loss rate, etc) and/or priorities relative to each other, in periods of congestion of the radio resources.

[0077] In particular, measurements similar to those for handover (HO) decision can be used to measure a degree of fairness between UEs with respect to their respective resource utilization in the cell, for the purpose of congestion marking and or dropping at the IP transport level. UE measurements that indicate that the UE is getting closer to the threshold used to decide to make a HO means that the UE is in a non-favorable locations, and that radio conditions are deteriorating. In this case, more radio resources (power, retransmissions, etc) are needed to "reach" this UE. In other words, a strong received signal means that the UE does not require as many DL resources to receive the signal, but a weakly received signal means that the UE requires or wants more DL resources. Congestions (and thereby marking) may also occur somewhere in the cell where is not possible to do a handover, hence other measures for congestion marking can also be implemented.

[0078] The decision whether or not a packet is marked (or dropped) can also include whether the radio resources consumed by the user exceed the allocated guaranteed bit rate or not, in the case where congestion is experienced or a certain utilization threshold is reached.

[0079] For example, capacity gains (or the effect of marking on overall congestion in the cell) may be bigger if flows targeted at UEs in bad radio conditions are marked first - those are using more resources than others because of their poor radio situation. Fairness can be achieved by targeting traffic in the Non-GBR area for such UEs.

[0080] Fig. 4 shows the inputs to a MAC scheduler 56 which, in an example embodiment, performs the role of packet marker and thus performs the decision for packet marking and canceling according to the criteria described herein. In an example embodiment, the packet marker or scheduling function can be implemented by a processor or controller.

[0081] Fig. 4 shows that HARQ feedback and CQI reports from representative wireless terminal UE_k 30 are used as input to the MAC scheduler 56 for reporting the allocation of the shared resources to the receiver. This can be another type of input to the assessment of how much congestion is generated by a UE (relative to others).

[0082] The packet marker illustrated as MAC scheduler 56 also receives input regarding the logical channels for the representative wireless terminal 30_k, e.g.,, from the buffer/queue or buffer/queue manager for the logical channels 70_k for the representative wireless terminal 30_k. For each such channel/queue, the packet marker receives an indication of wireless terminal weight (UE weight); label, GBR/MBR status, and ARP (allocation/retention priority), queue delay, and queue (buffer) size. "Label: is also called QoS class identifier (qci) [see, e.g., 3GPP TS 23.203], and can be a scalar that is used as a reference to a specific packet forwarding behavior (e.g., packet loss rate, packet delay budget) to be provided to a SDF.

[0083] The packet marker illustrated as MAC scheduler 56 also receives input from a functionality or unit 72 that monitors the system frame number (SFN) flow and apprises the MAC scheduler 56 of the number of radio bearers required for the representative wireless terminal 30_k.

[0084] The packet marker illustrated as MAC scheduler 56 can also receive input from a suitable unit 74 regarding a multicast logical channel in the event that the representative wireless terminal 30_k participates in a multicast transmission. The information received by the packet marker from unit 74 regarding the multicast transmission basically pertain to the buffer for the multicast transmission and include label; GBR/MBR status; buffer/queue delay; and queue (buffer) size.

[0085] The packet marker illustrated as MAC scheduler 56 also receives other restriction information inputs such as those depicted as ICIC/RRM restrictions; UE capability restrictions; and other restrictions (e.g., DRX, TN, ...).

[0086] The packet marker illustrated as MAC scheduler 56 also receives input from link adaptor 76, particularly a number of bits input. The packet marker illustrated as MAC scheduler 56 outputs to link adaptor 76 a resource indication [which is a request for resources given the inputs from the data queue, e.g., for an uplink scheduling request

and for a downlink scheduling assignment. The link adaptor 76 in turn outputs an indication of the transport format for each scheduled transport channel.

[0087] The packet marker illustrated as MAC scheduler 56 outputs the number of resource blocks for each scheduled transport channel.

[0088] As indicated above, the selective marking/dropping technique of the present technology is related to or dependent the probability that a packet will be marked with the relative efficiency of usage of the radio link by the receiver, e.g., dependent upon radio resource usage costs and/or fairness.

[0089] Examples of transmitter measurements that can be used to determine a user's share of the total cost include the following:

DL total Tx power: Transmitted carrier power measured over the entire cell transmission bandwidth.

DL resource block Tx power: Transmitted carrier power measured over a resource block.

DL total Tx power per antenna branch: Transmitted carrier power measured over the entire bandwidth per antenna branch.

DL resource block Tx power per antenna branch: Transmitted carrier power measured over a resource block.

DL total resource block usage: Ratio of downlink resource blocks used to total available downlink resource blocks (or simply the number of downlink resource blocks used).

UL total resource block usage: Ratio of uplink resource blocks used to total available uplink resource blocks (or simply the number of uplink resource blocks used).

DL resource block activity: Ratio of scheduled time of downlink resource block to the measurement period.

UL resource block activity: Ratio of scheduled time of uplink resource block to the measurement period.

UL received resource block power: Total received power including noise measured over one resource block at the eNode B.

UL SIR (per UE): Ratio of the received power of the reference signal transmitted by the UE to the total interference received by the eNode B over the UE occupied bandwidth.

UL HARQ BLER: The block error ratio based on CRC check of each HARQ level transport block.

[0090] Examples of receiver feedback and/or measurements that can be used to determine a user's share of the total cost include, e.g. CQI/HARQ feedback as described above. In particular, handover measurements and CQI/HARQ feedback can be used in an example mode.

[0091] Examples of calculations would include the user's fraction of total power, the user's fraction of total interference, the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost), Channel quality indications (CQI, i.e. the UEs measurements of reception quality), handover measurements (where the logic that determines how close to the threshold for performing a handover the UE is, e.g. how close the UE is to getting out of coverage), the type of Modulation and coding scheme used for the user (where lower modulation and higher amount of redundancy indicates higher cost). All these can be used individually or in combination with each other.

[0092] Using LTE as a non-limiting example, measurements that can be used to determine a user's share of the total cost include:

- Measurements from the serving eNB: Received total WB power, SIR, transmitted (total) carrier power, Transmitted carrier power per resource block (per UE).
- Measurements from the UE, reported to the eNB: Reference symbol receiver power, reference symbol received quality, carrier received signal strength indicator.

[0093] Some of the layer handler/functionalities or units involved and/or illustrated in Fig. 3 are elaborated below.

[0094] In a first step of the transport-channel processing, a cyclic redundancy check (CRC) is calculated and appended to each transport block by ciphering units 52_B. The CRC is used to detect transmission errors in the receiver.

[0095] For channel coding as performed by coding units 62_B, only Turbo-coding can be applied in case of downlink shared channel (DL-SCH) transmission. Channel coding

adds redundancy (similar to Forward Error Correction - FEC) to the bits to be transmitted, to compensate for possible transmission errors. The amount of redundancy added depends on the channel quality as estimated by the eNB.

[0096] The task of the downlink physical-layer hybrid-ARQ functionality 60 is to extract the exact set of bits to be transmitted at each transmission/retransmission instant from the blocks of code bits delivered by the channel coder. Thus, it is also implicitly the task of the hybrid-ARQ functionality to match the number of bits at the output of the channel coder to the number of bits to be transmitted. The latter is given by the number of assigned resource blocks and the selected modulation scheme and spatial-multiplexing order. In case of a retransmission, the HARQ functionality will, in the general case, select a different set of code bits to be transmitted (Incremental Redundancy).

[0097] The downlink data modulation performed by modulators 64_B maps blocks of scrambled bits to corresponding blocks of complex modulation symbols. The set of modulation schemes supported for the LTE downlink includes QPSK, 16QAM, and 64QAM, corresponding to two, four, and six bits per modulation symbol respectively.

[0098] As indicated above, the base station node 28 can also receive Channel Quality Indicator (CQI) reports from the UE, which measures the quality of the DL reception based on a reference signal either per resource block or per group of resource blocks. The UE can also measure and report the observed DL HARQ BLER, which is the block error rate based on CRC check of each HARQ level transport block. The eNB also can receive HARQ ACKs and NACKs for every downlink transmission.

[0099] Functions that determine QoS in shared channel access networks (not only radio) are the following:

(1) Scheduling (UL + DL)
(2) Traffic Conditioning (UL + DL)
    - o Admission control for GBR bearers
    - o Rate policing/shaping for GBR and Non-GBR bearers

[00100] Another relevant function that can be implemented in an eNode B is queue management which can be optimized for either real-time or non-real-time traffic.

[00101] Advantageously the technology solves a problem of how to mark (or drop) IP packets in a radio transmitter (e.g. eNB) so that the radio receiver that contributes the most to the congestion can be signaled that the radio network is experiencing congestion.

[00102] In at least some example embodiments, a mechanism such as ECN (marking) or detection or packet losses (dropping) is assumed to be available and to reach the application. It also assumed that the application in the receiver as the means to propagate back feedback to the IP application in the sender. It can be expected that such mechanisms will get deployed in a foreseeable future.

[00103] The technology advantageously handles the logic for marking dropping packets, and is thus a component in a broader solution where congestion can be handled with as little packet losses as possible by enabling the sender of IP packets to adjust its send rate to the radio conditions along the path, as well as to adjust to the usage their IP packets are consuming.

[00104] Without this functionality, there is a fair risk that the impact on the quality of the session media, when congestion occurs, is distributed randomly in an unfair manner and to a larger number of receivers, resulting in a more drastic drop in media quality and user experience.

[00105] With this functionality, on the other hand, the impact of congestion is redistributed to the receivers most responsible for the congested state, in a manner that is fairer than by randomly marking or dropping packets based on e.g. queue state in the transmitter.

[00106] Although the description above contains many specificities, these should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments. Therefore, it will be appreciated that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art. Reference to an element in the singular is not intended to mean "one and only one" unless explicitly so

stated, but rather "one or more." All structural, chemical, and functional equivalents to the elements of the above-described preferred embodiment that are known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed hereby. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved or described herein.

WHAT IS CLAIMED IS:

1. A method of operating a communications network comprising:
detecting congestion of a shared radio resource;
characterized by:
for a user of the shared radio resource, selectively dropping packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

2. The method of claim 1, wherein the user's share is expressed in terms of cost or amount of resources associated to a user.

3. The method of claim 2, further comprising determining the cost, or the amount of resources associated to the user, based on transmitter measurements.

4. The method of claim 3, wherein the transmitter measurements include at least one of the following: downlink total transmit power; downlink resource block transmit power; downlink total transmit power per antenna branch; downlink resource block transmit power per antenna branch; downlink total resource block usage; uplink total resource block usage; downlink resource block activity; uplink resource block activity; uplink received resource block power; uplink signal to interference ratio (per user equipment unit); uplink UL HARQ block error rate.

5. The method of claim 2, further comprising determining the cost, or the amount of resources associated to the user, based on at least one of receiver feedback and/or measurements.

6. The method of claim 5, wherein the receiver feedback and/or measurements include channel quality indication/(CQI/HARQ) feedback.

7. The method of claim 1, further comprising determining the user's share in terms of one or more of the following: the user's fraction of total power; the user's fraction of total interference; the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost); channel quality

indications; handover measurements; and, the type of modulation and coding scheme used for the user.

8. The method of claim 1, further comprising selectively dropping the packets in accordance with the user's share of radio resource usage and relative priority of the user relative to other users in periods of congestion of the shared radio resource.

9. A node (28) of a communications network comprising:

a transceiver (68B) configured to transmit a shared radio resource to a user;

characterized by:

a packet marker (56) configured, upon detection of congestion of the shared radio resource, to selectively drop packets allocated to the shared radio resource in accordance with the user's share of the shared radio resources.

10. The node (28) of claim 9, wherein the user's share is expressed in terms of cost or amount of resources associated to a user.

11. The node (28) of claim 10, wherein the packet marker (56) is configured to determine the cost, or the amount of resources associated to the user, based on transmitter measurements.

12. The node (28) of claim 11, wherein the node (28) is configured to use transmitter measurements including at least one of the following: downlink total transmit power; downlink resource block transmit power; downlink total transmit power per antenna branch; downlink resource block transmit power per antenna branch; downlink total resource block usage; uplink total resource block usage; downlink resource block activity; uplink resource block activity; uplink received resource block power; uplink signal to interference ratio (per user equipment unit); uplink UL HARQ block error rate.

13. The node (28) of claim 10, wherein the packet marker (56) is configured to determine the cost, or the amount of resources associated to the user, based on at least one of receiver feedback and/or measurements.

14. The node (28) of claim 13, wherein the receiver feedback and/or measurements include channel quality indication/(CQI/HARQ) feedback.

15. The node (28) of claim 9, wherein the packet marker (56) is configured to determine the user's share in terms of one or more of the following: the user's fraction of total power; the user's fraction of total interference; the user's fraction of the total number of retransmissions (where in all of the previous a higher ration means a higher cost); channel quality indications; handover measurements; and, the type of modulation and coding scheme used for the user.

16. The node (28) of claim 9, wherein the packet marker (56) is configured to selectively drop the packets in accordance with the user's share of radio resource usage and relative priority of the user relative to other users in periods of congestion of the shared radio resource.

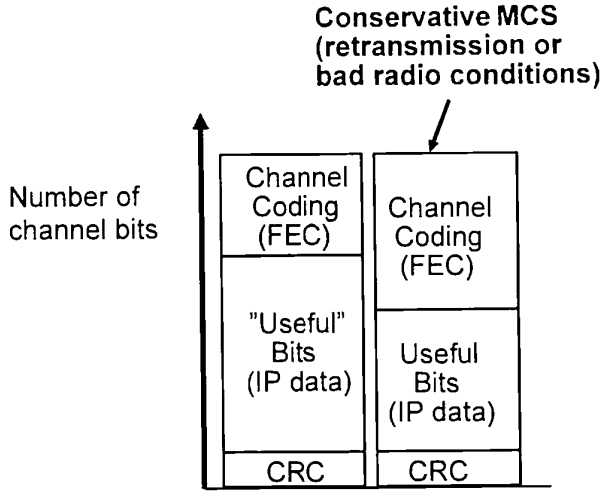

Conservative MCS
(retransmission or
bad radio conditions)
Number of
channel bits
Channel
Coding
(FEC)
"Useful"
Bits
(IP data)
CRC
Channel
Coding
(FEC)
Useful
Bits
(IP data)
CRC

FIG. 1

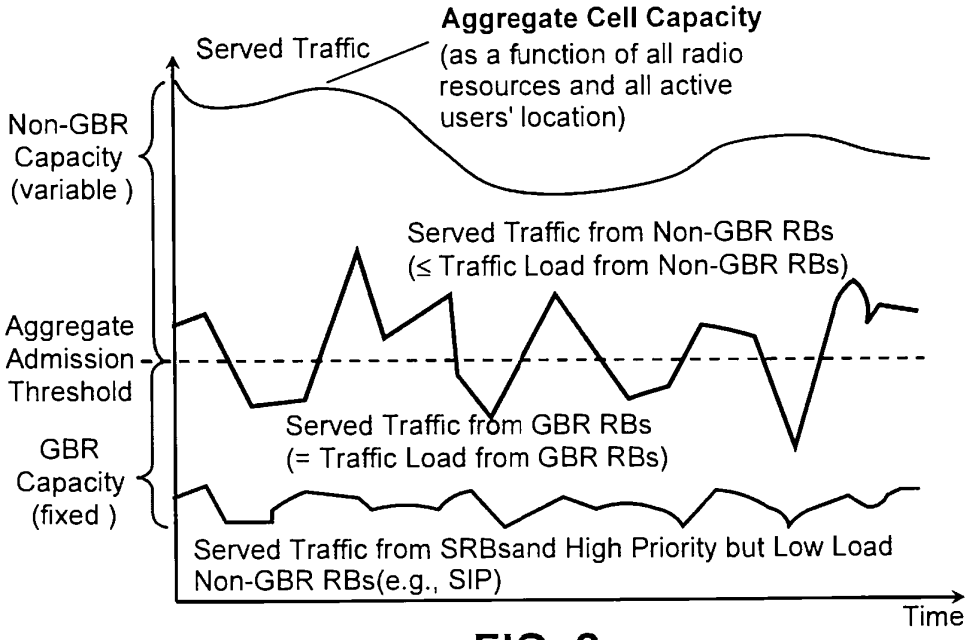

Aggregate Cell Capacity
(as a function of all radio
resources and all active
users' location)
Served Traffic
Non-GBR
Capacity
(variable)
Served Traffic from Non-GBR RBs
(≤ Traffic Load from Non-GBR RBs)
Aggregate
Admission
Threshold
Served Traffic from GBR RBs
(= Traffic Load from GBR RBs)
GBR
Capacity
(fixed)
Served Traffic from SRBsand High Priority but Low Load
Non-GBR RBs(e.g., SIP)
Time

FIG. 2

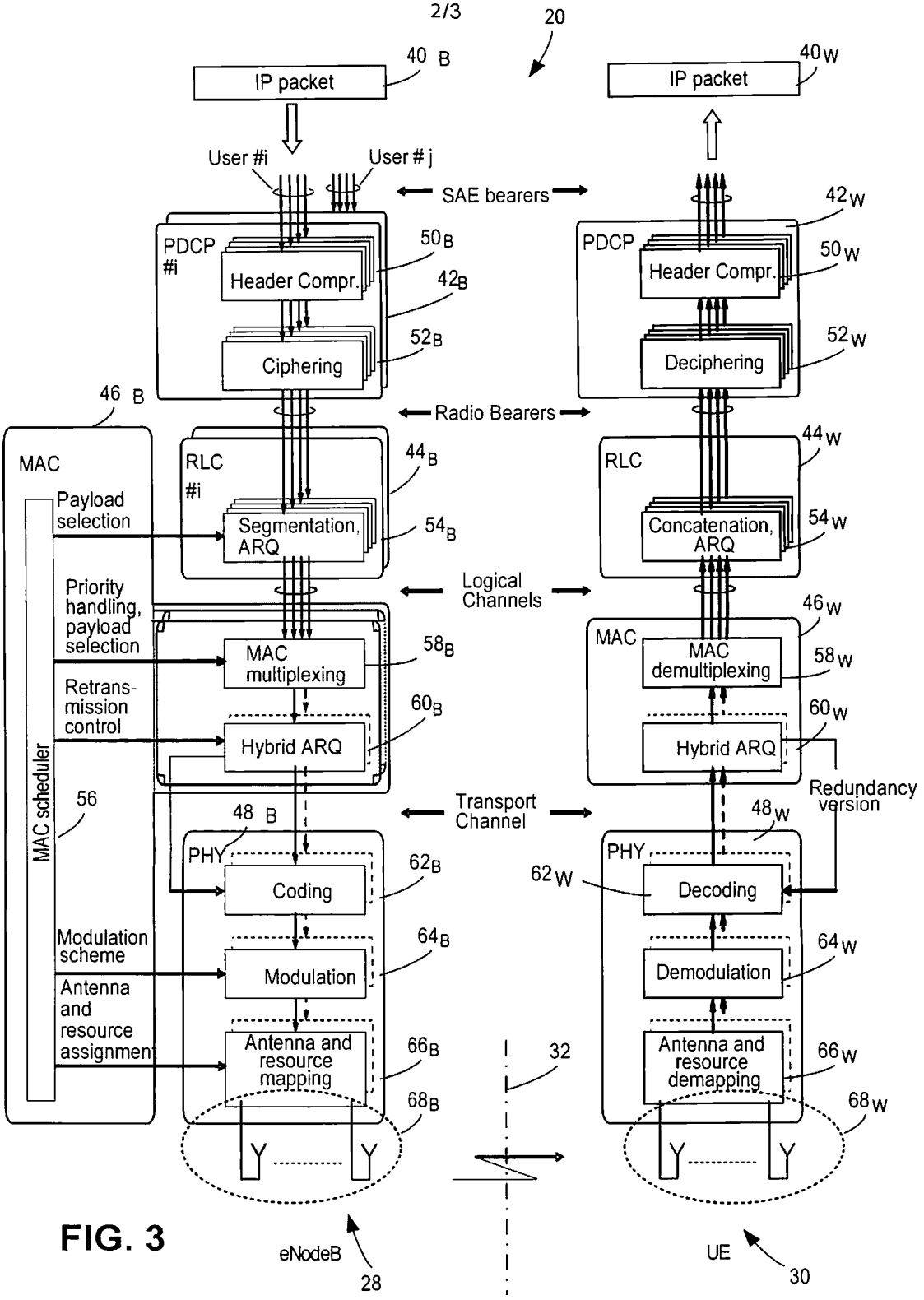

20
IP packet
40 B
IP packet
40W
User #i
User # j
SAE bearers
42W
PDCP
#i
50B
Header Compr.
42B
PDCP
50W
Header Compr.
52B
Ciphering
52W
Deciphering
46 B
Radio Bearers
MAC
RLC
#i
44B
RLC
44W
Payload selection
Segmentation, ARQ
54B
Concatenation, ARQ
54W
Priority handling, payload selection
Logical Channels
46W
MAC
MAC multiplexing
58B
MAC demultiplexing
58W
Retrans-mission control
Hybrid ARQ
60B
Hybrid ARQ
60W
Redundancy version
MAC scheduler
56
Transport Channel
48 B
48W
PHY
Coding
62B
PHY
62W
Decoding
Modulation scheme
Modulation
64B
Demodulation
64W
Antenna and resource assignment
Antenna and resource mapping
66B
32
Antenna and resource demapping
66W
68B
68W
eNodeB
28
UE
30

FIG. 3

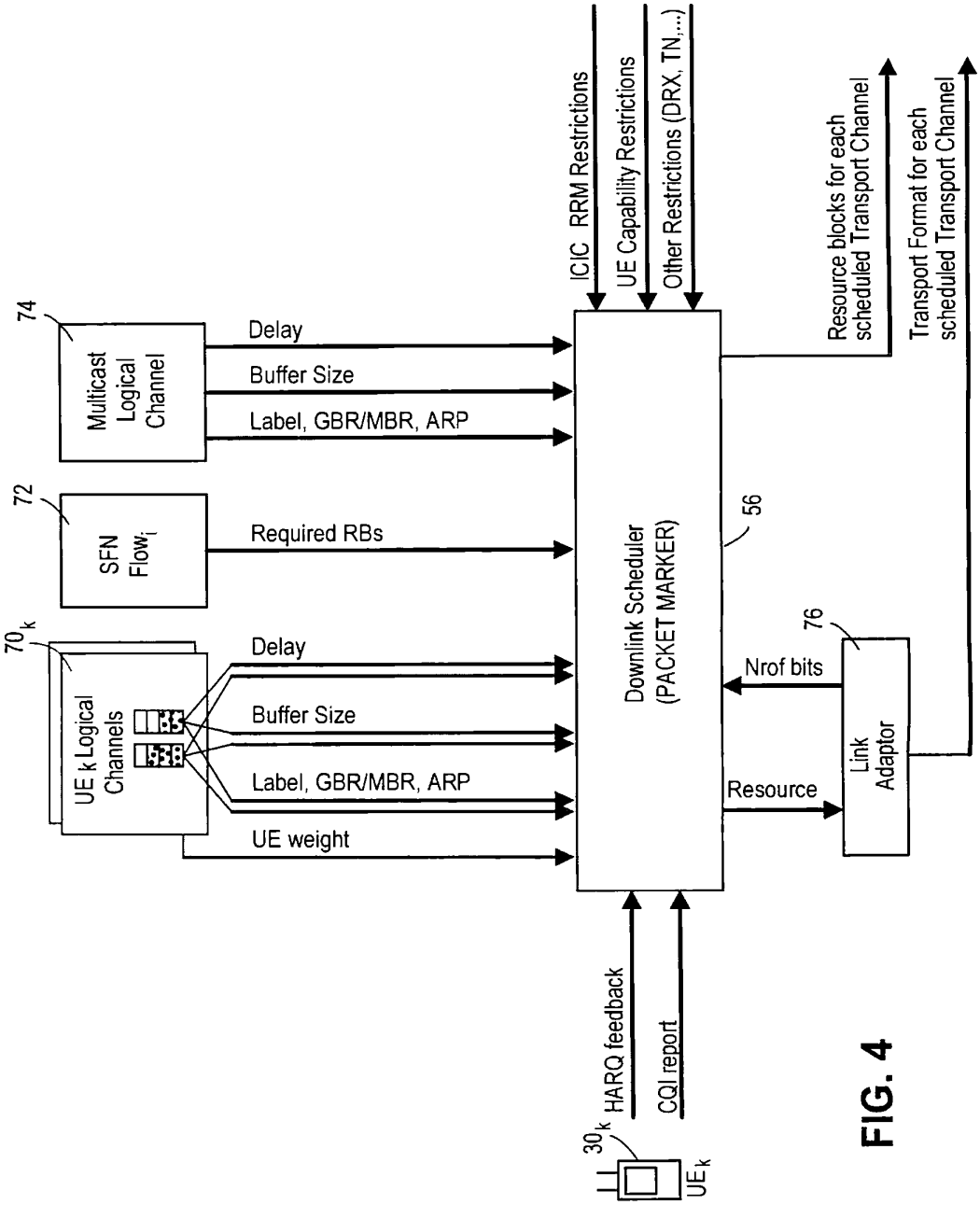

ICIC RRM Restrictions
UE Capability Restrictions
Other Restrictions (DRX, TN,...)
Resource blocks for each scheduled Transport Channel
Transport Format for each scheduled Transport Channel
74
Multicast Logical Channel
Delay
Buffer Size
Label, GBR/MBR, ARP
72
SFN Flow$_f$
Required RBs
70$_k$
UE k Logical Channels
Delay
Buffer Size
Label, GBR/MBR, ARP
UE weight
Downlink Scheduler (PACKET MARKER)
56
76
Nrof bits
Resource
Link Adaptor
HARQ feedback
CQI report
30$_k$
UE$_k$

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050830

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20030086413 A1 (TARTARELLI, S ET AL), 8 May 2003 (08.05.2003), claims 1-28, abstract, paragraphs [0005]-[0047]	1-7,9-15
Y	--	8,16
P,X	US 20080101354 A1 (ARNDT, M R), 1 May 2008 (01.05.2008), figure 4, claims 1-21, abstract, paragraphs [0021]-[0029]	1-16
	--	
Y	EP 1365545 A1 (SIEMENS AG), 26 November 2003 (26.11.2003), abstract, paragraphs [0118]-[0124]	8,16
A	--	1-7,9-15

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2008	19 -11- 2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Elisabet Åselius /LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050830

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02098153 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 5 December 2002 (05.12.2002), page 7, line 13 - page 13, line 5; page 20, line 1 - page 23, line 15, claims 1-29, abstract -- --------	1-16

Form PCT/ISA/210 (continuation of second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.

International patent classification (IPC)
H04L 12/56 (2006.01)
H04L 12/26 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **OVTXPKETAA**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/11/2008

International application No.
PCT/SE2008/050830

US	20030086413	A1	08/05/2003	DE	10220213	A	27/03/2003
				JP	4032231	B	16/01/2008
				JP	2003087316	A	20/03/2003
US	20080101354	A1	01/05/2008	NONE			
EP	1365545	A1	26/11/2003	NONE			
WO	02098153	A1	05/12/2002	AT	410892	T	15/10/2008
				EP	1391128	A,B	25/02/2004
				EP	1876779	A	09/01/2008
				GB	0113214	D	00/00/0000
				GB	2372172	A,B	14/08/2002
				US	20040218617	A	04/11/2004

Form PCT/ISA/210 (patent family annex) (April 2005)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/45315 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US01/43140

(22) International Filing Date:
21 November 2001 (21.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/724,025 28 November 2000 (28.11.2000) US

(71) Applicant: **MICROMUSE INC.** [US/US]; 139 Townsend Street, 5th Floor, San Francisko, CA 94107 (US).

(72) Inventors: **HERRING, David**; 45 Church Road East Crowthorne, Berkshire RE45 7ND (GB). **CARROLL, John, D.**; 4543 North O'Connor Road, Apt. 1249, Irving, Texas 75062 (US). **O'GRADY, Rehan**; Basement Flat, 32 Addison Avenue, Hollamd Park, London W11 4QR (GB). **COLEMAN, Neil**; 40 Belle Vue Road, Quary Bank, West Midlands DY5 1AD (GB). **MARKS, Felix**; 251 Mayall Road, London SE24 OPQ (GB).

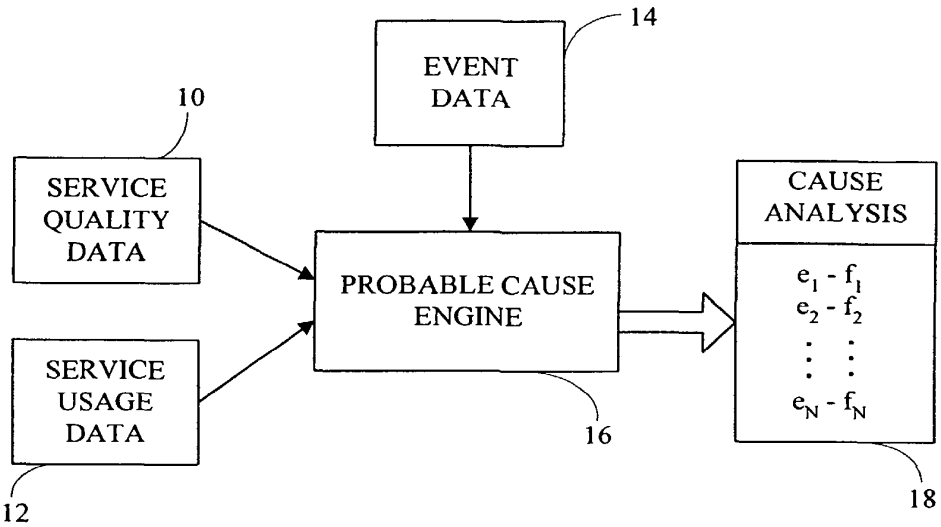
(74) Agent: **OSTROW, Seth. H.**; Brown Rausman Millstein, Felder & Steiner LLP, 900 Third Avenue, New York 10022 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PREDICTING CAUSES OF NETWORK SERVICE OUTAGES USING TIME DOMAIN CORRELATION



(57) Abstract: Method and system are described for predicting the likely causes of service outages using only time information, and for predicting and the likely costs of service outages. The likely causes are found by defining a narrow likely cause window around an outage based on service quality and/or service usage data, and correlating service events to the likely cause window in the time domain to find a probability distribution for the events. The likely costs are found by measuring usage loss and duration for a given point during anoutage and using cost component functions of the time and usage to extrapolate over the outage. These cause and cost predictions supply service administration with tools for making more informed decisions about allocation of resources in preventing and correcting service outages.

WO 02/45315 A2

GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR PREDICTING CAUSES OF NETWORK SERVICE OUTAGES USING TIME DOMAIN CORRELATION

COPYRIGHT NOTICE

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND OF THE INVENTION

The invention disclosed herein relates to the field of fault event correlation and assessment in computerized services such as telecommunications networks or application programs. More particularly, the invention relates to methods, systems, and software for determining likely causes of service outages and assessing the costs of the service outages. The invention described herein is useful in correcting service outages, preventing future occurrences of similar service outages, and determining the appropriate level of resources which should be allocated to correct and prevent such outages.

Maintaining the proper operation of various types of computerized services is usually an important but difficult task. Service administrators are often called upon to react to a service failure by identifying the problem which caused the failure and then taking steps to correct the problem. To avoid wasting resources investigating the wrong problems, administrators must make accurate assessments as to the causes of failures. Because substantial time and resources are often required, administrators must also make accurate decisions as to when to allocate resources to the tasks of identifying problems and fixing them.

A number of tools are available to assist administrators in completing these tasks. One example is the NETCOOL® suite of applications available from Micromuse Inc., assignee of the present application, which allows network administrators to monitor activity on networks such as wired and wireless voice communication networks, intranets, wide areas networks, or the Internet. The NETCOOL suite logs and collects network events, including network occurrences such as alerts, alarms, or other faults, and then reports them to network administrators in graphical and text based formats. Administrators are thus able to observe network events on a real-time basis and respond to them more quickly. The NETCOOL suite

also includes network service monitors of various types which measure performance of a network so that, among other things, network resources can be shifted as needed to cover outages.

Even knowing that events are occurring in real time, however, administrators must still make judgments as to which events are responsible for causing service failures or outages and which service outages are worth the expenditure of resources to fix. Although experienced administrators can usually make reasonably accurate judgments, it is desirable to provide additional application tools which improve the chances that these judgments are accurate.

A number of existing systems attempt to correlate events with service failures. For example, U.S. Patent No. 5,872,911 to Berg describes a system that monitors a telecommunications network for faults and assesses fault data to determine the likely cause of the fault. The system accomplishes this by filtering and reducing the full set of fault data based on a correlation of various faults or alarms. The correlation is performed using a rules-based engine or knowledge base which determines or defines relationships among types of faults. The system then uses the filtered and reduced fault data to determine actual service impact on the network by determining whether a network outage occurred as a result of the fault. The system further determines which customers or equipment are affected by the network outage using conventional mechanisms which track network traffic.

As another example, U.S. Patent No. 5,748,098 to Grace describes a system which uses stored historical data concerning alarms and when they occur to determine the probability of a relationship between events occurring within a window of time. The window of time is either fixed or determined with reference to the nature of the network or the stored historical data. Additional patents, including U.S. Patent No. 5,646,864 to Whitney, U.S. Patent No. 5,661,668 to Yemini, and U.S. Patent No. 6,049,792 to Hart, describe still further schemes for attempting to correlate and relate network faults or alarms using expert systems, logic models, or complex causality matrices.

These patents, which are hereby incorporated by reference herein, describe systems which monitor and attempt to correlate faults in a network. However, among other things, these systems fail to take full advantage of available performance or usage data in correlating events. That is, the inventors have found that a more careful analysis of the level of usage of a service improves the correlation of events to service outages. There is therefore

a need for methods and systems for accounting for service usage information among other data to improve correlation between events and service failures.

Furthermore, there is a need for improved methods and systems for helping administrators make decisions about how to prioritize outages and allocate resources in the correction or prevention of service failures. Commonly assigned application serial no. 09/476,846 and U.S. Patent No. 5,872,911, discussed above, describe different systems for determining the impact of a service failure on customers or users. However, these systems do not quantify the impact in a way to provide the administrator with the ability to compare the effects of outages in different, unrelated services in order to prioritize the allocation of resources, or to perform a strict cost/benefit analysis for the allocation of the resources. Improved methods and systems are thus needed to quantify the cost of a service outage in such a way as to allow the cost to be compared to costs of other service outages in services or systems which may differ in type or use.

SUMMARY OF THE INVENTION

It is an object of the present invention to solve the problems described above with existing network analysis systems.

It is another object of the present invention to improve correlation between events and outages in computerized services.

It is another object of the present invention to improve the correlation without requiring substantive knowledge of the nature of the event and its effect on the service.

It is another object of the present invention to help service administrators make better decisions about how to apply resources to correct service failures.

It is another object of the present invention to quantify the overall cost of a service outage.

It is another object of the present invention to quantify the cost in a way which allows outages in different types of services or systems to be easily compared with one another.

It is another object of the present invention predict the cost of an outage during the outage.

Some of the above and other objects are achieved by a method for analyzing a potential cause of a service change, such as a service outage or service recovery. The method involves monitoring service quality of the service and usage amount of the service, and

determining a service change time window based at least in part upon a change in service quality between a first working state and a second, non-working state as well as upon a change in service usage amount. The service change time window encompasses at least part of a service outage, such as the onset or completion of the outage. As used herein, a service outage or failure is intended to include not only total failures and complete losses of service but also reductions in level of a service to a level considered to be unacceptable or requiring corrective action. The method further involves detecting an event and a time in which the event occurred, and computing a probability that the detected event caused the service change based at least in part on a relation between the event time and the service change time window.

The present invention provides a significant improvement over prior attempts to correlate faults or alarms in a number of ways. For example, in certain aspects of the present invention, three items of information are taken - service quality, service usage, and events - and they are correlated in the time domain, based only on their times. In addition, using both the service quality and service usage data to define a service change time window which is likely to contain or near the cause of a service outage the correlation between the detected event and the service outage.

The method is applicable to various types of computerized services, including: telecommunication networks such as voice or data telephony systems, wired or wireless telephony, email, or instant messaging; computer networks such as intranets, extranets, local or wide area networks, or the Internet; and application programs such as web server software, operating systems, financial system software, etc. The method may be implemented in a computer program which is stored on a computer readable medium such as a magnetic or optical disk and is executed to cause the computer to perform the method.

In some embodiments, the service quality is monitored by a service monitor which regularly polls the service to determine a binary classification of the service as either good or bad. Alternatively, the service quality monitor may identify a number of discrete states of the service, and the administrator selects which combination of the states represents a working state versus a non-working state. The service usage amount is measured by a usage meter, which may be part of the service monitor or another component, and which tracks the level of traffic, performance or usage of the service on a substantially continuous basis.

Since in these embodiments the service quality is monitored by polling, a finding of bad service at some point indicates that an outage occurred at some prior point in time after the last monitored level of good. In some embodiments, the service change time window is determined by first defining a service failure time window bounded by successive readings of good and bad service levels, and then narrowing the service failure time window based upon the service usage amount measured during that service failure time window. This combination provides a more accurate time window encompassing the outage and which more likely encompasses or correlates to the event causing the outage.

The probability that the detected event caused the service change may be computed in a number of ways. In some embodiments, one or more weighting functions are used to compute a probability distribution covering events occurring during the service change time window and within a given time period prior to the window. Although the probability distribution could include events occurring a relatively long time prior to the outage, the likelihood that these older events are responsible for the outage exponentially decreases with distance from the time window and at some point are too negligible to be considered. The weighting functions may be combined to produce a combined weighting function. Exemplary weighting functions used in various embodiments of the invention include:

- a time weighting function for each detected event which decreases exponentially with the distance between the detected event occurrence time or times and the service outage time window;
- a false occurrence weighting function for each event which decreases the probability of the event as the cause of the service outage for instances in which an event of the same type occurred outside the service change time window;
- a positive occurrence weighting function for each detected event which increases the probability of the detected event as the cause of the service change based on instances stored in a historical database in which a detected event of the same type occurred within a prior service change time window; and
- a historical weighting function for each detected event which increases the probability of the detected event as the cause of the service outage based

on instances in the historical database in which a detected event of the same type was identified as having caused a prior service change, perhaps by a user or some automated mechanism.

Some of the above and other objects are achieved by method for analyzing potential causes of a service change. The method involves determining a service change time window encompassing a change of service between a first working state and a service outage, the service change being determined at least in part based on measured service usage levels. For example, a service change may be detected by detecting a step change in service usage, without the need to resort to separate service quality data. A set of events occurring within a given time prior to and during the service change time window are detected, each occurrence of an event being associated with a time at which the event occurred. A probability distribution is computed for the set of events, which probability distribution determines for each event in the set the probability that the detected event caused the service change, the probability distribution being based at least in part on relations between the time of each event occurrence and the service change time window.

Some of the above and other objects of the invention are achieved by a network monitoring system having a service monitor for monitoring quality of service on the network, a usage meter for monitoring usage of the network, an event detector for detecting network events and times at which the network events occur, and a probable cause engine, coupled to receive data from the service monitor, usage meter, and event detector. The probable cause engine sets a service outage time window based upon data received from the service monitor and usage meter, the service outage time window encompassing an occurrence of a service outage in the network. The probable cause engine further determines which of the network events detected by the event detector is the most likely cause of the service outage based at least in part on the relation between the detected network event times and the service outage time window.

Some of the above and other objects of the invention are achieved by a method for quantifying the effect of a service outage over a first period of time. The method involves monitoring or measuring levels of service usage over time, defining a cost of outage time window. The cost of outage time window includes the first time period and a second time period following the first time period. The method further involves computing a cost of the outage as the difference between the measured service usage during the cost of outage time

window and service usage measured in a comparison window. The comparison window is substantially equal in time to the time of the cost of outage window and reflects a similar period of service activity as the cost of outage window, but has no service outage.

In some embodiments, the second period of time is the time in which the service usage returns or recovers from the outage to within a given percentage of a normal service usage level. This recovery should last for more than a mere instant to reflect a return to a state of relative equilibrium, as the service usage is likely to fluctuate following the restoration of service. For example, in an email system, a large number of messages may accumulate in the queue while the email system is down, and a this larger number of messages may be conveyed in a short period of time once the system is returned, resulting in very high volumes. In some embodiments, the second period of time is bounded by a maximum time, e.g., a multiple of the time of the outage.

In some embodiments, the cost of outage is computed in units of service usage. What constitutes a unit of usage depends upon the nature of the service. For example, if the service is a communication service conveying messages, such as telephony or email, the unit of usage is one or more messages. If the service is a network server providing data items such as web pages in response to requests such as from clients, the unit of usage may be a received request or data item provided by a server.

Units of usage may be normalized across different services by converting them to a value such as a monetary value, number of users, time value, or other value representing a loss resulting from not receiving the unit of usage. This may be accomplished by multiplying the units of usage by an assigned value of usage per unit. The normalized value of the service outage cost may then be used by administrators or an automated decision making program to compare costs of difference services and prioritize the allocation of resources across the services to prevent or repair service outages.

In some embodiments, the service usage is continuously monitored, including after the end of cost of outage window, and is used to measure the long term effects of the service outage. This is accomplished by computing the difference between the service usage following the cost of outage time window and a normal service usage level. If the service usage is substantially below or above the normal level following the outage, this is an indication that the outage is of the type that causes loss of use of the service, including loss of users.

Some of the above and other objects of the invention are achieved by a method for predicting a cost of an outage of a service such as during the outage itself. The method involves measuring the time duration for and service usage during the outage, and comparing the measured usage amounts to normal usage amounts measured under similar service conditions for a similar period of time where no service outage occurs, to thereby determine a usage loss amount. This usage loss amount is used to compute a predicted cost of the outage based at least upon a cost component, the cost component comprising a function of the measured time of the outage and measured usage loss amount. The predicted cost of service outage may be compared to a second predicted cost of outage value for a different service so that outages in the two services may be prioritized based on the compared costs.

In some embodiments, the cost components include a service demand cost component representing an affect on service usage based upon the duration of an outage, a customer retention cost component representing a number or percentage of customers lost due to the outage, an agreement penalty component representing penalties arising under one or more service agreements due to a service outage, and a trust loss component representing empirically collected assessments of cost due to loss of trust in the service. The service demand cost component may be computed by multiplying the measured usage loss by a usage loss curve which is a function of time duration of an outage and represents a predicted percentage usage due to an outage based on time duration of the outage. The usage loss curve may be generated using historical data derived from prior service outages.

The methods and systems of the present invention thus provide a service administrator with the ability to more accurately assess what events are likely to have caused a service outage, without the need to know very much about the nature of the events, and to make a more well informed prioritization of service outages and allocation of resources in correcting or preventing the events and corresponding outages.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is illustrated in the figures of the accompanying drawings which are meant to be exemplary and not limiting, in which like references are intended to refer to like or corresponding parts, and in which:

Fig. 1 is a data flow diagram showing a time-based event correlation methodology in accordance with one embodiment of the present invention;

Fig. 2 is a block diagram showing a service with service level and usage monitors in accordance with one embodiment of the present invention;

Fig. 3 is a block diagram showing a network event correlation system in accordance with one embodiment of the present invention;

Fig. 4 is a flow chart showing a process of correlating events with a service outage in accordance with one embodiment of the present invention;

Fig. 5 is a graphical representation of an exemplary set of service quality data;

Fig. 6 is a graphical representation of an exemplary set of service usage data;

Figs. 7-9 are graphical representations of techniques for defining a likely cause window using service level or service usage data in accordance with embodiments of the present invention;

Fig. 10 is a graphical representation of an exemplary time weighting function in accordance with one embodiment of the present invention;

Fig. 11 is a graphical representation of exemplary outages and events;

Fig. 12 is a table showing a probability distribution for the events shown in Fig. 11 to have caused one of the outages shown in Fig. 11;

Fig. 13 is a graphical representation of a technique for defining a likely cause window for a service recovery using service level or service usage data in accordance with one embodiment of the present invention;

Fig. 14 is a flow chart showing a process of predicting the cost of an outage in accordance with one embodiment of the present invention;

Figs. 15A-15B contain a flow chart showing a process of quantifying the cost of a completed outage in accordance with one embodiment of the present invention;

Figs. 16-19 are graphical representations of techniques for quantifying outage costs in accordance with one embodiment of the present invention;

Figs. 20-22 are graphical representations of exemplary cost of outage analyses performed in accordance with embodiments of the present invention;

Figs. 23-34 are graphical representations of techniques for predicting the cost of an outage during the outage in accordance with embodiments of the present invention;

Fig. 25 is an exemplary usage loss curve as a function of time for use in predicting the cost of an outage in accordance with one embodiment of the present invention; and

Figs. 26-28 are graphical representations of exemplary usage loss scenarios for use in generating a usage loss curve in accordance with one embodiments of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present invention are now described with reference to the drawings in the Figures.

One goal of these embodiments is to discover the likely cause of a service outage or service recovery by identifying which event or events occurring in the service are most likely to have caused the outage or recovery. For the sake of simplicity, the following description will focus on predicting costs of service outages, but the techniques and system described herein can be applied to service recovery, as explained further below.

Referring to Fig. 1, three sources of data are used to achieve this goal - service level or quality data 10, service usage data 12, and events and timestamps associated with the events 14. A probable cause engine 16 receives these three sources of data and processes them using various heuristics as described herein to build a probability distribution 18 over the events in the system, based on which events are most likely to have caused the outage. In some embodiments, the probable cause engine uses the service level data 10 and service usage data 12 to define a time window, sometimes referred to herein as a Likely Cause Window (LCW), which has a high probability of containing the event which caused the outage. The events 14 are then related to the outage based upon a time domain correlation. By virtue of the probability distribution, the probable cause engine 16 orders the events and assigns a discrete probability to each event, so that a service administrator may more accurately assess which event caused the outage.

Event data 14 consists of a timestamp and identifier for each event. In some embodiments, the probabilistic analysis performed by the probable cause engine 16 relies only on the time and type of an event, and does not involve or require any further knowledge of what a particular event consists of or the nature of the event. For purposes of the description below, an event is often distinguished from an event type. An event generally refers to a single alarm, alert, or fault generated in or detected by the system monitoring the service. The same happening in the service may generate multiple events. An event type, on the other hand, generally refers to the network happening that generated the events. Events 14 having the same identifier all come under the umbrella of a single event type.

In addition, a specific terminology is used herein in which a set, E, is a set of events. Members of this set are referenced with double subscript notation. Several events may, for example, have the same identifier and hence all represent alarms generated by a single event type. An event type is referred to by a single subscript. Different events of a particular type are distinguished with the second subscript. For example, events e_{11} and e_{12} would refer to two events of type e_1. These events have the same identifier but different timestamps. Event e_{11} represents the first chronological event of type e_1 in the set E, event e_{12} represents the second chronological event of type e_1, event e_{21} represents the first chronological event of type e_2 in the set E, and so on.

The service level or quality data and service usage data are collected through any conventional devices depending upon the particular service. For example, referring to Fig. 2, in one embodiment of the invention, a service accessed by a number of end users 22 is monitored by service level monitors 24 as well as usage meter(s) 26. As shown, the usage meter or meters measure the total amount in which the service is used. This measurement will depend upon the nature of the service. For example, in a telecommunication service, the usage meter 26 measures the number of messages being conveyed by the service in an hour or other time period. Such a telecommunication service may include a wireless telephony system using the smart message service protocol, in which the usage meter measures the number of messages conveyed over the system. Similarly, in a computer network, the amount of traffic may be measured over a given period. For a service consisting of an application software program, the usage may be measured in any appropriate manner, such as time spent, number of memory calls over time, number of documents accessed over time, etc.

The service level monitors 24 monitor the status of the service on a polled basis. That is, they poll the service on a regular basis to determine whether the service is working. In some embodiments, this inquiry is binary in nature, resulting in a status of either working or non-working, sometimes referred to herein as a status of good or bad service. Alternatively, the service level monitors 24 may detect several types of service status, and an outage would be defined as desired as a transition from one status in which the service is considered to be working properly to a second status in which it is not providing an acceptable level of service. Multiple discrete service monitors 24 may be used to monitor the quality of service from different locations. For example, for a network accessible from several remotely located sites, each site would have a service monitor 24 to monitor the

quality of service being received at that site, while the traffic on the entire network would be measured by usage meters 26.

As explained further below, the service quality and service usage data are singly or jointly used to detect when an outage has occurred in the service. As used herein, an outage of a service is generally a period or window of time during which positive affirmation of the service being good or acceptable can not be obtained. When an outage is detected by a service monitor 24, for example, an outage time window contains one or more bad polls and is bounded at each end by two good polls. This guarantees that the outage window encompasses the entire outage incident.

One embodiment of the present invention implemented in a computerized network environment is shown in Fig. 3. In this embodiment various activity on a network 30 is monitored by a network monitoring system 32, such as the NETCOOL suite available from Micromuse Inc., as described above. Other commercially available network monitoring systems 32 may be used, as would be understood by one skilled in the art. The network monitoring system 32 works in conjunction with one or more service quality monitors 24, such as Internet Service Monitors, a set of active monitors which work with the NETCOOL suite to provide availability information on Internet service elements including DNS, HTTP, LDAP, POP3, RADIUS, SMTP, and TCP Port Monitoring, or NT Service Monitors, which work with the network monitoring system 32 to collect management events from a network operations center regarding Windows NT environments.

Further, a set of service usage meters 26A, 26B, and 26C work with the network monitoring system 32 to track the amount of activity seen at different locations on the network 30. In particular, in some embodiments service specific usage meters 26A track activity on different services 34 available within the network, including, for example, a cache server, an email server, Radius, HTTP/HTML, LDAP, and other applications and services available to end users over the network 30. Other, network edge usage meters 26B measure activity in and out of the network, including, for example, a usage meter 26B detecting activity at a firewall monitoring application which collects security information, a usage meter 26B at Cisco Net Flow, a usage meter 26B at a PIX firewall, and others as known to those skilled in the art.

Furthermore, network sniffing usage meters 26C, sometimes referred to as snooping agents, capture and listen to packets on the network received at a network interface.

Examples of conventional network sniffing usage meters include Snoop, Etherreal, and Etherfind. Etherfind, for example, examines packets traversing a network interface and outputs a text file describing the traffic. In the file, the text describing a single packet contains values such as protocol type, length, source, and destination. Further packet filtering can be done on the basis of protocol, e.g., IP, ARP, RARP, ICMP, UDP, TCP, and filtering can also be done based on the source, destination addresses as well as TCP and UDP port numbers.

Events are detected by the network monitoring system 32 through probes or similar conventional mechanisms and are stored in an event object server 40. The object server is an object-oriented data repository where information on events is stored, viewed and managed. Events are stored as objects on the server 40 which can be more easily manipulated for processing. A gateway 42 allows a mediator program suite 44 to share the event data stored in the object server 40. The mediator program suite 44 includes the probable cause engine 16 as well as a cost of outage engine 46 for quantifying the effect of an outage, as described in greater detail below. An administrator desktop and user interface 48 allows a network administrator to interact with the mediator 44 and execute the probable cause engine 16 and cost of outage engine 46.

The operation of one embodiment of the probable cause engine 16 is now described with reference to the flow chart in Fig. 4 and the graphical diagrams in Fig. 5-13. Referring to Fig. 4, the probable cause engine receives service quality data from service quality monitors and service usage data from the service usage meters, step 60. This received data is used to detect the occurrence of an outage, step 62. When an outage is detected, the probable cause engine defines a time window, sometimes referred to herein as the likely cause window or LCW, using the service quality data, service usage data, or preferably both, step 64. The probable cause engine then retrieves event data from the event object server for events which occurred during the defined likely cause window and for a period prior to the LCW, step 66. The events retrieved are each assumed to have a non-zero probability of having caused the outage, and it is further assumed that at least one of the retrieved events caused the outage. The engine then computes a probability distribution for the events which maps the probabilities that each event caused the detected outage, step 68. These probabilities are then associated with the events and output to the administrator in a suitable form.

Particular implementations of steps in this methodology are now described with reference to the graphs shown in Figs. 5-12. Figs. 5 and 6 illustrate sample data sets for service quality and service usage, respectively. As shown in Fig. 5, service quality data consists of a series of points 80 regularly spaced at points in time. As shown, the service quality is monitored at one of two levels or states - good and bad - although a number of quality states might be detected. The classification of a quality state as good or bad is defined in the service monitor configuration by its discrete measurement classification. For purposes of simplicity in this application, it is understood that a transition from one of such states to another of such states is considered to represent a failure or outage in the service, with the definition of what loss of service constitutes an outage being a design consideration.

Fig. 6 shows service usage data consisting of a greater number of points measured on a significantly more continuous basis. The service usage data points may be measured on an entirely continuous basis, e.g., every email message conveyed or every HTTP request is counted, or sufficient samplings of usage may be taken to accurately represent the actual usage of the service.

As explained above, the service quality and service usage data are used to detect outages and define the likely cause window. For purposes of this discussion, time windows are understood to generally cover continuous subsets of the time line. In the notation used below, square brackets denote inclusion of endpoints in the subset, while round brackets mean the end point is not included. For example, given two times a and b, a window (a,b] denotes a time window starting but not including time a and ending at and including time b. In addition, for an event e, and a window, W, the notation $e \in W$ indicates that the timestamp associated with event e falls within the window W.

Figs. 7 and 8 illustrate two ways in which outages are detected and the likely cause window is defined. One method of detecting an outage is through the service quality data received from a service monitor. As illustrated in Fig. 7, when a poll of the service monitor registers as bad for the first time following one or more pollings of good quality, the probable cause engine interprets that the service went bad at some stage between the current bad poll and the previous good poll. The time window between these two polls is defined as the service failure window or SFW. In the diagram in Fig. 7, the SFW is the set (b,c]. The time period between two readings of good in the service quality data in which one or more bad quality readings are monitored is defined as the outage window. In Fig. 7, the outage

window is the set (b,e). As described in greater detail below, the outage window is used among other things by the cost of outage engine to predict the cost of the outage and to quantify the cost of the outage in terms which may be compared to other service outages for purposes of prioritizing the application of resources in response to the outages.

In the absence of further information, the probable cause engine defines the LCW as the SFW plus a small, preset time tolerance consisting of the windows [a,b] and [c,d]. The LCW thus represents [a,d] in the diagram in Fig. 7. Alternatively, the time tolerances are set to zero, in which case the LCW = the SFW.

Alternatively, the probable cause engine detects an outage using only the service usage data, without necessarily resorting to the service quality data. In this embodiment, illustrated in Fig. 8, the engine detects a usage step change and verifies based on the step change whether the service has gone bad. To detect a usage step change, the probable cause engine detects a changepoint in a univariate time series, the time series consisting of the discrete measurements of units of usage. If a change in the service quality has already been detected by a service monitor, the SFW is defined as explained above as the period during which the service outage started. The usage step change is found in this window using an offline changepoint detection algorithm. Some such algorithms are described in Booth, N.B. and Smith A.F.M. *A Bayesian approach to Retrospective Identification of Change Points*, J. Econ., 19, (1982), which article is hereby incorporated herein by reference. If service quality data is not available, the probable cause engine analyzes the service usage data itself to detect an outage. This analysis employs an online changepoint detection algorithm. Some online changepoint detection algorithms are described in Basseville, M and Nikiforov, I.V., *Detection of abrupt Changes, Theory and Applications*, Prentice Hall, Englewood, New Jersey (1993), which article is also incorporated by reference herein.

As with an outage detection based on service quality change alone, the LCW may be defined by the probable cause engine as the time window from briefly before the usage step change up to and including the step change. However the outage is detected, clearly getting a tight bound on when the actual outage occurred is important to determining which event caused the outage. The smaller the LCW, the more likely it is that the probable cause engine will be able to pinpoint the event which caused the outage. Preferably, the

LCW should be the smallest time window that can reasonably be specified in which the data indicates the outage occurred.

In some embodiments, then, the probable cause engine uses the usage step change to provide a tighter bound on a SFW previously established using service quality data. As above, a service monitor detects that the service quality has gone bad. With the addition of usage data, however, the probable cause engine puts a much tighter bound on the SFW to produce a narrower LCW. This is illustrated in Fig. 8, in which the service quality data of Fig. 7 is shown in conjunction with usage data. It will be recognized by one skilled in the art that, for purposes of comparing the two types of data and graphing them together in Fig. 8 and later drawings, either or both of the service quality data and service usage data have been normalized. The probable cause engine analyzes the usage data for the time period within the SFW found through the service quality data and detects a usage data step change. The LCW is then defined as the period of the step change plus time tolerances.

As a result, in some embodiments the definition of the likely cause window is based on the service quality and service usage data received regarding a specific service. In other embodiments, the probable cause engine considers outages in other services to achieve a more refined definition of the service failure window and ultimately the likely cause window. This is based on a theory that the cause of an outage under consideration often causes outages in other, related services. Thus, referring to Fig. 9, the engine identifies related services as services experiencing an outage whose service failure window overlaps with the service failure window for the outage under consideration. Alternatively, the engine can use stored information about the relatedness of various services, e.g., a knowledge base or expert system. The engine then superimposes the service failure window for the main or principle service with service monitor or usage meter data received regarding the related services. This results in a smaller composite service failure window, as shown in Fig. 9, and thus improves the probable cause analysis. If the probable cause engine is performing the analysis on a service which has recovered, as described below, then a similar condition can be applied to the corresponding service recovery window.

Once the probable cause engine identifies a likely cause window, it retrieves event data defining a set of events and builds a discrete probability distribution function, P, such that for any event, e, the probability that this event caused the service outage is $P(e)$. The probability distribution, P, is based on heuristic observations of cause and effect. While

many suitable heuristics will accomplish the task, four heuristics are described below, one for each criterion included in the model. In some embodiments, each heuristic can be considered on its own. Alternatively, two or more of these four heuristics are incorporated by means of mathematical weighting functions. A probability is assigned to each event type, rather to each individual event.

A first heuristic is a time weighting function T(e). This function reflects the heuristic that events in the outage window are much more likely to have caused the service outage than events outside it. Indeed, the probability assigned to events outside the outage window should decay as we move further away from the outage window.

A second heuristic is a false occurrence weighting function FO(e). This function reflects the heuristic that if an event appears many times in the retrieved set of events E, while the service was good, this event is less likely to have caused the outage. The more times an event has occurred outside of any outage window, the less probability is assigned to it.

A third heuristic is a positive occurrence weighting function PO(e). This function reflects the heuristic that the more previous outage windows an event has appeared in, the greater the probability that it has caused the current outage. The use of this heuristic requires the storage of event and outage data for reuse in later analyses.

A historic or user input weighting function U(e) reflects information provided by users of the system in the past, as stored in a database. If a user of the system has, in the past, associated a previous outage with a particular event, then this event is assigned a much higher probability. The more times an event has been associated with previous outages (by a user), the higher the probability is assigned to it.

An overall weighting function F(e) is defined as follows:

$F(e) = T(e) * FO(e) * PO(e) * U(e)$

In building the distribution, the probable cause engine computes the distribution such that the sum of all the probabilities for each of the different events is 1, i.e., if the set of events, E, contains n events, $e_1, \ldots, e_n$, then Sum(P(e1), ... , P(en)) = 1. The engine accomplishes this by discounting each of the individual weights by the sum of all the weights. Thus an event, e, has probability

$$P(e) = \frac{F(e)}{\sum_{i=1}^{n} F(e_i)}$$

And as required,

$$\sum_{i=1}^{n} P(e_i) = 1$$

Exemplary weighting functions used by the probable cause engine are now described. As will be understood by one skilled in the art, other weighting functions may be used within the spirit of the present invention to achieve a probabilistic time domain correlation of events and outages.

For the time weighting function, a certain constant weighting, K, is assigned to events inside the LCW. The function models an exponential decay in the weighting assigned to events, decreasing as events occur further away from the LCW. Let e_{ij} be an event, and let [a,d] define the LCW on a timeline. Let *t* be the minimum absolute distance from the event e_{ij} to an endpoint of the LCW. If e_{ij} is in the LCW, then t =0. $T(e_{ij})$ is thus defined as follows:

$T(e_{ij}) = K$ If $a \leq \text{timestamp}(e_{ij}) \leq b$

$T(e_{ij}) = K*2^{-t/(d-a)}$ If $\text{timestamp}(e_{ij}) < a$

$T(e_{ij}) = K*2^{-2t/(d-a)}$ If $\text{timestamp}(e_{ij}) > b$

This choice of $T(e_{ij})$ assigns a weighting of K/2 to an event occurring at time a - |LCW|, and a weighting of K/4 to an event occurring at time b + |LCW|. The time weighting function for an event of a given type is then defined as the maximum over all the events of that event type, or

$T(e_i) = \max_j (T(e_{ij}))$

A resulting time weighting function having exponential decay is illustrated in Fig. 10.

For the positive occurrence weighting function, defining posOcc(e) as the number of previous occurrences of events of this type inside LCWs, the function may be defined as follows:

PO(e) = 1 if posOcc(e) = 0

PO(e) = 2 if posOcc(e) = 1

PO(e) = 4 if posOcc(e) ≥ 2

An alternative definition of this function is:

PO(e) = 1 if posOcc(e) = 0

PO(e) = posOcc(e)*1.5 if posOcc(e) > 0

For the false occurrence weighting function, defining negOcc(e) as the number of previous occurrences outside any outage windows, i.e., during periods of good service uninterrupted by outages, the false occurrence weighting function can be defined as:

$FO(e) = 1$ if $negOcc(e) = 0$

$FO(e) = 1/2$ if $negOcc(e) = 1$

$FO(e) = 1/4$ if $negOcc(e) \geq 2$

An alternative definition of this function is:

$FO(e) = 1$ if $negOcc(e) = 0$

$FO(e) = 1/(negOcc(e)*1.5)$ if $negOcc(e) > 0$

For the historic or user input weighting function, defining userPrevSelected(e) as the number of times events of this type have previously been selected by a user as having caused an outage of this service, the function may be defined as

$U(e) = 1$ if $userPrevSelected(e) = 0$

$U(e) = userPrevSelected(e)*4$ if $userPrevSelected(e) > 0$

Thus, using these exemplary weighting functions, the probability distribution is performed in the time domain, relying only on the temporal relation of events to the likely cause window containing the outage. The invention thus advantageously avoids the need to take into account of the nature of an event, but only needs to consider its timestamp and identifier. As will be recognized by one skilled in the art, this information and previous user knowledge may be incorporated to add more sophisticated weighting to the probability distribution performed by the probable cause engine. For example, the engine may account for where on the network an event occurred or on which type of device.

The understanding of the invention will be enhanced through an example. The service quality data and event data for the example is illustrated in the diagram in Fig. 11. The probable cause engine is concerned with the second of the two service outages shown in the Figure, and is trying to find the most probable cause for this second outage. The set of events, E, contains eight event types (event types e_1-e_8) and fourteen instances of events. The engine retrieves stored data showing that a user previously nominated event type e_2 as the cause of a previous outage of this service. Applying the functions provided above, the probable cause engine determines a probability distribution as shown in the table in Fig. 12, where the event types are ordered on the probability of having caused the outage. The table

in Fig. 12 also shows how the different weighting functions have influenced the probability assigned to each event type.

The probable cause engine can also be used in a similar manner to that previously described to identify the resolution of a service and predict its likely cause. To predict service resolution a service quality change is detected by a service monitor and/or a usage change showing the service changing from a non-working state such as an outage to a good status. From this, a service recovery window (SRW) is defined, as illustrated in Fig. 13. A likely recovery window (LRW) is initially defined as the SRW plus a small preset time tolerance, or using any of the other techniques for leveraging service usage data as described above. Then, in a similar manner as previously described for service failure, the LRW can be refined based upon current usage data for the service and sympathetic services which have overlapping LRW's. A series of weighting functions can similarly be applied to the events to assign probabilities as to which event caused the service to recover.

This service recover analysis is useful, among other things, within systems which have auto-correction with discrete devices or in which changes are being made to devices independent of the knowledge of the service outage - which nevertheless are service effecting.

Using these algorithms, the probable cause engine identifies the most likely cause(s) of a service outage or service recovery. This helps network administrators identify these events as ones which should be prevented or more quickly fixed to minimize the likelihood of future outages, or to identify events which work towards correcting outages sooner to enhance the chances of a quicker service recovery. However, when outages in different services, or the events that are likely to cause them, occur at around the same time, administrators need to prioritize the outages or events to properly allocate resources. The cost of outage engine in the mediator assists the administrator in this evaluation.

The cost of outage engine, sometimes referred to herein as a costing engine, relies on historical service usage data for a service stored in a database accessible to the mediator. The cost of outage engine analyzes the usage which takes place over a window of time which incorporates a service outage with comparison to the usage which has taken place during a similar comparison window of time without a service outage. This comparison is used to predict or calculate a loss in service usage due to this outage. This is then recalculated as a monetary loss by applying a value to the usage of the service. This

quantifies the motivational factor for fixing a current outage and the motivational factor for ensuring a previous outage is not repeated. The cost of outage engine performs its analysis during a service outage and retrospectively for a previous service outage.

Referring to Fig. 14, as explained above the service quality monitors regularly poll the service for quality level and the service usage meters continuously measure the activity in a service, step 84. If a service outage is detected, step 86, based on the service quality or service usage data using techniques described above, the costing engine predicts the cost of the outage based on the current outage window length, for current outages, and including various extended outage windows for completed outages, step 88. The use of window lengths to predict and compute outage costs is described in greater detail below. Once a predicted cost is computed, it is compared to the outage costs determined for other services, step 90. This comparison may then be used to prioritize outages and allocate resources to the service outages, step 92.

As a result, the costing engine both predicts costs of ongoing outages and computes costs for completed outages which have at least partially recovered. Because the prediction of outages is based in part on historical computations of outage costs, specific techniques for computing outage costs for completed outages are described first, followed by specific techniques for predicting costs of an outage during the outage.

Turning first to computing outage costs, and referring to Figs. 15A-15B, the service quality monitors regularly poll the service for quality level and the service usage meters continuously measure the activity in a service, step 100. For purposes of this aspect of the invention, the usage meters preferably measure the usage in units of usage. The unit of usage varies according to the service being measured, and is typically measured over a timed interval. For example, a unit of usage for a web server is the number of hits on the web server in a minute; for an email server, the number of emails sent and received by a company per hour; for a mobile telephone service, the number of mobile phone calls made by an individual per hour.

If a service outage is detected as completed, step 102, using techniques described above for detecting the onset of an outage and its at least partial recovery, an outage window is defined using the service quality data and/or service usage data, step 104. For example, as described above, the outage window may be defined as the period between two service quality readings of good service with one or more bad quality readings in between.

The cost of outage engine then defines an extended window which includes the outage window and a second time window, step 106. This extended window is referred to herein as a cost of outage window. The cost of outage window is the time span over which the usage data is considered for any given outage, with the goal being to analyze the usage data over a period corresponding to that which incorporates all the effects of the outage on usage patterns. The cost of outage window thus extends beyond the bounds of the outage window to pick up the recovery in usage, subsequent to the outage.

The cost of outage window is limited to a time frame around the outage, and in some embodiments is initially defined in terms of a time span equal to a multiple of outage windows in duration, starting at the same time as the outage. In one embodiment, the cost of outage window is set equal to four times the outage window in length, starting at the same time the outage window begins and continuing for three outage windows duration past the end of the outage window. This is illustrated in Fig. 16.

In accordance with the invention, the cost of outage window can be reduced from the full window if the time to recover occurs within this window. Thus, returning to Fig. 15A, the cost of outage engine determines whether the service recovered during the extended cost of outage window, step 108. The cost of outage engine determines a recovery as the return to "normal" service usage, with normal service varying and being service specific. In some embodiments, a recovery occurs when the units of usage are within 75% - 90% of the same units of usage for the comparison window, explained further below. In other embodiments, a recovery is considered to occur when the units of usage remain within a range of plus or minus 20% of the comparison window's usage value for a sustained period equal to 1/4 the outage window in length, as illustrated graphically in Fig. 17.

If the service usage does not recover within the cost of outage window, the cost of outage window is defined as the full, extended cost of outage window, e.g., four times the outage window, step 110. If the service usage recovers during the cost of outage window, the cost of outage window is shrunk to end at the recovery time, step 112, i.e., the cost of outage window is set at the outage window plus the time to recover. This shortening of the cost of outage window to the time to recover is illustrated in Fig. 18.

Once the cost of outage window is set, the cost of outage engine defines a comparison window, step 114, as having a time period equal in length to the cost of outage window and chosen to reflect a similar period of activity as would have occurred during the

cost of outage window, had there not been an outage. The definition of the comparison window typically takes into account the cyclic nature of service access, and is typically the same period of time for the previous day/week/month or year. In most corporate services this is the previous week. The cost of outage engine then retrieves the service usage data collected and stored for the defined comparison window, step 116.

The measured usage data for the current cost of outage window is then compared to the retrieved usage data for the comparison window, step 118. This comparison yields several important items of information. For example, the cost of outage engine uses this comparison to compute a percentage peak usage, as the highest percentage units of usage recorded during the cost of outage window when calculated as a percentage against the comparison window. This can be used as a measure of demand for a service after an outage has occurred, i.e., a service usage overshoot. In addition, the cost of outage engine can compute a percentage minimum usage as the minimum units of usage recorded during a cost of outage window, computed in one embodiment as a percentage based upon the previous service usage in the comparison window. This computed comparison can be used as a measure of how complete the service outage was. These two computed values are illustrated on the usage data shown in Fig. 19.

A primary purpose of comparing the service usage data in the cost of outage window is to determine the effect of the outage on overall service and users. Thus, returning to Fig. 15B, the cost of outage engine compares the usage data in the two windows to determine whether any loss of usage occurred, step 120. This comparison is performed as the difference over the cost of outage window compared the comparison window. If the difference is zero or negligible, the cost of outage engine determines that loss of service usage occurred, and that the service made a full recovery, step 122. Otherwise, the engine computes the loss of service, step 124.

In addition, the cost of outage engine analyzes the usage data at the instance at the end of the cost of outage window to normal levels as represented in some embodiments by the levels depicted in the comparison window, step 126, and determines the difference, step 128. This difference in actual and expected service usage at the end of the cost of outage window, sometimes referred to herein as percentage churn, is considered as a measurement of the long term effect of this outage. For example, this computed difference may be used as an indication of the loss of users to the service, perhaps because of the increased difficulty in

accessing the service or lost opportunity. The units of usage in the percentage churn is converted to a number of users by dividing the usage units by a conversion factor representing a number of usage units per user. This calculated number of users may then be converted to cost by multiplying the number of users by a factor representing a set cost per user.

In order to make the loss of usage valuable as a tool to compare various types of service outages, the loss of usage and related computed values must be normalized against different services. This is accomplished by applying a value of usage weighting, where the value of usage represents, for example, the monetary loss to an organization for not achieving a given unit of usage. This may vary as a function of time, the individual or group attempting that unit of usage, etc. The cost of usage is computed, step 130, by multiplying the loss of usage by a set value of usage represents the monetary cost of the outage. Once the usage values are normalized, the cost of outage engine can compare the costs of two or more outages, for example, outages which may be overlapping, and prioritize them based on cost.

This aspect of the invention would be better understood by the application of this methodology to several examples of service failure. In the first example, a momentary (e.g., less than one minute) loss of service is detected for a corporate email service. As shown in Fig. 20, the time to recover defines and shortens the cost of outage window, and there is a service overshoot as a result of the pent up demand caused by a small time of outage. One can infer a stickiness for different services in the likelihood of a user returning to use the service after a service outage. Many factors effect the stickiness of a service, such as alternative options, importance of service to user, etc. Ideally, from a service usage perspective, a service overshoot should equal the loss of usage area, meaning that effectively there was zero loss in service usage as a result of this small service outage. There is no percentage churn as the time to recover defines the cost of outage window.

In a second example, a corporate web service fails for a medium period (e.g., less than three hours). As illustrated in Fig. 21, the cost of outage engine finds a definite loss in usage of the service, showing that any intended usage of the service during the outage has not been carried forward to when the service was restored. However the usage has recovered to show no overall percentage churn.

In a third example, an e-commerce web service fails for a relatively long period (e.g., one day). As illustrated in Fig. 22, the cost of outage engine finds effects of the

outage lasting beyond the cost of outage window, giving a percentage churn value of approximately 50%.

As described herein, the cost of an outage is thus determined based on three basic factors - the type of service, the length of the outage window, and the time the outage occurred.

The description turns now to techniques used by the cost of outage engine for predicting the total cost of an outage during the outage based on a given outage length. This cost prediction may be used, among other things, to assess the priority of allocating resources to fix this outage. In some embodiments, the prediction of service outage cost is based on the results of a combination of outage costing components. Each costing component is a function that returns a cost when given an outage length among other possible variables. Each costing component model a particular way an outage can cost money.

In some embodiments, the costing components include the following:

- a component modeling service demand behavior in relation to the length of service outage, covering the short to medium term effects of a service outage and derived from empirical observation, represented herein as C_d;
- a component modeling level of customer retention in relation to the length of outage, represented herein as C_r;
- a component modeling penalty clauses in service level agreements (C_p); and
- a component modeling loss of trust in the service or the company providing the service, based upon historical or empirical data, represented herein as C_t.

Each costing component produces a monetary cost using some or all of the following data: length of outage, usage levels at time of outage, historical usage trends, and empirical knowledge. The total monetary cost C is a sum of the component costs:

$$C(\text{outage}) = C_d(\text{outage}) + C_r(\text{outage}) + C_p(\text{outage}) + C_t(\text{outage})$$

The Service Demand component embodies how the length of outage affects the short to medium term usage of a service. The two diagrams in Figs. 23 and 24 illustrate the anatomy of an outage. The measured usage during an outage determines the severity of the outage. A complete outage results in no measured usage. Usage measured during an outage is treated as fulfilled demand, and the usage loss is measured as the difference

between expected or normal usage as determined, for example, by service usage during a comparison window, and the measured usage, as shown in Fig. 23. The service demand component aims to derive a cost for all usage loss attributable to the given, current outage. The loss of usage includes usage lost in the outage window as well as predicted usage lost and regained during the recovery period, as shown in Fig. 24.

The costing engine computes the service demand cost component using a Usage Loss Curve. For purposes of this discussion, it should be understood that usage loss refers to the absence of usage, either measured or projected, as compared to usage measurements for a comparable period, and total usage loss for an outage refers to the combined usage loss from both the outage window and the recovery period.

An example Usage Loss Curve is shown in Fig. 25. The horizontal axis represents outage window length, that is, the measured duration of the outage. The vertical axis represents total usage loss as a percentage of usage loss in the outage window. In Fig. 25, the vertical axis plots 100 * (total usage loss / usage loss in outage window). This allows the predicted total usage loss for an outage in progress to be derived from the measured loss in usage and the current length of the outage. For this prediction the final outage length is taken to be the current outage length. This method is also used to predict the costs of an outage when the outage is not expected to finish at the time the prediction is made. Modeling such a scenario relies on the assumption that level of usage in the outage window will remain constant from the last measured usage value to the projected end of the outage window.

In the exemplary, typical service demand curve shown in Fig. 25, the letters A-E on the length of outage axis denote inflection points and are used to illustrate some of the features of a Usage Loss curve. To point A, outage length is zero, and no outage has occurred. From points A - B - 0% usage loss – all usage missed during outage is regained post outage. From points B-C – 0-100% usage loss – outage affected usage – some usage lost during outage is not recovered. From points C-D – 100% usage loss – all usage missed during outage is lost. From points D-E – 100-200% usage loss– all usage missed during outage is lost and outage causes post usage to be affected.

During an outage, the costing engine estimates cost of the outage using the service demand curve and the Usage Loss curve. In some embodiments, the engine uses the following formula:

C_d(outage) = (usage lost in comparative usage window up to time O_L) x F_U (O_L) x (cost unit multiplier),

Wherein

O_L is the length of the outage, which may be the length of the outage to date or the length of the outage at some future point; and

F_U is the function represented by the Usage Loss Curve.

Usage Loss Curves for service instances and types may be derived from previous outage analyses. For each previous outage of a service two variables are extracted: total usage loss as a percentage of usage loss during the outage window, and length of the outage window. Outage data from a series of outages may be transformed into a Usage Loss Curve using a local regression model such as Lowess, as described in W. S. Cleveland, *Visual and Computational Considerations in Smoothing Scatterplots by Locally Weighted Regression*, Computer Science and Statistics: Eleventh Annual Symposium on the Interface, pages 96-100, Institute of Statistics, North Carolina State University, Raleigh, North Carolina, 1978, which is incorporated herein by reference.

In some embodiments the transformation of outage information into a Usage Loss Curve is improved by applying usage patterns to the outages. These are used to better determine the amount of usage lost. Usage patterns have two components:

- Method to identify pattern – expressed as a set of rules.
- Method to calculate usage loss percentage, i.e., total usage lost as a percentage of the usage lost during the outage, which is expressed as a equation.

Both methods make use of the following set of functions and values:

- OW- outage window length
- T_S – outage start
- T_E – outage end
- C_{USAGE} (T_1,T_2) – the expect usage between points T_1 and T_2 based on comparative usage data
- S_{USAGE} (T_1,T_2) – the usage between points T_1 and T_2 seen in the current usage data.

A number of usage patterns are identified and defined on the basis of observations of human interaction with a service during the outage recovery period. These

usage patterns are described with reference to Figs. 26-28. In other embodiments patterns may be used that model the behavior of Internet protocols and hardware during outages.

A first such usage pattern, a blip outage, has the characteristics of a short length outage, that usage lost during outage is regained post outage, and that users are typically unaware of the outage. An exemplary blip outage is a one minute POP3 outage, in which emails not served during the outage are served when the outage completes. Fig. 26 graphically represents this usage pattern, in which overshoot usage during recovery makes up for lost usage during the outage. This pattern may be defined by the rule that greater than 75% of the usage loss in the outage window is recovered within one outage window past end of outage. The usage loss during this usage pattern is zero, and the identification rule for this usage pattern is:

$$[S_{USAGE}(T_E,T_E+|OW|) - C_{USAGE}(T_E,T_E+|OW|)] > 0.75 * [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$$

A second usage pattern, a loss outage, has the characteristics of a medium length outage in which usage that would have occurred during the outage period is not regained when outage ends, and that users are aware of the outage. An example of a loss outage is a one hour POP3 outage, during which the telephone is used as an alternative to email during outage period. The usage graph of a loss outage is shown in Fig. 27, in which the usage loss during the outage exceeds the usage gained during recovery. A loss usage may be defined as one in which less than 25% of the usage loss during outage is recovered within 3 outage windows past end of outage. The identification rule for this usage pattern is:

$$0 \le [S_{USAGE}(T_E,T_E + 3*|OW|) - C_{USAGE}(T_E,T_E+3*|OW|)] < 0.25 * [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$$

The usage loss calculation is:

$$100*[S_{USAGE}(T_S,T_E + 3*|OW|) - C_{USAGE}(T_S,T_E+3*|OW|)] / [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$$

A third usage pattern, a suppressant outage, has the features of a long outage in which usage that would have occurred during the outage period is not regained when the outage ends, and usage does not return to pre-outage levels quickly after the outage, and in which a user's short term confidence in the service is lost and alternatives are sought. An example of a suppressant outage is a one day POP3 outage, in which the telephone is used as an alternative to email even when the outage ends. Fig. 28 graphs this usage pattern, showing that, usage continues to be below normal levels well after the outage has recovered. A suppressant outage may be characterized in that, for some value *n*, usage levels in each of the

n subsequent outage window lengths past the end of the outage are less than 90% of the *n* corresponding comparison windows. A suitable value for *n* is 5.

The identification rule for a suppressant outage is:

for all $i \in \{0,1,\ldots,n\}$, the following must hold true:

$(S_{USAGE}(T_E + i * |OW|, T_E + (i+1)*|OW|) / (C_{USAGE}(T_E + i * |OW|, T_E + (i+1)*|OW|)) < 0.9$

The usage loss percentage calculation is:

$100 * [C_{USAGE}(T_S,T_E + n*|OW|) - S_{USAGE}(T_S,T_E+n*|OW|)] / [C_{USAGE}(T_S,T_E) - S_{USAGE}(T_S,T_E)]$

The level of customer retention component models the cost of an outage in terms of the long term loss of customers. This relationship is be represented by a function that linearly maps the percentage of existing customers lost to the outage length, the mapping being based upon historical or empirical data for the service or upon a relationship of number of customers lost to measured usage loss amount:

C_r(outage) =(customer lost) x (cost per customer)

The service level agreement penalty component derives financial penalties based on the outage details. This financial penalty could be fixed ($x per outage), time linear ($x per minute of outage) or usage linear ($x per byte of usage missed).

While the invention has been described and illustrated in connection with preferred embodiments, many variations and modifications as will be evident to those skilled in this art may be made without departing from the spirit and scope of the invention, and the invention is thus not to be limited to the precise details of methodology or construction set forth above as such variations and modification are intended to be included within the scope of the invention.

WHAT IS CLAIMED IS:

1. A method for analyzing a potential cause of a change in a service, wherein service quality of the service is monitored, usage of the service is measured, and service events are detected, the method comprising:

determining a service change time window based at least in part upon a change in service quality between a first working state and a second, non-working state, and upon a change in service usage amount, the service change time window encompassing at least part of a service outage;

retrieving data representing a detected event and a time in which the event occurred; and

computing a probability that the detected event caused the service change based at least in part on a correlation between the event time and the service change time window.

2. The method of claim 1, wherein determining the service change time window comprises determining a service failure time window based upon the change in service quality and narrowing the service failure time window to the service change time window based upon the service usage amount measured during that service failure time window.

3. The method of claim 2, wherein the service quality is monitored through periodic polling of the service quality, and comprising determining the service failure time window as bounded by a polled point of the first working state and a polled point of the second, non-working state.

4. The method of claim 1, wherein computing the probability comprises computing the probability using at least in part a time weighting function which decreases exponentially with the distance between the event time and the service change time window.

5. The method of claim 1, comprising determining whether one or more other events of a type identical to the detected event occurred, and wherein computing the probability comprises computing the probability using at least in part a false occurrence weighting function which decreases the probability of the detected event as the cause of the service change for instances in which the detected event occurred outside the service change time window.

6. The method of claim 1, comprising storing historical data associating occurrences of prior events with prior service changes, and wherein computing the probability that the detected event caused the service change comprises computing the probability based at least in part on the historical data.

7. The method of claim 6, wherein storing historical data comprises storing data representing instances in which prior events occurred within prior service change time windows, and wherein computing the probability that the detected event caused the service change comprises using at least in part a positive occurrence weighting function which increases the probability of the detected event as the cause of the service change based on instances in the historical data in which a prior event of a type identical to the detected event occurred within a prior service change time window.

8. The method of claim 6, wherein storing historical data comprises storing data representing instances in which prior events were identified as having caused prior service changes, and wherein computing the probability that the detected event caused the service change comprises using at least in part a historical weighting function which increases the probability of the detected event as the cause of the service change based on instances in the historical data in which a prior event of a type identical to the detected event was identified as having caused a prior service change.

9. The method of claim 1, comprising retrieving data representing a plurality of detected events and corresponding event times, and wherein computing the probability comprises computing probabilities for each of the plurality of detected events.

10. The method of claim 9, wherein computing probabilities comprises computing the probabilities such that the total of all computed probabilities is 1.

11. The method of claim 1, wherein the service comprises service over a communication network and wherein the detected event comprises a network event.

12. The method of claim 1, wherein the service comprises service provided by an application program and wherein the detected event comprises an application program event.

13. The method of claim 1, wherein the service change is a service outage, comprising determining the service change time window as a change in service quality from the first working state to the second, non-working state.

14. The method of claim 1, wherein the service change is a service recovery, comprising determining the service change time window as a change in service quality from the second, non-working state to the first, working state.

15. The method of claim 1, wherein determining the service change time window comprises detecting a change in service quality by detecting a step change in measured usage.

16. A method for analyzing potential causes of a service change, the method comprising:

determining a service change time window encompassing a change of service between a first working state and a service outage, the service change being determined at least in part based on measured service usage levels;

detecting occurrences of a set of events within a given time prior to and during the service change time window, each occurrence of an event being associated with a time at which the event occurred; and

computing a probability distribution for the set of events, which probability distribution determines for each event in the set the probability that the detected event caused the service change, the probability distribution being based at least in part on relations between the time of each event occurrence and the service change time window.

17. The method of claim 16, wherein computing the probability distribution for the set of events comprises computing the probability distribution using a first weighting function which is the product of two or more second weighting functions.

18. The method of claim 16, wherein the two or more second functions are selected from the group consisting of:

a time weighting function which decreases exponentially the probability of a given event as the cause of the service change with the distance between the given event time and the service change time window;

a false occurrence weighting function which decreases the probability of a given event as the cause of the service change for instances in which events of the same type as the given event occurred outside the service change time window;

a positive occurrence weighting function which increases the probability of a given event as the cause of the service change based on instances stored in a historical

database in which events of the same type as the given event occurred within a prior service change time window; and

a historical weighting function which increases the probability of a given event as the cause of the service change based on instances in the historical database in which events of the same type as the given event were identified as having caused a prior service outage.

19. The method of claim 18, wherein the step of computing the probability distribution comprises using a first weighting function which is the product of the time weighting function, false occurrence weighting function, positive occurrence weighting function, and user weighting function.

20. The method of claim 16, comprising monitoring service quality, and wherein determining the service change time window comprises determining a service failure time window based upon a change in monitored service quality and narrowing the service failure time window to the service change time window based upon the service usage amount measured during that service failure time window.

21. The method of claim 20, wherein the service quality is monitored through periodic polling of the service quality, and comprising determining the service failure time window as bounded by a polled point of the first working state and a polled point of the second, non-working state.

22. The method of claim 16, comprising computing the probability distribution such that the total of all probabilities in the distribution is 1.

23. The method of claim 16, wherein the service comprises service over a communication network and wherein the detected events comprise network events.

24. The method of claim 16, wherein the service comprises service provided by an application program and wherein the detected events comprise application program events.

25. The method of claim 16, wherein the service change is a service outage, comprising determining the service change time window as a change in service from the first working state to the second, non-working state.

26. The method of claim 16, wherein the service change is a service recovery, comprising determining the service change time window as a change in service from the second, non-working state to the first, working state.

27. The method of claim 1, wherein determining the service change time window comprises detecting a step change in measured usage.

28. A network monitoring system comprising:

a service monitor for monitoring quality of service on the network;

a usage meter for measuring usage of the network;

an event detector for detecting network events and times at which the network events occur; and

a probable cause engine, coupled to receive data from the service monitor, usage meter, and the event detector, for:

setting a service change time window based upon data received from the service monitor or usage meter, the service change time window encompassing at least part of an occurrence of a service outage in the network; and

determining which of the network events detected by the event detector is the most likely cause of a service change based at least in part of the relations of the detected network event times to the service change time window.

29. A computer readable medium storing program code for, when executed, causing a computer to perform a method for analyzing a potential cause of an change in a service, wherein service quality of the service is monitored, usage amount of the service is measured, and service events are detected, the method comprising:

determining a service change time window based at least in part upon a change in service quality between a first working state and a second, non-working state, and upon a change in service usage amount, the service change time window encompassing at least part of a service outage;

retrieving data representing a detected event and a time in which the event occurred; and

computing a probability that the detected event caused the service change based at least in part on a correlation between the event time and the service change time window.

30. A method for quantifying the effect of an outage in a service over a first period of time, the method comprising:

measuring usage of the service over time;

defining a cost of outage time window comprising the first time period and a second time period following the first time period; and

computing a cost of outage as the difference between the measured service usage during the cost of outage time window with service usage measured during a comparison window, the comparison window being substantially equal in time to that of the cost of outage time window and reflecting a similar period of service activity as that of the cost of outage time window without having a service outage.

31. The method of claim 30, comprising determining the second period of time to be a time in which the measured service usage returns to within a given percentage of a normal service usage.

32. The method of claim 30, comprising determining the second period of time to be the shorter of (1) a time in which the measured service usage returns to within a given percentage of a normal service usage and (2) a maximum time period.

33. The method of claim 30, wherein computing the cost of outage comprises computing the difference in units of service usage.

34. The method of claim 33, wherein the service is a communication service conveying a plurality of messages, the method comprising computing the cost of outage in numbers of messages conveyed.

35. The method of claim 33, wherein the service is a network server providing data items in response to requests therefor, the method comprising computing the cost of outage in numbers of requests received or data items provided by a server on the network.

36. The method of claim 33, comprising converting the computed units of cost of service outage to a monetary value.

37. The method of claim 36, wherein converting the computed units of cost of service outage comprises multiplying the units of cost of service outage by a first monetary value per unit of usage.

38. The method of claim 30, comprising comparing the cost of outage to a second cost of outage value for a different service and prioritizing the outages based on the compared costs.

39. The method of claim 30, comprising computing the difference between the monitored service usage following the cost of outage time window and a normal service usage level to thereby measure a long term effect of the service outage.

40. A method for quantifying the effect of an outage in a service, the method comprising:

measuring usage amounts of the service during a period of the service outage and a second period following the service outage;

comparing the measured usage amounts to normal usage amounts measured under similar service conditions for a similar period of time where no service outage occurs; and

determining a level of loss of service due to the service outage based on the comparison.

41. The method of claim 40, comprising defining the second period as the shorter of a time period in which measured service usage amounts return to within a given range of normal usage amounts and a predefined maximum time period.

42. The method of claim 40, wherein measuring service usage amounts comprises measuring service usage amounts in terms of units of service usage.

43. The method of claim 42, wherein the service is a communication service conveying a plurality of messages, comprising measuring service usage amounts in terms of number of messages conveyed by the system.

44. The method of claim 42, wherein the service is a network server providing data items in response to requests therefor, comprising measuring service usage amounts in terms of numbers of requests received or data items provided by a server on the network.

45. The method of claim 40, wherein determining the level of service loss comprises determining that substantially no loss of service occurred due to the outage based on the measured service usage amounts and normal service usage amounts being substantially equal.

46. The method of claim 40, comprising:

measuring service usage amounts during a third period following the second period;

comparing the measured third period service usage amounts to normal usage amounts measured under similar service conditions for a similar period of time; and

determining a long term effect on the service due to the service outage based on the comparison.

47. A computer readable medium storing program code which, when executed, causes a computer to perform a method for quantifying the effect of an outage in a service over a first period of time, the method comprising:

measuring service usage over time;

defining a cost of outage time window comprising the first time period and a second time period; and

computing a cost of outage as the difference between the measured level of service usage during the cost of outage time window with a level of usage in a comparison window, the comparison window being substantially equal in time to the cost of outage time window and reflecting a similar period of service activity as the cost of outage time window without having a service outage.

48. A method for predicting a cost of an outage of a service, the method comprising:

measuring time duration for and service usage during the outage;

comparing the measured usage amounts to normal usage amounts measured under similar service conditions for a similar period of time where no service outage occurs, to thereby determine a usage loss amount; and

computing a predicted cost of the outage based at least upon a cost component, the cost component comprising a function of the measured time of the outage and measured usage loss amount.

49. The method of claim 48, comprising measuring service usage on an ongoing basis and detecting the onset of the service outage using the measured service usage.

50. The method of claim 49, wherein detecting the onset of the service outage comprises detecting a step change in service usage.

51. The method of claim 48, comprising monitoring quality of the service and detecting the onset of a service outage based upon the service quality.

52. The method of claim 51, wherein monitoring service quality comprises monitoring service quality through periodic polling of the service quality, and wherein detecting the onset of a service outage comprises detecting the outage onset as bounded by a polled point of a first, working state and a polled point of a second, non-working state.

53. The method of claim 48, wherein computing the predicted cost of the outage comprises using a service demand cost component representing an affect on service usage based upon the duration of an outage.

54. The method of claim 53, wherein using the service demand cost component comprises multiplying the measured usage loss by a usage loss curve which is a function of time duration of an outage and represents a predicted percentage usage due to an outage based on time duration of the outage.

55. The method of claim 54, comprising generating the usage loss curve using historical data derived from prior service outages.

56. The method of claim 48, wherein computing the predicted cost of the outage comprises using a customer retention cost component representing a number or percentage of customers lost due to the outage.

57. The method of claim 48, wherein computing the predicted cost of the outage comprises using an agreement penalty component representing penalties arising under one or more service agreements due to a service outage.

58. The method of claim 48, wherein computing the predicted cost of the outage comprises computing the cost in units of service usage.

59. The method of claim 58, comprising converting the computed units of predicted cost to a monetary value by multiplying the units of predicted cost by a first monetary value per unit of usage.

60. The method of claim 48, comprising comparing the predicted cost of service outage to a second predicted cost of outage value for a different service and prioritizing the outages based on the compared costs.

61. A network monitoring system comprising:

a usage meter for measuring usage of a service on the network;

an event detector for detecting network events and times at which the network events occur;

a probable cause engine, coupled to receive data from the usage meter and the event detector, for determining which of the network events detected by the event detector is the most likely cause of a service outage based at least in part of the relations of the detected network event times to a service change time window, the service change time window encompassing at least part of an occurrence of the service outage in the network; and

a costing engine, coupled to receive data from the usage meter, for predicting the cost of the service outage.

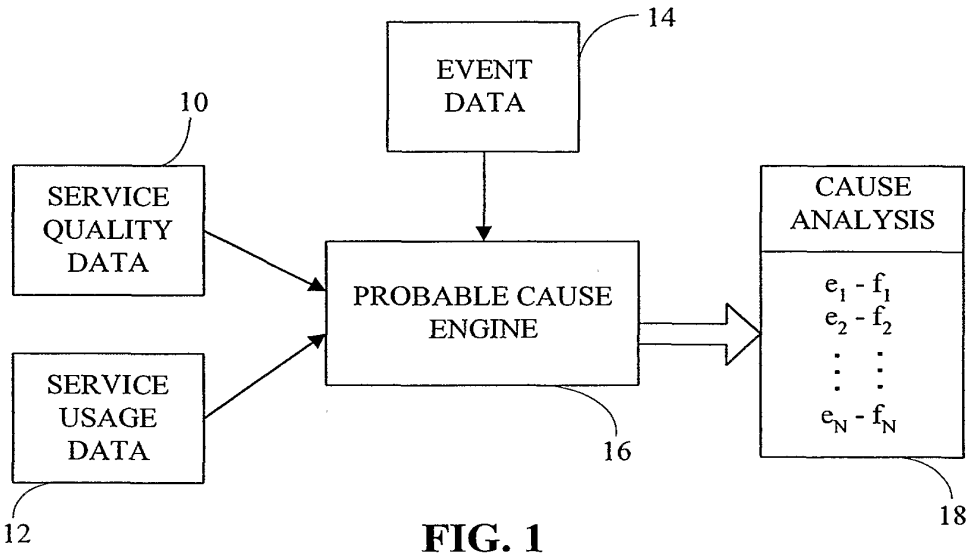

14
EVENT DATA
10
SERVICE QUALITY DATA
SERVICE USAGE DATA
12
PROBABLE CAUSE ENGINE
16
CAUSE ANALYSIS
e_1 - f_1
e_2 - f_2
e_N - f_N
18

FIG. 1

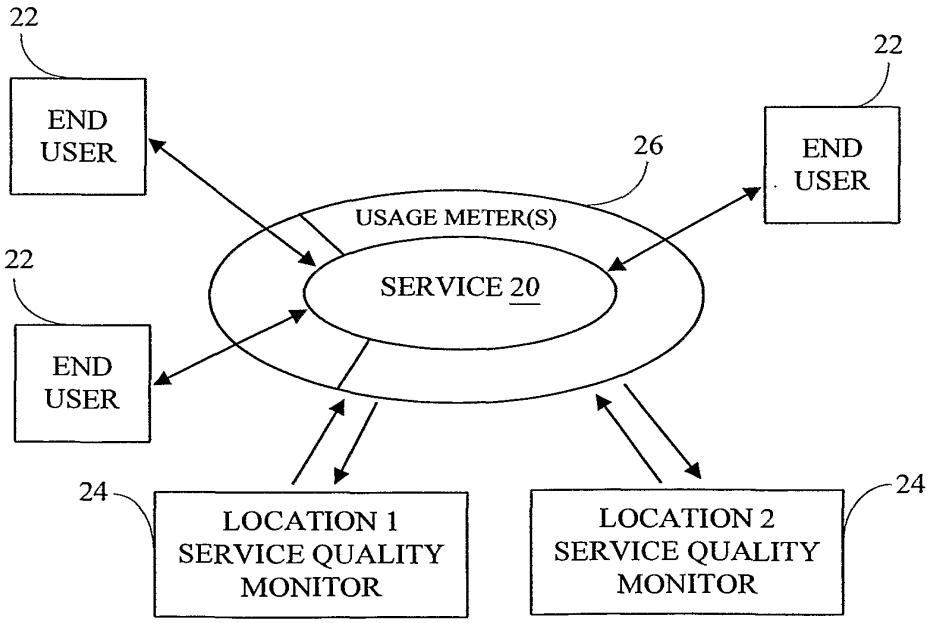
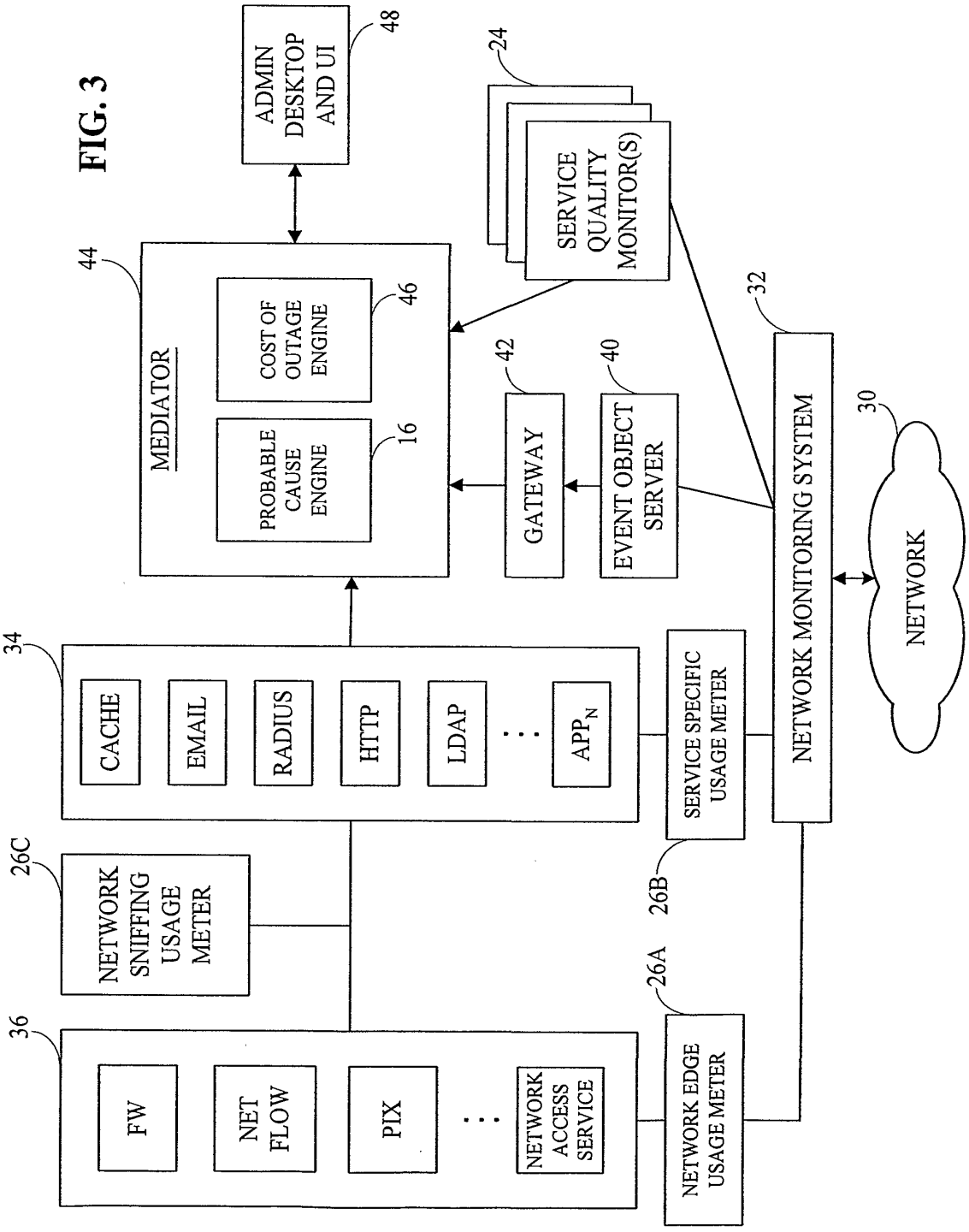

22
END USER
22
END USER
26
USAGE METER(S)
SERVICE 20
22
END USER
24
LOCATION 1 SERVICE QUALITY MONITOR
LOCATION 2 SERVICE QUALITY MONITOR
24

FIG. 2

FIG. 3


ADMIN DESKTOP AND UI
48
24
SERVICE QUALITY MONITOR(S)
44
MEDIATOR
COST OF OUTAGE ENGINE
46
PROBABLE CAUSE ENGINE
16
42
GATEWAY
40
EVENT OBJECT SERVER
32
NETWORK MONITORING SYSTEM
30
NETWORK
34
CACHE
EMAIL
RADIUS
HTTP
LDAP
APP$_N$
SERVICE SPECIFIC USAGE METER
26B
26C
NETWORK SNIFFING USAGE METER
36
FW
NET FLOW
PIX
NETWORK ACCESS SERVICE
26A
NETWORK EDGE USAGE METER

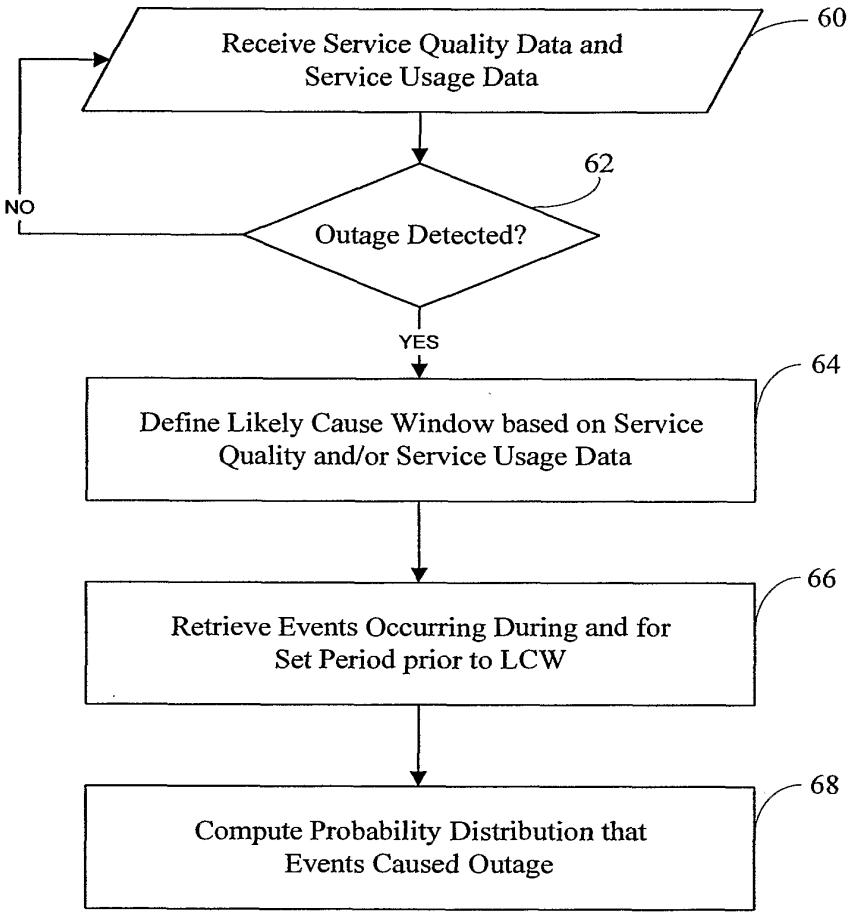

Receive Service Quality Data and Service Usage Data
60
62
Outage Detected?
NO
YES
Define Likely Cause Window based on Service Quality and/or Service Usage Data
64
Retrieve Events Occurring During and for Set Period prior to LCW
66
Compute Probability Distribution that Events Caused Outage
68

FIG. 4

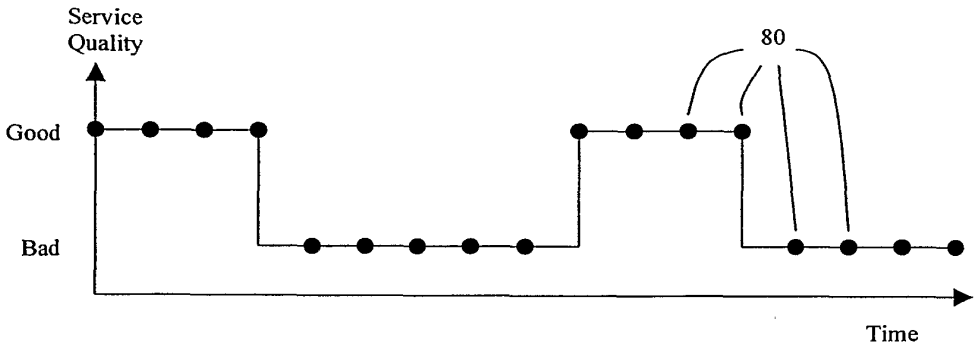


Fig. 5

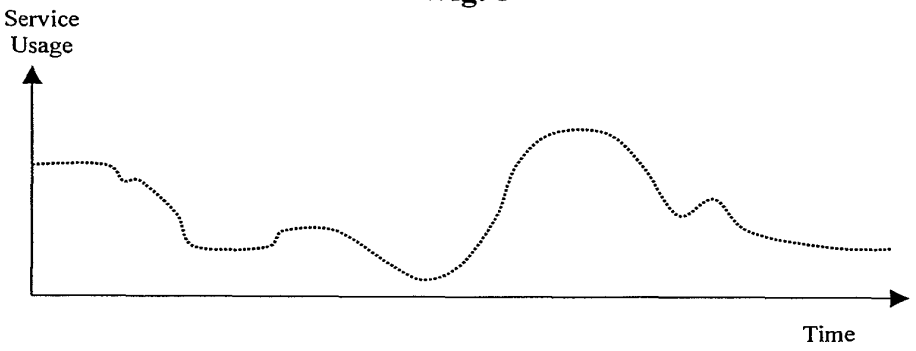


Fig. 6

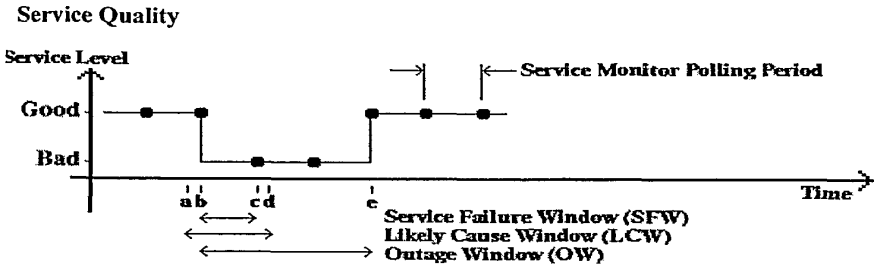


FIG. 7

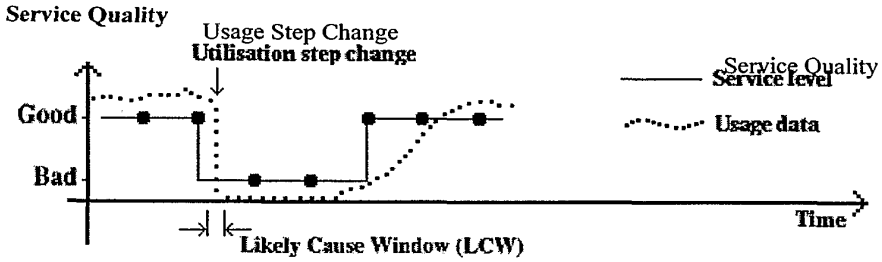


FIG. 8

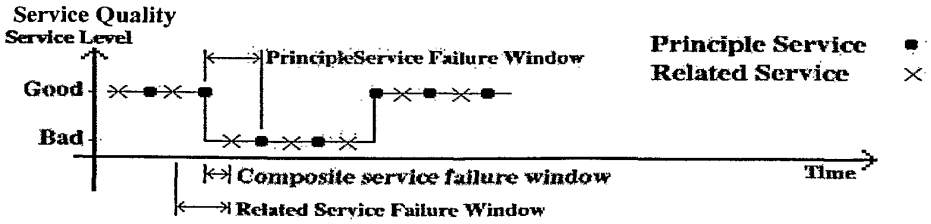


FIG. 9

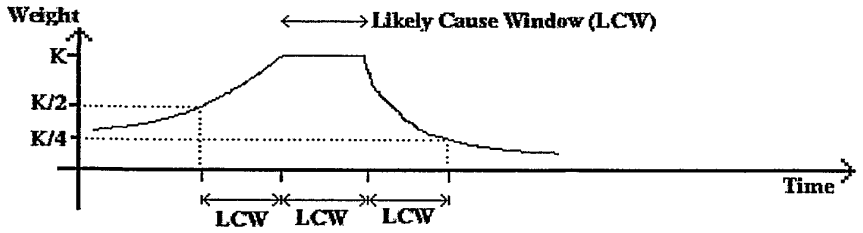


FIG. 10

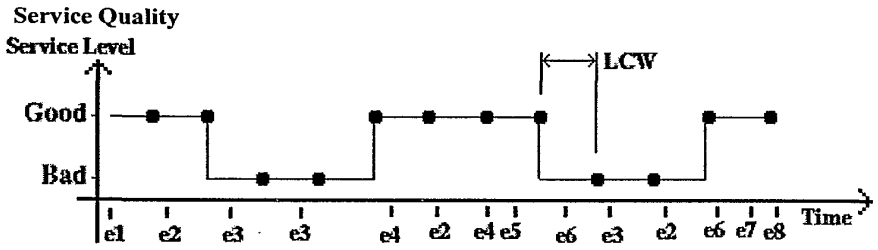


FIG. 11

Event	T(e)	FO(e)	PO(e)	U(e)	F(e)	P(e)
e3	2.11	1.00	4	1	8.44	0.5072
e6	4.00	0.50	2	1	4.00	0.2404
e2	1.24	0.25	2	4	2.48	0.1488
e5	2.61	0.50	1	1	1.31	0.0785
e4	1.38	0.25	1	1	0.34	0.0207
e7	0.07	0.50	1	1	0.03	0.0021
e1	0.06	0.50	1	1	0.03	0.0019
e8	0.02	0.50	1	1	0.01	0.0005
				Total:	16.64	1.0000

FIG. 12

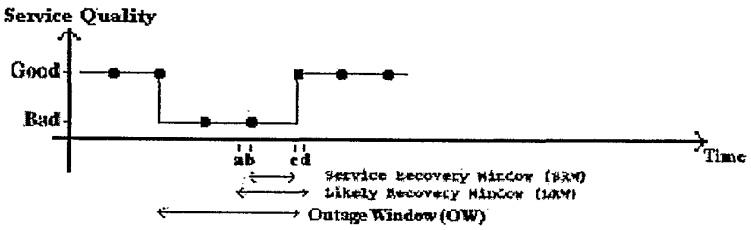

Service Quality
Good
Bad
Time
ab
cd
Service Recovery Window (SRW)
Likely Recovery Window (LRW)
Outage Window (OW)

Fig 13

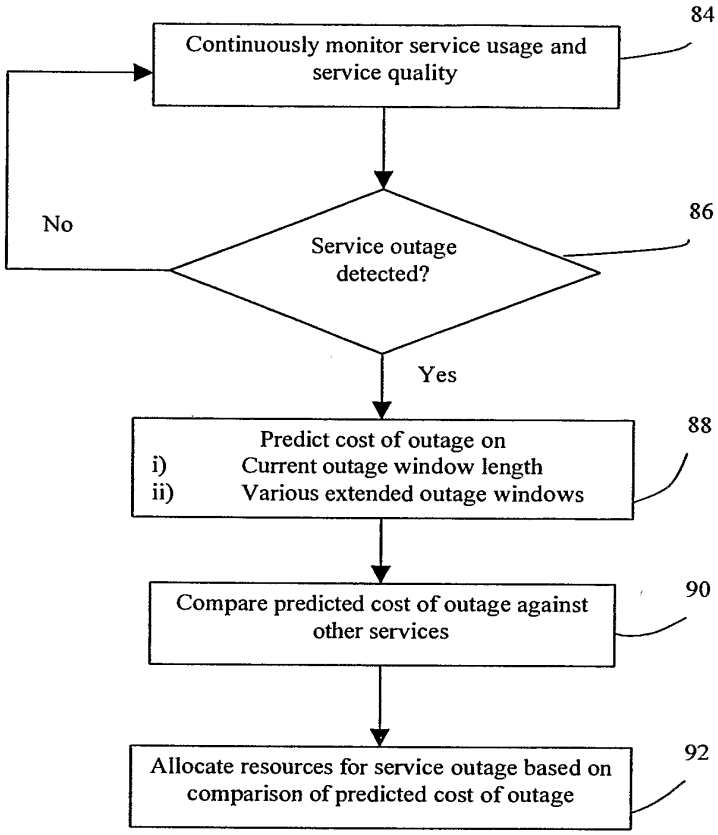

84
Continuously monitor service usage and service quality
86
Service outage detected?
No
Yes
88
Predict cost of outage on
i) Current outage window length
ii) Various extended outage windows
90
Compare predicted cost of outage against other services
92
Allocate resources for service outage based on comparison of predicted cost of outage

FIG. 14

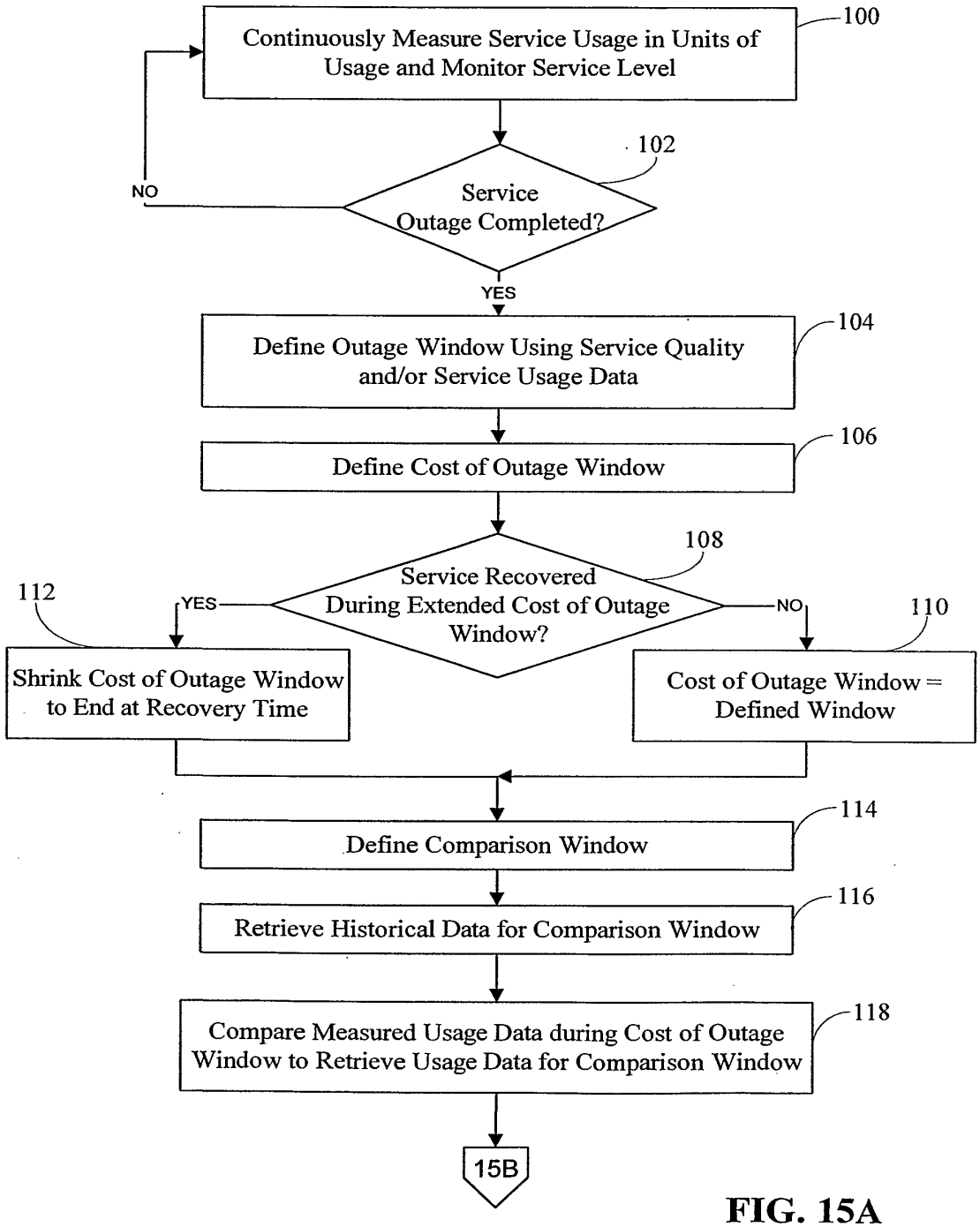

Continuously Measure Service Usage in Units of Usage and Monitor Service Level
100
Service Outage Completed?
102
NO
YES
Define Outage Window Using Service Quality and/or Service Usage Data
104
Define Cost of Outage Window
106
Service Recovered During Extended Cost of Outage Window?
108
YES
NO
112
110
Shrink Cost of Outage Window to End at Recovery Time
Cost of Outage Window = Defined Window
Define Comparison Window
114
Retrieve Historical Data for Comparison Window
116
Compare Measured Usage Data during Cost of Outage Window to Retrieve Usage Data for Comparison Window
118
15B

FIG. 15A

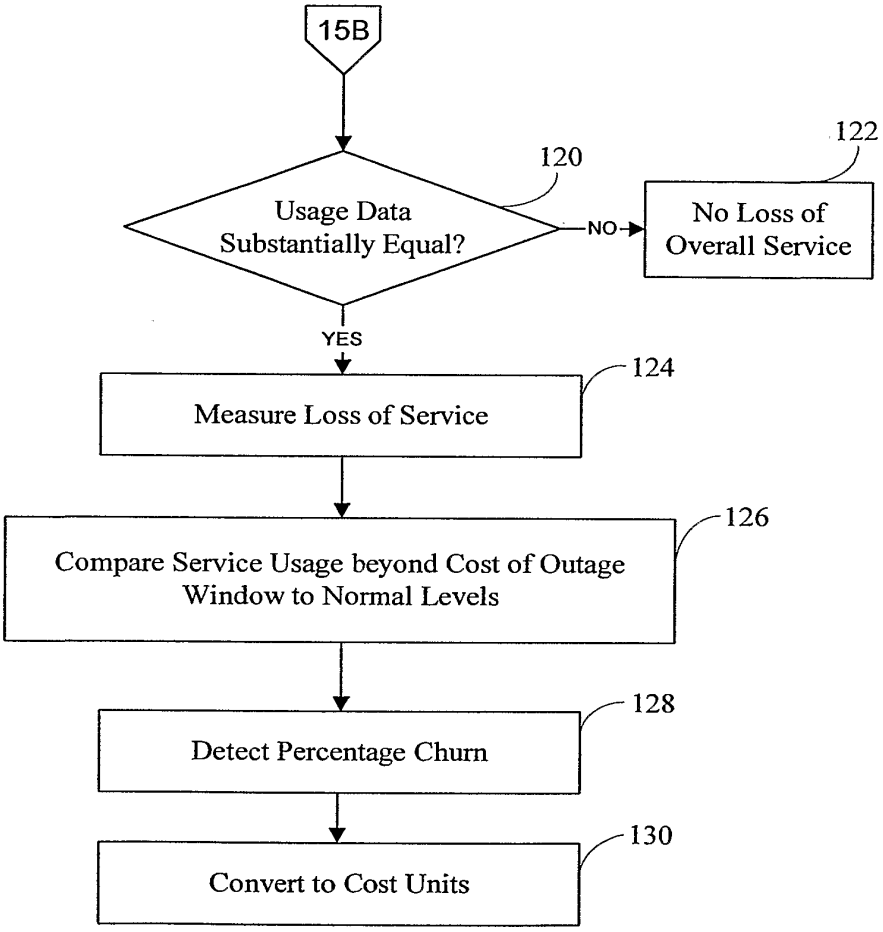

15B
120
Usage Data Substantially Equal?
NO
122
No Loss of Overall Service
YES
124
Measure Loss of Service
126
Compare Service Usage beyond Cost of Outage Window to Normal Levels
128
Detect Percentage Churn
130
Convert to Cost Units

FIG. 15B

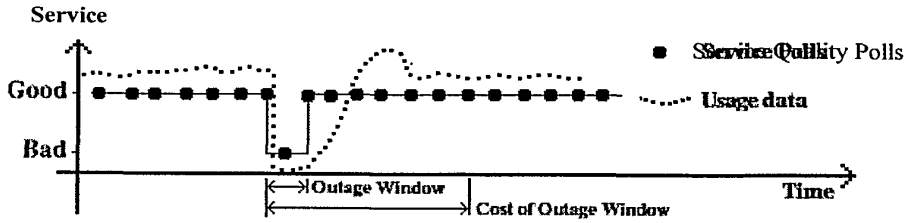


FIG. 16

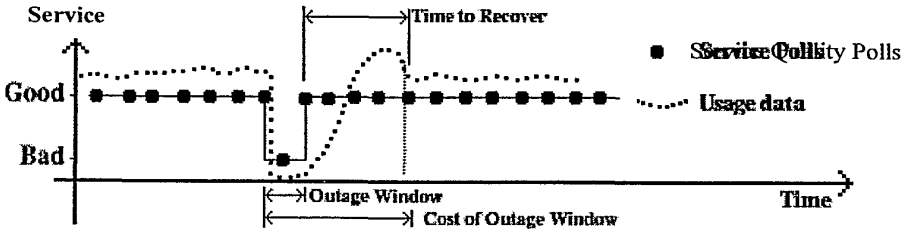


FIG. 18

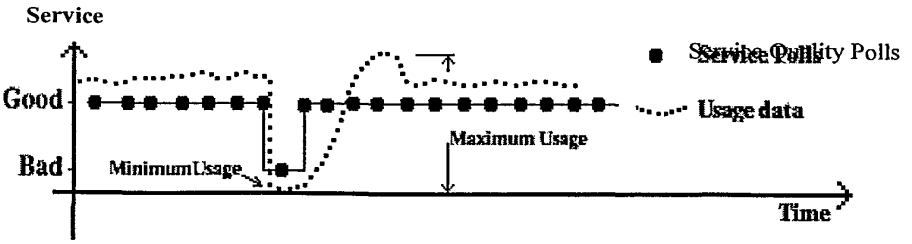


FIG. 19

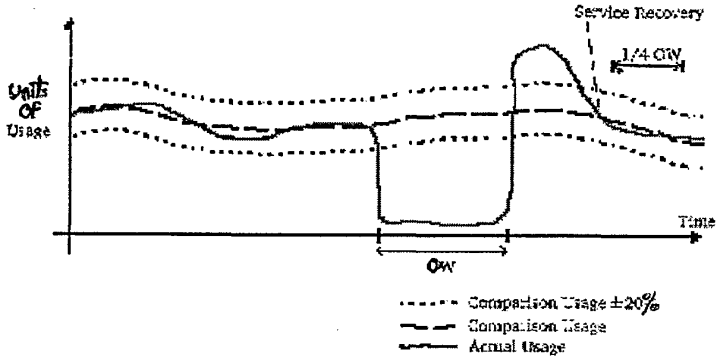

Service Recovery
1/4 OW
Units of Usage
Time
OW
Comparison Usage ±20%
Comparison Usage
Actual Usage

FIG. 17

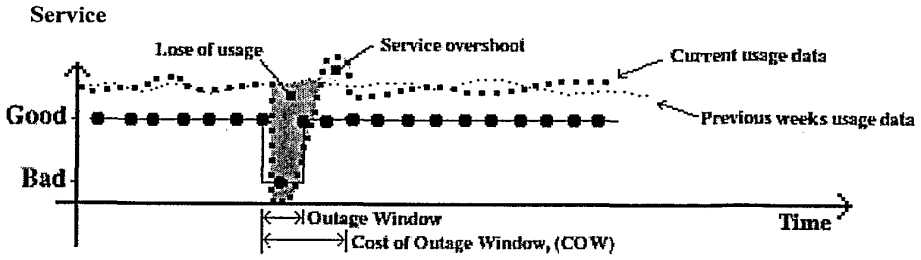


FIG. 20

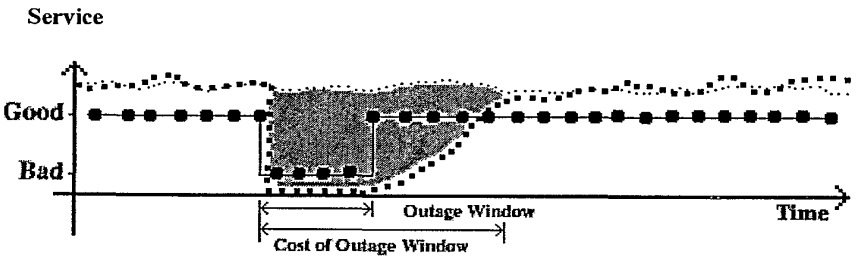


FIG. 21

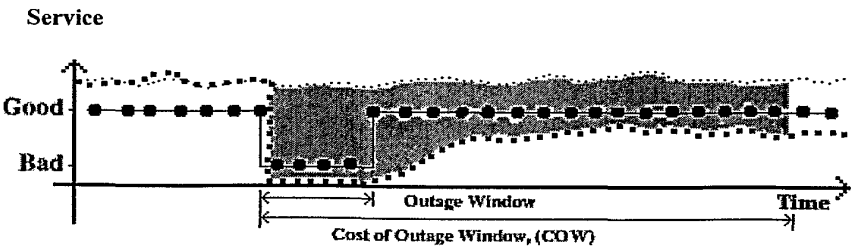


FIG. 22

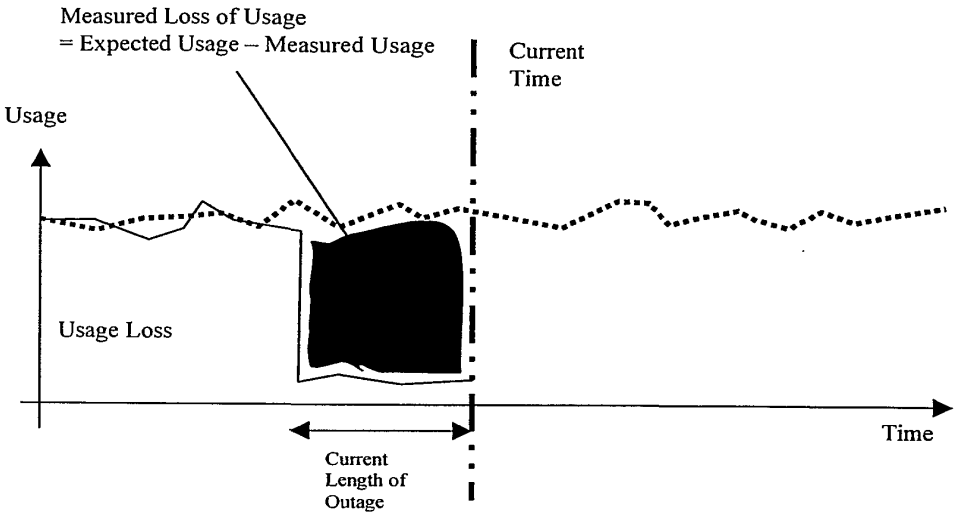

Measured Loss of Usage
= Expected Usage – Measured Usage
Current
Time
Usage
Usage Loss
Time
Current
Length of
Outage

FIG. 23

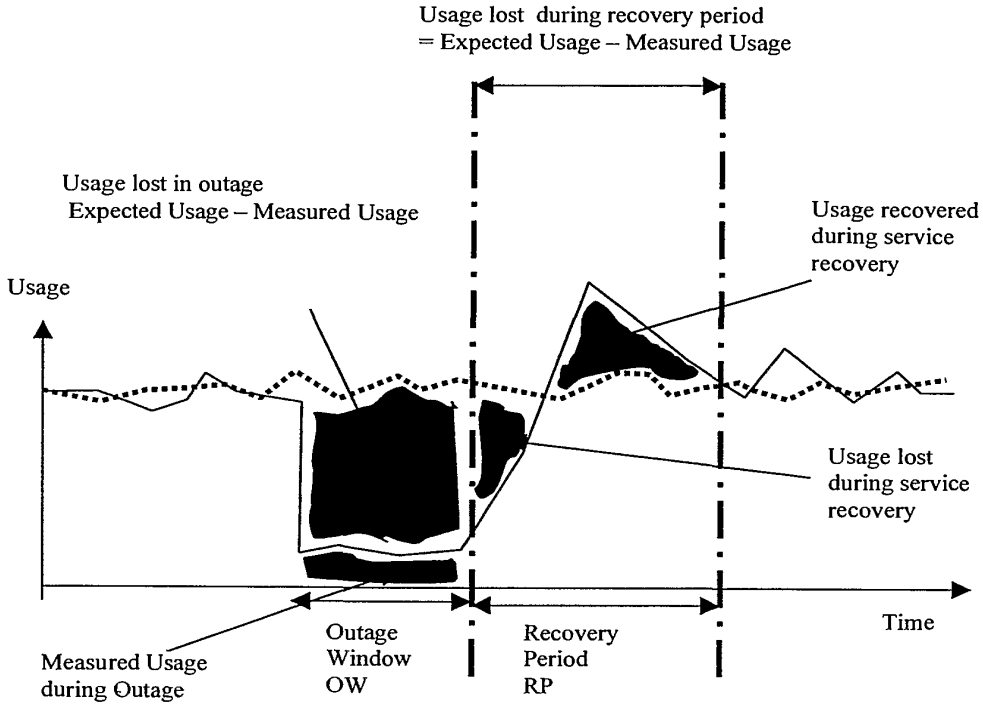

Usage lost during recovery period
= Expected Usage – Measured Usage
Usage lost in outage
Expected Usage – Measured Usage
Usage recovered
during service
recovery
Usage
Usage lost
during service
recovery
Time
Measured Usage
during Outage
Outage
Window
OW
Recovery
Period
RP

FIG. 24

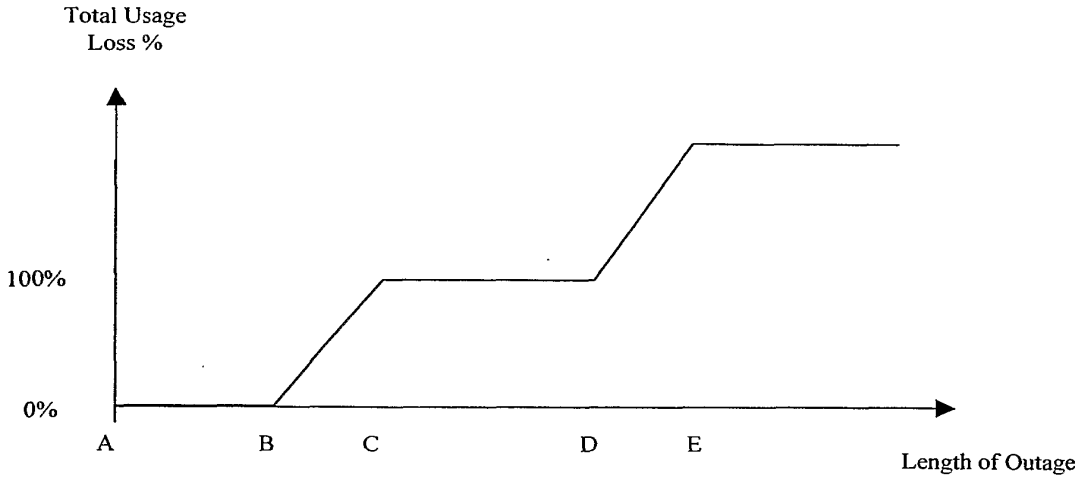


FIG. 25

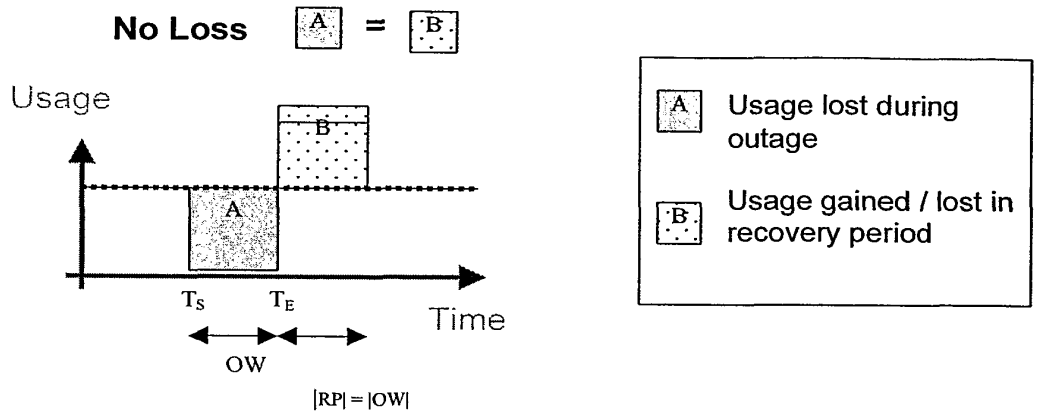

No Loss A = B
Usage
B
A
T_S
T_E
Time
OW
|RP| = |OW|
A Usage lost during outage
B Usage gained / lost in recovery period

FIG. 26

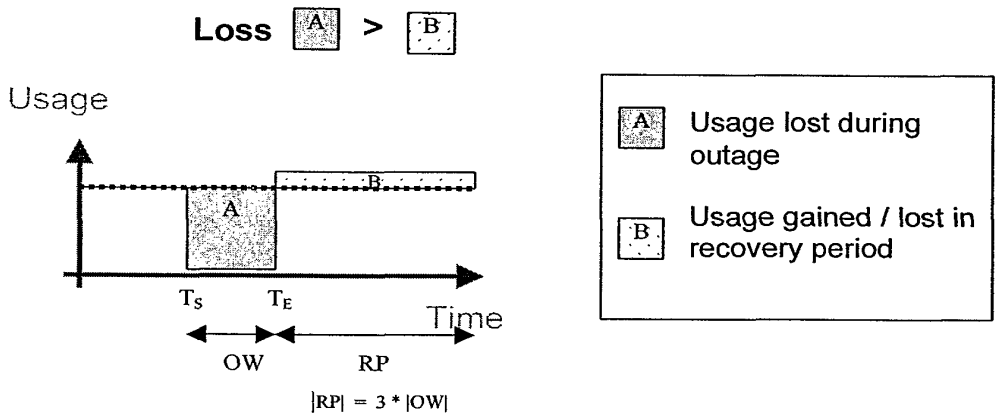

Loss A > B
Usage
B
A
T_S
T_E
Time
OW
RP
|RP| = 3 * |OW|
A Usage lost during outage
B Usage gained / lost in recovery period

FIG. 27

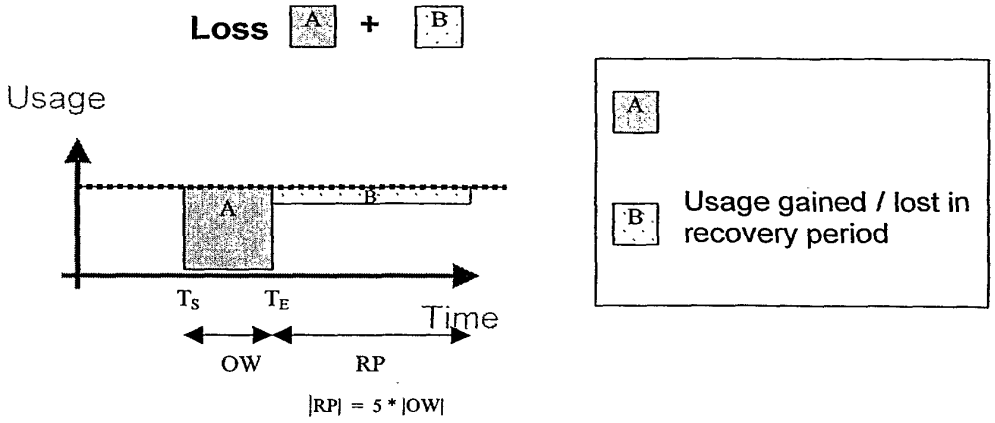

Loss A + B
Usage
A
B
T_S
T_E
Time
OW
RP
|RP| = 5 * |OW|
A
B
Usage gained / lost in recovery period

FIG. 28

Electronic Acknowledgement Receipt

EFS ID:	25158154
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	10-MAR-2016
Filing Date:	15-NOV-2013
Time Stamp:	12:49:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1.pdf	613129 2b84995b8166b4d4179e792e8cef57fdb623e667	no	8

Warnings:	
Information:	

2	Foreign Reference	2072.pdf	819567 9bd3134bd27e9dd9d134e7565086a86315c0ab30	no	33
Warnings:					
Information:					
3	Foreign Reference	2073.pdf	1463202 ba90a6bf82143d32fc7a1fbab25c6e727606a4c3	no	59
Warnings:					
Information:					
			Total Files Size (in bytes):	2895898	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5974439	A	1999-10-26	Bollella, Gregory	
	2	6038540	A	2000-03-14	Krist et al.	
	3	6058434	A	2000-05-02	Wilt et al.	
	4	6125391	A	2000-09-26	Meltzer et al.	
	5	6393014	B1	2002-05-21	Daly et al.	
	6	6397259	B1	2002-05-28	Lincke et al.	
	7	6735206	B1	2004-05-11	Oki et al.	
	8	6748437	B1	2004-06-08	Mankude et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6882718	B1	2005-04-19	Smith, Benjamin V.	
	10	7017189	B1	2006-03-21	DeMello et al.	
	11	7024460	B2	2006-04-04	Koopmas et al.	
	12	7047276	B2	2006-05-16	Liu et al.	
	13	7058022	B1	2006-06-06	Carolan et al.	
	14	7149521	B2	2006-12-12	Sundar et al.	
	15	7162237	B1	2007-01-09	Silver et al.	
	16	7200112	B2	2007-04-03	Sundar et al.	
	17	7248570	B2	2007-07-24	Bahl et al.	
	18	7266371	B1	2007-09-04	Amin et al.	
	19	7366654	B2	2008-04-29	Moore, Robert C.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7391724	B2	2008-06-24	Alakoski et al.	
	21	7395244	B1	2008-07-01	Kingsford, Bryan	
	22	7411930	B2	2008-08-12	Montojo et al.	
	23	7454191	B2	2008-11-18	Dawson et al.	
	24	7508799	B2	2009-03-24	Sumner et al.	
	25	7512128	B2	2009-03-31	DiMambro et al.	
	26	7554983	B1	2009-06-30	Muppala, Suresh	
	27	7564799	B2	2009-07-21	Holland et al.	
	28	7627767	B2	2009-12-01	Sherman et al.	
	29	7676673	B2	2010-03-09	Weller et al.	
	30	7817615	B1	2010-10-19	Breau et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7844034	B1	2010-11-30	Oh et al.	
	32	7849161	B2	2010-12-07	Koch et al.	
	33	7849477	B2	2010-12-07	Cristofalo et al.	
	34	7860088	B2	2010-12-28	Lioy, Marcello	
	35	7889384	B2	2011-02-15	Armentrout et al.	
	36	7894431	B2	2011-02-22	Goring et al.	
	37	7899039	B2	2011-03-01	Andreasen et al.	
	38	7966405	B2	2011-06-21	Sundaresan et al.	
	39	7978686	B2	2011-07-12	Goyal et al.	
	40	7987496	B2	2011-07-26	Bryce et al.	
	41	8032168	B2	2011-10-04	Ikaheimo, Jorma	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8073427	B2	2011-12-06	Koch et al.	
	43	8104080	B2	2012-01-24	Burns et al.	
	44	8131840	B1	2012-03-06	Denker, Richard E.	
	45	8150394	B2	2012-04-03	Bianconi et al.	
	46	8190122	B1	2012-05-29	Alexander et al.	
	47	8385964	B2	2013-02-26	Haney, Richard D.	
	48	8407763	B2	2013-03-26	Weller et al.	
	49	8484568	B2	2013-07-09	Rados et al.	
	50	8503455	B2	2013-08-06	Heikens, Heico	
	51	8504032	B2	2013-08-06	Lott et al.	
	52	8504687	B2	2013-08-06	Maffione et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8504690	B2	2013-08-06	Shah et al.	
	54	8522337	B2	2013-08-27	Adusumilli et al.	
	55	8527662	B2	2013-09-03	Biswas et al.	
	56	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	57	8644813	B1	2014-02-04	Gailloux et al.	
	58	8667542	B1	2014-03-04	Bertz et al.	
	59	8793304	B2	2014-07-29	Lu et al.	
	60	8812525	B1	2014-08-19	Taylor III, Buford Leonard	
	61	8863111	B2	2014-10-14	Selitser et al.	
	62	8948726	B2	2015-02-03	Smith et al.	
	63	8966018	B2	2015-02-24	Bugwadia et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	9002342	B2	2015-04-07	Tenhunen et al.	
	65	RE44412		2013-08-06	Naqvi et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030134650	A1	2003-07-17	Sundar et al.	
	2	20030159030	A1	2003-08-21	Evans, Junius A.	
	3	20040127208	A1	2004-07-01	Nair et al.	
	4	20040260766	A1	2004-12-23	Barros et al.	
	5	20050041617	A1	2005-02-24	Huotari et al.	
	6	20050096024	A1	2005-05-05	Bicker et al.	
	7	20060075506	A1	2006-04-06	Sanda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	8	20060095517	A1	2006-05-04	O'Connor et al.	
	9	20060126562	A1	2006-06-15	Liu, Huitao	
	10	20060277590	A1	2006-12-07	Limont et al.	
	11	20060291419	A1	2006-12-28	McConnell et al.	
	12	20070257767	A1	2007-11-08	Beeson, Curt	
	13	20080018494	A1	2008-01-24	Waite et al.	
	14	20080034063	A1	2008-02-07	Yee, Robert	
	15	20090036111	A1	2009-02-05	Danford et al.	
	16	20120108225	A1	2012-05-03	Luna et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-12-15
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	24373900
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	15-DEC-2015
Filing Date:	15-NOV-2013
Time Stamp:	22:06:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS.pdf	613890 918db8067eebbe45a4e25a5bdb153ed226d277fd	no	11

Warnings:	
Information:	

Total Files Size (in bytes):	613890

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 11/27/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
11/27/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com
krista@jacobseniplaw.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/082,040	15 November, 2013	RALEIGH ET AL.	RALEP032C1

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
ANDREW JOSEPH RUDY	
ART UNIT	PAPER
3687	20151118

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The Restriction Requirement mailed November 17, 2015 is hereby vacated. Another office action will be forthcoming.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

PTO-90C (Rev.04-03)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 11/17/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
11/17/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com
krista@jacobseniplaw.com

Office Action Summary	Application No. 14/082,040	Applicant(s) RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☒ Claim(s) *1-23* are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

Election/Restrictions

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-21, drawn to a system, classified in 709/224.

II. Claims 22-23 drawn to a method/medium, classified in 705/30.

3. The inventions are distinct, each from the other because of the following reasons:

Inventions Group II and Group I are related as process and apparatus for its practice. The inventions are distinct if it can be shown that either: (1) the process as claimed can be practiced by another and materially different apparatus or by hand, or (2) the apparatus as claimed can be used to practice another and materially different process. (MPEP § 806.05(e)). In this case the process may be practiced by hand or by non-statutory electronic signals.

3. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and/or examination burden if restriction were not required because one or more of the following reasons apply:

The inventions are distinct from each other.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of an invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

Should applicant traverse on the ground that the inventions are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103 or pre-AIA 35 U.S.C. 103(a) of the other invention.

4. A telephone call was made to Mr. Jonathan Darrow (Reg. No. 51,595) on November 10, 2015 to request an oral election to the above restriction requirement, but did not result in an election being made.

5. The examiner has required restriction between product or apparatus claims and process claims. Where applicant elects claims directed to the product/apparatus, and all product/apparatus claims are subsequently found allowable, withdrawn process claims that include all the limitations of the allowable product/apparatus claims should be considered for rejoinder. All claims directed to a nonelected process invention must include all the limitations of an allowable product/apparatus claim for that process invention to be rejoined.

In the event of rejoinder, the requirement for restriction between the product/apparatus claims and the rejoined process claims will be withdrawn, and the rejoined process claims will be fully examined for patentability in accordance with 37 CFR 1.104. Thus, to be allowable, the rejoined claims must meet all criteria for patentability including the requirements of 35 U.S.C. 101, 102, 103 and 112. Until all claims to the elected product/apparatus are found allowable, an otherwise proper restriction requirement between product/apparatus claims and process claims may be maintained. Withdrawn process claims that are not commensurate in scope with an allowable product/apparatus claim will not be rejoined. See MPEP § 821.04. Additionally, in order for rejoinder to occur, applicant is advised that the process claims should be amended during prosecution to require the limitations of the product/apparatus claims. **Failure to do so may result in no rejoinder.** Further, note that the prohibition against double patenting rejections of 35 U.S.C. 121 does not apply

where the restriction requirement is withdrawn by the examiner before the patent issues. See MPEP § 804.01.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/

Primary Examiner

Art Unit 3687

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	14/082,040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

SEARCHED			
Class	Subclass	Date	Examiner

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Inventor name search conducted.	11/10/2015	AJR
Continuity data reviewed.	11/10/2015	AJR
Bibliographic data updated.	11/10/2015	AJR

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1015

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/082,040	11/15/2013 RULE	709	3687	RALEP032C1

APPLICANTS

Headwater Partners I LLC, Redwood Shores, CA;

INVENTORS

Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

**** CONTINUING DATA ****************************

This application is a DIV of 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009 ABN
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009 PAT 9137739
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009 PAT 8839387
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,783 03/02/2009 ABN
and is a CIP of 12/380,757 03/02/2009 PAT 8326958
and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009 PAT 8799451
and is a CIP of 12/380,769 03/02/2009 PAT 8675507
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and is a CIP of 12/694,451 01/27/2010 PAT 8548428
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and is a CIP of 12/695,980 01/28/2010 PAT 8340634
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5572528	A	1996-11-05	Shuen, Pauline	
	2	5754953	A	1998-05-19	Briancon et al.	
	3	6628934	A	2003-09-30	Rosenberg et al.	
	4	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	5	6757717	B1	2004-06-29	Goldstein, Leonid	
	6	6901440	B1	2005-05-31	Bimm et al.	
	7	6970692	B2	2005-11-29	Tysor, Arthur James	
	8	7007295	B1	2006-02-28	Rose et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7203752	B2	2007-04-10	Rice et al.	
	10	7222190	B2	2007-05-22	Klinker et al.	
	11	7224968	B2	2007-05-29	Dobson et al.	
	12	7379731	B2	2008-05-27	Natsuno et al.	
	13	7457870	B1	2008-11-25	Lownsbrough et al.	
	14	7515926	B2	2009-04-07	Bu et al.	
	15	7536695	B2	2009-05-19	Alam et al.	
	16	7586871	B2	2009-09-08	Hamilton et al.	
	17	7752330	B2	2010-07-06	Olsen et al.	
	18	7792257	B1	2010-09-07	Vanier et al.	
	19	7801783	B2	2010-09-21	Kende et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7865187	B2	2011-01-04	Ramer et al.	
	21	7933274	B2	2011-04-26	Verma et al.	
	22	8005726	B1	2011-08-23	Bao, Yulin	
	23	8050690	B2	2011-11-01	Neeraj, Chawla	
	24	8086398	B2	2011-12-27	Sanchez et al.	
	25	8107953	B2	2012-01-31	Zimmerman et al.	
	26	8112435	B2	2012-02-07	Epstein et al.	
	27	8174378	B2	2012-05-08	Richman et al.	
	28	8195661	B2	2012-06-05	Kalavade, Asawaree	
	29	8200163	B2	2012-06-12	Hoffman, George E.	
	30	8200818	B2	2012-06-12	Freund et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8208788	B2	2012-06-26	Ando et al.	
	32	8254880	B2	2012-08-28	Aaltonen et al.	
	33	8270955	B2	2012-09-18	Ramer et al.	
	34	8326828	B2	2012-12-04	Zhou et al.	
	35	8331223	B2	2012-12-11	Hill et al.	
	36	8358975	B2	2013-01-22	Bahl et al.	
	37	8533775	B2	2013-09-10	Alcorn et al.	
	38	8538394	B2	2013-09-17	Zimmerman et al.	
	39	8538458	B2	2013-09-17	Haney, Richard D.	
	40	8565746	B2	2013-10-22	Hoffman, George E.	
	41	8571501	B2	2013-10-29	Miller et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	43	8713535	B2	2014-04-29	Malhotra et al.	
	44	8713641	B1	2014-04-29	Pagan et al.	
	45	8730842	B2	2014-05-20	Collins et al.	
	46	8732808	B2	2014-05-20	Sewall et al.	
	47	8761711	B2	2014-06-24	Grignani et al.	
	48	9049010		2015-06-02	Jueneman et al.	
	49	6445777		2002-09-03	Clark, Curtis	
	50	7039027		2006-05-02	Bridgelall, Raj	
	51	7990049		2011-08-02	Shioya, Shunsuke	
	52	8180886		2012-05-15	Overcash et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8339991		2012-12-25	Biswas et al.	
	54	8630314		2014-01-14	York, Frederick John	
	55	8868725		2014-10-21	Samba, Augustine S.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020154751	A1	2002-10-24	Thompson et al.	
	2	20030084321	A1	2003-05-01	Tarquini et al.	
	3	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	4	20060136882	A1	2006-06-22	Noonan et al.	
	5	20060143066	A1	2006-06-29	Calabria	
	6	20070073899	A1	2007-03-29	Judge et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	7	20070174490	A1	2007-07-26	Choi et al.	
	8	20070234402	A1	2007-10-04	Khosravi et al.	
	9	20090048913	A1	2009-02-19	Shenfield et al.	
	10	20090181662	A1	2009-07-16	Fleischman et al.	
	11	20120166604	A1	2012-06-28	Fortier et al.	
	12	20020191573		2002-12-19	Whitehill et al.	
	13	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	14	20090070379		2009-03-12	Rappaport, Theodore R.	
	15	20100318652		2010-12-16	Samba, Augustine S.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐
	2	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	3	1850575	EP	A1	2007-10-31	Research In Motion		☐
	4	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐
	5	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	6	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	3	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	4	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	5	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
	6	Loopt User Guide, metroPCS, 7/17/2008	☐
	7	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
	8	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
	9	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	11	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-09-17
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

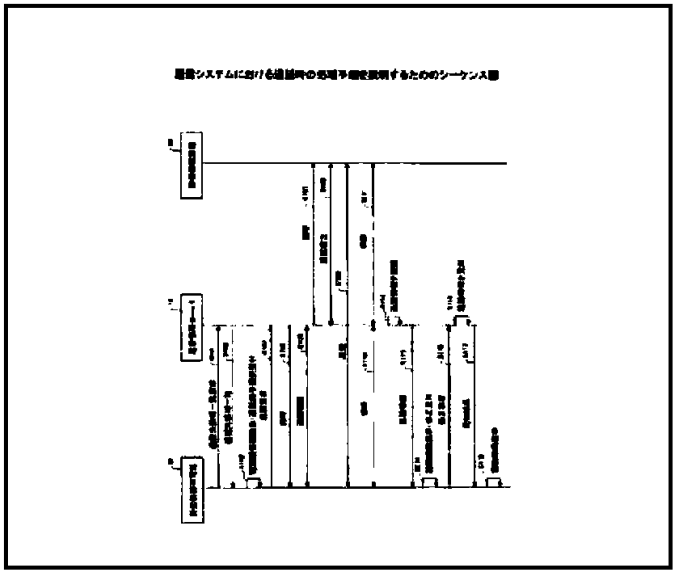
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(11)Publication number 2009-232107
(43)Date of publication of application 08.10.2009
(51)Int.Cl. *H04M 15/00 (2006.01)*

(21)Application number 2008-074306
(22)Date of filing 21.03.2008
(71)Applicant FUJITSU LTD
(72)Inventor TSUJIUCHI HIDETOSHI



(54)SPEECH COMMUNICATION INFORMATION RECORDING PROGRAM, SPEECH COMMUNICATION INFORMATION RECORDING APPARATUS AND SPEECH COMMUNICATION INFORMATION RECORDING METHOD

(57)Abstract
PROBLEM TO BE SOLVED: To provide a speech communication information recording program, a speech communication information recording apparatus and a speech communication information recording method, for appropriately dividing the burden origin of a call charge for one telephone number.
SOLUTION: A computer is made to execute: a procedure of receiving information specifying a call originating telephone number and information specifying a call terminating telephone number from a telephone set on a call originating side; a speech communication relay procedure of establishing speech communication between the telephone set on the call originating side and the telephone set on the call terminating side on the basis of the received information; a billing destination determination procedure of determining a billing destination for the call terminating telephone number using a management means for managing the identification information of the billing destination of the call charge by telephone number; and a billing destination recording procedure of relating the identification information of the determined billing destination and the identification information of the speech communication and recording them in a storage device.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-232107
(P2009-232107A)
(43)公開日　平成21年10月8日(2009.10.8)

(51)Int.Cl.		F I		テーマコード（参考）
H04M 15/00	(2006.01)	H04M 15/00	E	5K025

審査請求 未請求　請求項の数 7　OL　（全 21 頁）

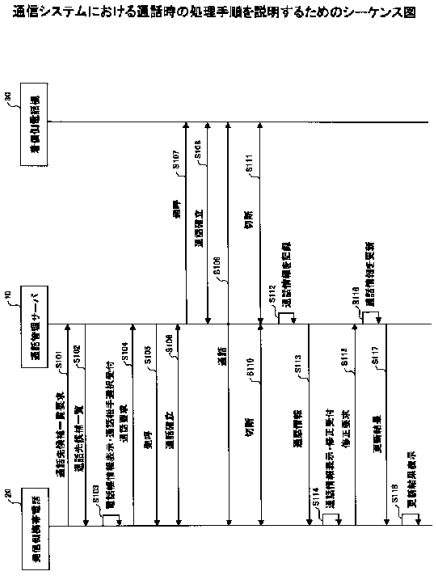
(21)出願番号　特願2008-74306 (P2008-74306)
(22)出願日　平成20年3月21日 (2008.3.21)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　辻内　秀敏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

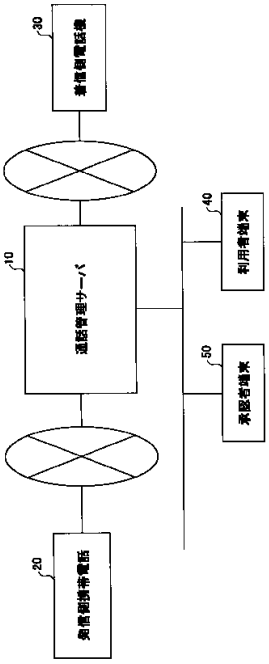
Ｆターム(参考)　5K025 AA01　CC01　CC07　GG10　GG12

(54)【発明の名称】通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法

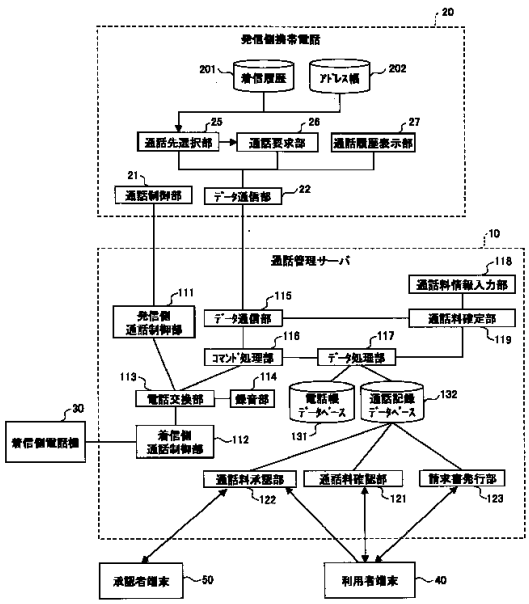
(57)【要約】
【課題】一つの電話番号に対する通話料の負担元を適切に区分することのできる通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法の提供を目的とする。
【解決手段】コンピュータに、発信側の電話機より発信電話番号を特定する情報と着信電話番号を特定する情報とを受信する手順と、受信された情報に基づいて前記発信側の電話機と着信側の電話機との間の通話を確立する通話中継手順と、電話番号ごとに通話料の請求先の識別情報を管理する管理手段を用いて、前記着信電話番号に対する請求先を判定する請求先判定手順と、判定された請求先の識別情報と前記通話の識別情報とを関連付けて記憶装置に記録する請求先記録手順とを実行させることにより上記課題を解決する。
【選択図】図４



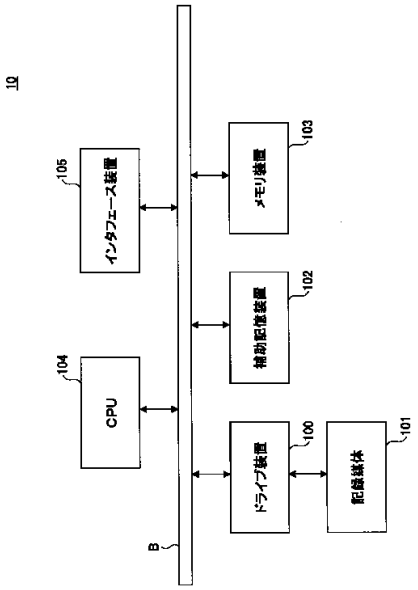
本発明の実施の形態における通信システム構成例を示す図



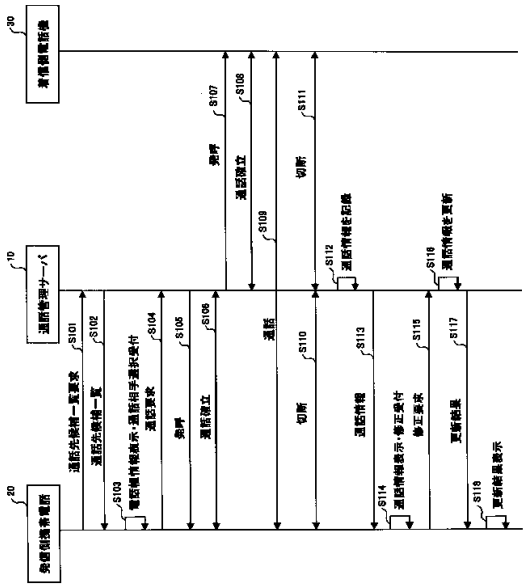
本発明の実施の形態における通信システムの機能構成例を示す図



本発明の実施の形態における通話管理サーバのハードウェア構成例を示す図



通信システムにおける通話時の処理手順を説明するためのシーケンス図

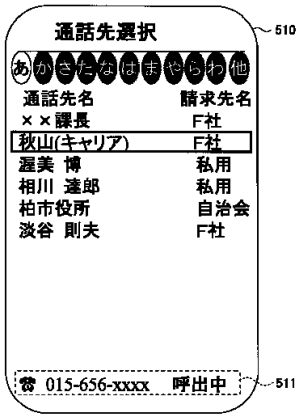


電話帳データベースの構成例を示す図

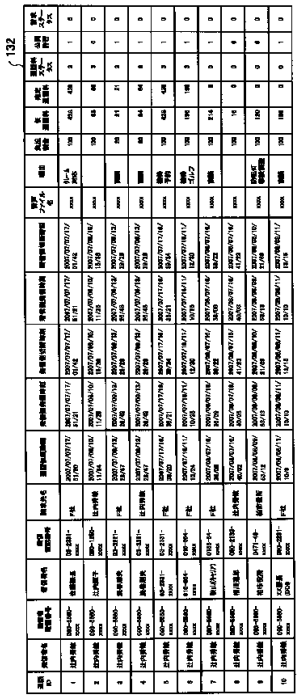
131

発信者名	発信者電話番号	通話先名	通話先電話番号	関係	請求先名	メールアドレス
辻内秀敏	090-5560-xxxx	辻内匡子	090-1250-xxxx	妻	辻内秀敏	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	渡谷則夫	03-3221-xxxx	松上電器	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	柏市役所	0471-48-xxxx	自治会	柏市役所	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	佐藤課長	03-2331-xxxx	○○商事	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	秋山(キャリア)	0156-64-xxxx	F社	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	相川達郎	050-2133-xxxx	親戚	辻内秀敏	
辻内秀敏	090-5560-xxxx	××課長	090-2231-xxxx	顧客	F社	xxx@xxxxxxx

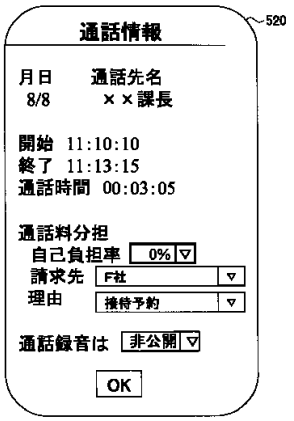
通話先選択画面の表示例を示す図



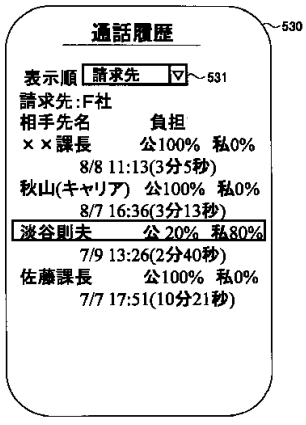
通話記録データベースの構成例を示す図



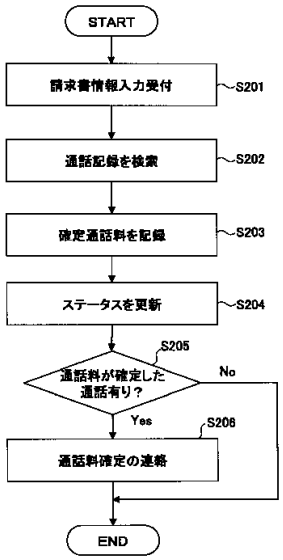
通話情報画面の表示例を示す図



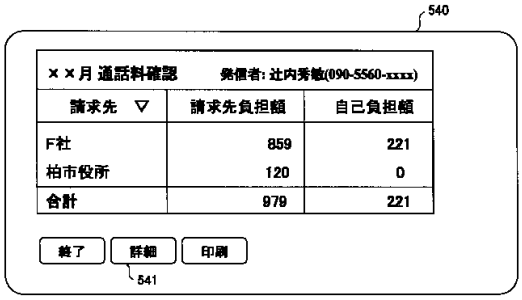
通話履歴画面の表示例を示す図



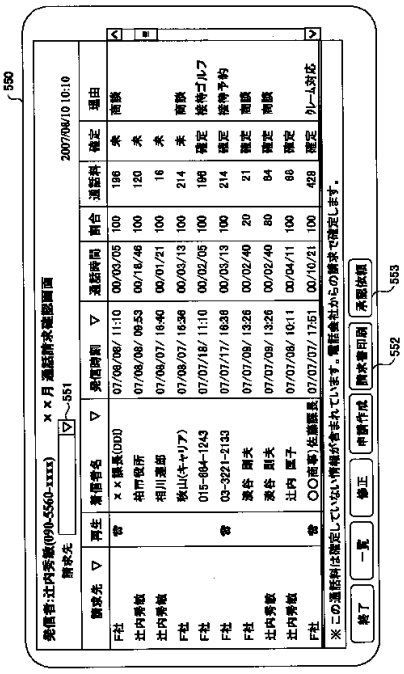
通話料の請求に応じて通話管理サーバによって実行される通話料の確定処理の処理手順を説明するためのフローチャート



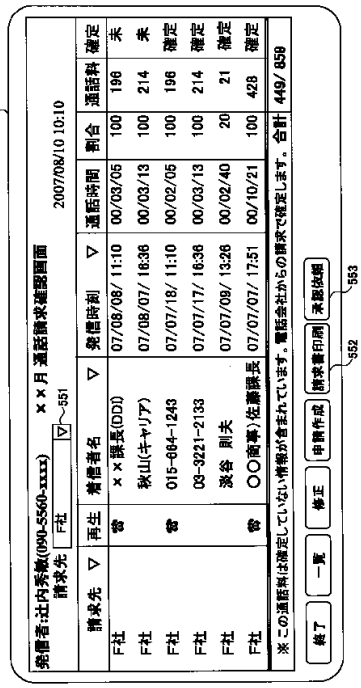
通話料確認画面の表示例を示す図



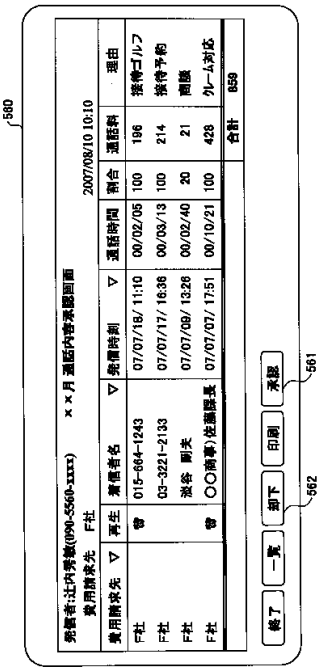
通話料確認詳細画面の表示例を示す図



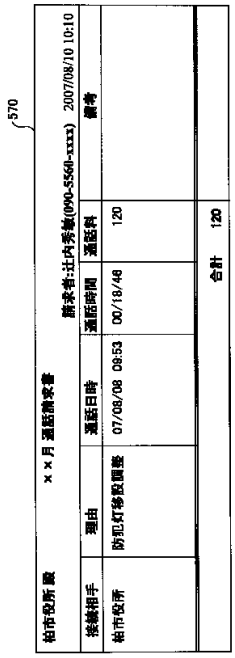
請求先が所属企業に絞り込まれた場合の通話料詳細画面の表示例を示す図



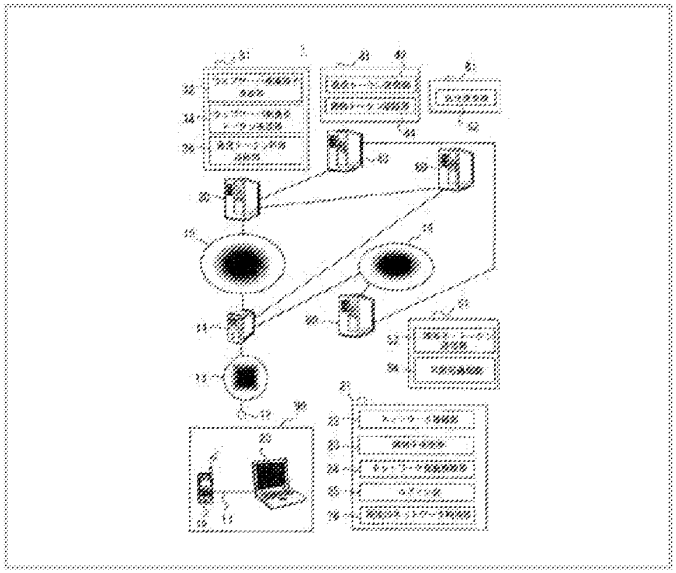
承認画面の表示例を示す図



請求書画面の表示例を示す図



(11)Publication number 2009-111919
(43)Date of publication of application 21.05.2009
(51)Int.Cl. *H04L 12/56 (2006.01)*
H04M 15/00 (2006.01)
H04M 11/00 (2006.01)
(21)Application number 2007-284415
(22)Date of filing 31.10.2007
(71)Applicant KYOCERA COMMUNICATION SYSTEMS CO LTD
(72)Inventor MASUDA KEIICHI



(54)SYSTEM, PROGRAM AND RECORDING MEDIUM FOR BILLING DATA COMMUNICATION FEE, AND METHOD OF BILLING DATA COMMUNICATION FEE

(57)Abstract
PROBLEM TO BE SOLVED: To provide a system or the like for billing a data communication fee, which can make account separately between official and private expenses when accessing a predetermined network 16 in a business-related matter, and which is also highly reliable as viewed from the carrier side.
SOLUTION: When a mobile party purchases a communication token T for a given network 16, the mobile party transmits the ID of the mobile phone 10 to a communication token issuing server 40 through the web server 30. The communication token T is generated based on the ID and transmitted to a PC 20 through the web server 30 and the mobile phone 10. After once disconnecting between the mobile phone and the network 15 for contents of the mobile phone, the mobile party tests the use of the predetermined network 16 through an authentication server 50 using the ID and the communication token T. The ID and the communication token T are transmitted to the communication token issuing server 40 and the validity of the communication token T is authenticated. The amount of the fee for data communication of the mobile phone 10, from which the fee for the communication token T is deducted, is charged to a billing destination on the mobile phone 10 side, and the fee for the communication token T is charged to another billing destination.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-111919
(P2009-111919A)
(43)公開日　平成21年5月21日(2009.5.21)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/56	(2006.01)	H04L 12/56	C	5K025
H04M 15/00	(2006.01)	H04M 15/00	G	5K030
H04M 11/00	(2006.01)	H04M 15/00	E	5K201
		H04M 11/00	302	

審査請求 有　請求項の数 23　OL　（全 26 頁）

(21)出願番号　特願2007-284415 (P2007-284415)
(22)出願日　平成19年10月31日 (2007.10.31)

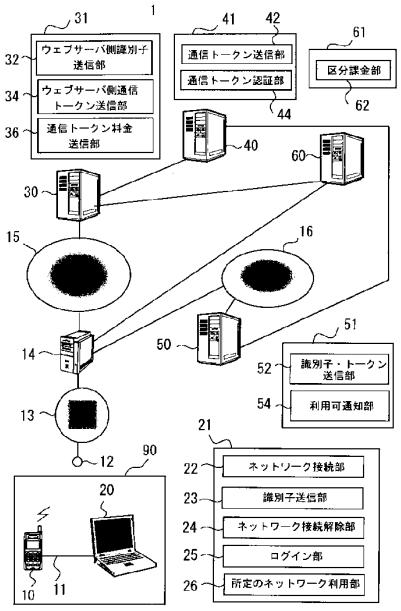
(71)出願人　596100812
京セラコミュニケーションシステム株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　100108372
弁理士　谷田　拓男
(72)発明者　増田　景一
京都府京都市伏見区竹田鳥羽殿町６番地
京セラコミュニケーションシステム株式会社内

Ｆターム(参考)　5K025 BB08 CC09 DD06 EE19 EE24
FF22 GG10 GG18
5K030 GA15 GA19 HA08 HB08 HB11
HC01 JA10 JT02 KA04 KA06
LB01 MC07

最終頁に続く

(54)【発明の名称】データ通信料金課金システム、プログラム、記録媒体およびデータ通信料金課金方法

(57)【要約】
【課題】業務上所定のネットワーク１６へアクセスする場合に公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供する。
【解決手段】所定のネットワーク１６用の通信トークンＴを購入する際、携帯電話器１０のＩＤをウェブサーバ３０経由で通信トークン発行サーバ４０へ送信する。ＩＤに基づき通信トークンＴが生成されウェブサーバ３０及び携帯電話器１０を介してＰＣ２０へ送信される。携帯電話コンテンツ用ネットワーク１５との接続を一旦解除した後、ＩＤ及び通信トークンＴを用い認証サーバ５０を介し所定のネットワーク１６の利用を試す。ＩＤ及び通信トークンＴは通信トークン発行サーバ４０へ送信され通信トークンＴの正当性が認証される。携帯電話器１０のデータ通信に対する料金から通信トークンＴの料金を控除した額が携帯電話器１０側の請求先に課金され通信トークンＴの料金は他の請求先に課金される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金システムであって、該移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバと、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバと、該ウェブサーバと接続され所定のネットワークの利用権を示す通信トークンを発行する通信トークン発行サーバと、該ウェブサーバと接続され該移動通信部に掛かるデータ通信料金を課金する課金サーバと、該所定のネットワークに接続された認証サーバとを備え、
前記移動情報端末は、
前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段と、
前記通信トークンの購入に際し前記移動通信部の識別子を前記ウェブサーバへ送信する識別子送信手段と、
前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段と、
前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記認証サーバを介して前記所定のネットワークの利用を試みるログイン手段と、
前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段とを備え、
前記ウェブサーバは、
前記識別子送信手段により送信された識別子を前記通信トークン発行サーバへ送信するウェブサーバ側識別子送信手段と、
前記通信トークン発行サーバから送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信手段と、
前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金を送信する通信トークン料金送信手段とを備え、
前記認証サーバは、
前記ログイン手段により用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信手段と、
前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知手段とを備え、
前記通信トークン発行サーバは、
前記ウェブサーバ側識別子送信手段により送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信手段と、
前記識別子・通信トークン送信手段により送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証手段とを備え、
前記課金サーバは、
前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段とを備えたことを特徴とするデータ通信料金課金システム。
【請求項２】
請求項１記載のデータ通信料金課金システムにおいて、前記移動通信部が無線ＬＡＮを

介して前記所定のネットワークの利用を行う場合、
前記通信トークン料金送信手段により送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記ログイン手段は、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信手段により送信された該通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用を試み、
前記利用可通知手段は、前記通信トークン認証手段により前記通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信することを特徴とするデータ通信料金課金システム。
【請求項３】
請求項１又は２記載のデータ通信料金課金システムにおいて、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバが該認証を行うウェブサーバ側認証手段をさらに備えたことを特徴とするデータ通信料金課金システム。
【請求項４】
請求項１乃至３のいずれかに記載のデータ通信料金課金システムにおいて、
前記通信トークン送信手段は、前記ウェブサーバ側識別子送信手段により送信された識別子と所定の鍵と所定の乱数とに基づき該通信トークンを生成して該ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、
前記通信トークン認証手段は、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信手段により該識別子と関連付けて記録された所定の乱数とに基づき前記通信トークンの正当性を認証することを特徴とするデータ通信料金課金システム。
【請求項５】
請求項１乃至４のいずれかに記載のデータ通信料金課金システムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、
前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、
前記通信トークン料金送信手段は、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金と前記識別子送信手段により送信された識別子とを送信し、
前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするデータ通信料金課金システム。
【請求項６】
請求項１乃至５のいずれかに記載のデータ通信料金課金システムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするデータ通信料金課金システム。
【請求項７】
請求項１乃至６のいずれかに記載のデータ通信料金課金システムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするデータ通信料金課金システム。
【請求項８】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末が実行するプログラムであって、該情報処理部のコンピュータを、

前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段、

前記移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信手段、

前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段、

前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログイン手段、

前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段として機能させるためのプログラムであり、

前記識別子送信手段により前記ウェブサーバへ送信された識別子は、該ウェブサーバにより、該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンは前記移動通信部を介して前記情報処理部へ送信され、該ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、該通信トークンの料金が送信されるものであり、

前記ログイン手段により用いられた識別子及び通信トークンは、前記認証サーバにより前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された識別子及び通信トークンに基づき通信トークンの正当性が認証され、該通信トークンの正当性が認証された場合、該認証サーバにより、前記移動通信部を介して前記情報処理部へ該所定のネットワークの利用を認める通知が送信され、

前記課金サーバにより、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額が該移動通信部側の請求先に課金され、該通信トークンの料金が他の請求先に課金されることを特徴とするプログラム。

【請求項９】

請求項８記載のプログラムにおいて、前記移動情報端末が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、

前記ウェブサーバ側から前記課金サーバ側へ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、

前記ログイン手段は、前記移動情報端末の識別子及び前記ウェブサーバ側から送信された通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、

前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることを特徴とするプログラム。

【請求項１０】

請求項８又は９記載のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、

前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、

前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記識別子送信手段により送信された識別子とが送信

され、
前記課金サーバにより、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記ウェブサーバにより送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするプログラム。
【請求項１１】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を課金する課金サーバが該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するためのプログラムであって、課金サーバのコンピュータを、
前記移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバから前記課金サーバへ送信された該所定の期間における所定のネットワークの利用権を示す通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段として機能させるためのプログラムであり、
前記移動情報端末により、該移動通信部を介して前記移動通信部側ネットワークに接続し、通信トークンの購入に際し該移動通信部の識別子が前記ウェブサーバへ送信され、該ウェブサーバにより、送信された該識別子が該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンが該移動通信部を介して該情報処理部へ送信され、前記課金サーバへ該通信トークンの料金が送信されるものであり、
前記移動情報端末により、従前に接続された前記移動通信部側ネットワークとの接続が解除され、前記移動通信部の識別子及び前記ウェブサーバから送信された前記通信トークンを用い、該移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用が試みられ、該認証サーバにより、移動情報端末により用いられた該識別子及び該通信トークンが前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子及び該通信トークンに基づき該通信トークンの正当性が認証された場合、該移動通信部を介して該情報処理部へ該所定のネットワークの利用を認める通知が送信され、該移動情報端末により、該認証サーバを介して該所定のネットワークの利用が行なわれることを特徴とするプログラム。
【請求項１２】
請求項１１記載のプログラムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、
前記ウェブサーバから前記課金サーバへ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記移動情報端末により、前記移動通信部の識別子及び前記ウェブサーバ側から該移動通信部を介して該情報処理部へ送信された前記通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用が試みられ、
前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることを特徴とするプログラム。
【請求項１３】
請求項１１又は１２記載のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、
前記移動情報端末により、前記通信トークンの購入に際し前記対応表に基づき前記移動

通信部の１以上の識別子の内の一つの識別子が前記ウェブサーバへ送信され、
前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記移動情報端末により送信された識別子とが送信され、
前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするプログラム。
【請求項１４】
請求項８乃至１３のいずれかに記載のプログラムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするプログラム。
【請求項１５】
請求項８乃至１４のいずれかに記載のプログラムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするプログラム。
【請求項１６】
請求項８乃至１５のいずれかに記載のプログラムを記録したコンピュータ読取り可能な記録媒体。
【請求項１７】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金方法であって、
前記移動情報端末が、
前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続ステップと、
前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信ステップと、
前記ウェブサーバが、
前記ウェブサーバと接続され前記通信トークンを発行する通信トークン発行サーバへ、前記識別子送信ステップで送信された識別子を送信するウェブサーバ側識別子送信ステップと、
前記通信トークン発行サーバが、
前記ウェブサーバ側識別子送信ステップで送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信ステップと、
前記ウェブサーバが、
前記通信トークン送信ステップで送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信ステップと、
前記ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金を送信する通信トークン料金送信ステップと、
前記移動情報端末が、
前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除ステップと、
前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログインステップと、

前記認証サーバが、
前記ログインステップで用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信ステップと、
前記通信トークン発行サーバが、
前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証ステップと、
前記認証サーバが、
前記通信トークン認証ステップで通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知ステップと、
前記移動情報端末が、
前記利用通知ステップで前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して前記所定のネットワークの利用を行う所定のネットワーク利用ステップと、
前記課金サーバが、
前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金ステップとを備えたことを特徴とするデータ通信料金課金方法。
【請求項１８】
請求項１７記載のデータ通信料金課金方法において、前記移動通信部が無線ＬＡＮを介して該所定のネットワークの利用を行う場合、
前記通信トークン料金送信ステップで送信された該通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記ログインステップは、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い前記無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、
前記利用可通知ステップは、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報端末装置へ前記所定のネットワークの利用を認める通知を送信することを特徴とするデータ通信料金課金方法。
【請求項１９】
請求項１７又は１８記載のデータ通信料金課金方法において、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバ側識別子送信ステップに先立ち、前記ウェブサーバが該認証を行うウェブサーバ側認証ステップをさらに備えたことを特徴とするデータ通信料金課金方法。
【請求項２０】
請求項１７乃至１９のいずれかに記載のデータ通信料金課金方法において、
前記通信トークン送信ステップは、前記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子と所定の鍵と所定の乱数とに基づき通信トークンを生成して前記ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、
前記通信トークン認証ステップは、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信ステップで該識別子と関連付けて記録された所定の乱数とに基づき該通信トークンの正当性を認証することを特徴とするデータ通信料金課金方法。
【請求項２１】
請求項１７乃至２０のいずれかに記載のデータ通信料金課金方法において、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対

応する前記他の請求先との対応表をさらに備え、
前記識別子送信ステップは、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、
前記通信トークン料金送信ステップは、前記課金サーバへ前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金と前記識別子送信ステップで送信された識別子とを送信し、
前記区分課金ステップは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信ステップで送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするデータ通信料金課金方法。
【請求項２２】
請求項１７乃至２１のいずれかに記載のデータ通信料金課金方法において、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするデータ通信料金課金方法。
【請求項２３】
請求項１７乃至２２のいずれかに記載のデータ通信料金課金方法において、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするデータ通信料金課金方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、移動情報端末装置のデータ通信料金を当該移動情報端末装置側の請求先と他の請求先とに区分して課金するデータ通信料金課金システム等に関する。
【背景技術】
【０００２】
近年、社外で携帯電話器とパーソナルコンピュータ（以下、「ＰＣ」と省略する。）とを用いてモバイル通信を行うことにより、業務を行う必要に迫られているビジネスマン等が増加している。所持している携帯電話器はビジネスマン等の個人契約によるものであることが多く、この場合、モバイル通信によるアクセスで発生したパケット通信料はビジネスマン等へ請求されることになる。ビジネスマン等は当該請求の明細書を用いて会社にパケット通信料を請求することは可能であるが、業務上であるのか個人使用であるのかという、いわゆる公私区分の事務処理は極めて面倒且つ困難である。このため、当該パケット通信料はビジネスマン等の個人負担になってしまうことが多いというのが実情である。
【０００３】
従来、携帯電話器の通話の分野では、公私区分の事務処理を容易にするために、相手の電話番号の前にいわゆる特番と呼ばれる認識番号を入力することにより、会社と個人とで通話料金を区分する公私分計サービスが行われている（非特許文献１参照）。
【０００４】
携帯電話器を用いたデータ通信向けの種々の公私分計サービスも既に行われている。例えば、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことにより、リアルタイムにデータ通信料およびデータ通信料金の概算を表示することもできる（非特許文献２参照）。
【０００５】
予めアクセス先を登録しておくことにより、パケットの宛先が登録されている場合には、個人使用の携帯電話器へのパケット通信料の請求を免除し、会社側へ請求するという仕組みも存在する。あるいは、企業側ネットワークへアクセスする場合を業務利用とし、他

のインターネット上のサーバへアクセスする場合を私的利用として、両者を分けて課金する通信料金分別方法も存在する（特許文献１参照）。

【０００６】

【非特許文献１】日経ＢＰ社、ITpro 、Network“ケータイonBussiness”、［online］、２００４年９月１６日、［平成１９年２月１日検索］、インターネット<URL: http://itpro.nikkeibp.co.jp/free/TIS/keitai/20040915/149943/?ST=keitai&P=2>

【非特許文献２】ＫＤＤＩ、モバイル通信、各種ソフトダウンロード“パケットカウンター”、［online］、［平成１９年２月１日検索］、インターネット<URL: http:// http://www.au.kddi.com/mobile/soft/packet_counter/index.html>

【特許文献１】国際公開第ＷＯ２００４／０７７７６５号

【発明の開示】

【発明が解決しようとする課題】

【０００７】

上述のように、携帯電話器の通話の分野では特番を用いることにより会社と個人とで通話料金を区分する公私分計サービスが行われている。しかし、通話の場合と比較してデータ通信の場合、パケットは同時に複数の箇所にアクセスすることができるため、特番のような認識番号を付加することにより公私分計することは困難であるという問題があった。

上述のように、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておく公私分計サービスも行われている。しかし、当該分計は概算にすぎない上、ＰＣ上でのパケットカウントはユーザがカウントしたものと同様であるため、当該分計はキャリヤ側からみて信頼度が低く、従って当該分計はキャリヤ側の請求に反映できるものではないという問題があった。上述のように、パケットの宛先が登録されている場合には、個人使用の携帯電話器へのパケット通信料の請求を免除し、会社側へ請求するという仕組みも存在する。しかし、この場合、宛先を登録する必要があるという問題があった。企業側ネットワークへアクセスする場合を業務利用とし、他の一般のインターネット上のサーバへアクセスする場合を私的利用として、両者を分けて課金する通信料金分別方法も存在する。しかし、業務上、インターネット上のサーバへアクセスする場合は私的利用となってしまうため、業務利用として分けて課金することができないという問題があった。

【０００８】

そこで、本発明の目的は、上記問題を解決するためになされたものであり、携帯電話器の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することにある。

【課題を解決するための手段】

【０００９】

この発明のデータ通信料金課金システムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金システムであって、該移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバと、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバと、該ウェブサーバと接続され所定のネットワークの利用権を示す通信トークンを発行する通信トークン発行サーバと、該ウェブサーバと接続され該移動通信部に掛かるデータ通信料金を課金する課金サーバと、該所定のネットワークに接続された認証サーバとを備え、前記移動情報端末は、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段と、前記通信トークンの購入に際し前記移動通信部の識別子を前記ウェブサーバへ送信する識別子送信手段と、前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの

接続を解除する移動通信部側ネットワーク接続解除手段と、前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記認証サーバを介して前記所定のネットワークの利用を試みるログイン手段と、前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段とを備え、前記ウェブサーバは、前記識別子送信手段により送信された識別子を前記通信トークン発行サーバへ送信するウェブサーバ側識別子送信手段と、前記通信トークン発行サーバから送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信手段と、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金を送信する通信トークン料金送信手段とを備え、前記認証サーバは、前記ログイン手段により用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信手段と、前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知手段とを備え、前記通信トークン発行サーバは、前記ウェブサーバ側識別子送信手段により送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信手段と、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証手段とを備え、前記課金サーバは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段とを備えたことを特徴とする。

【００１０】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記通信トークン料金送信手段により送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログイン手段は、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信手段により送信された該通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用を試み、前記利用可通知手段は、前記通信トークン認証手段により前記通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信することができる。

【００１１】

ここで、この発明のデータ通信料金課金システムにおいて、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバが該認証を行うウェブサーバ側認証手段をさらに備えることができる。

【００１２】

ここで、この発明のデータ通信料金課金システムにおいて、前記通信トークン送信手段は、前記ウェブサーバ側識別子送信手段により送信された識別子と所定の鍵と所定の乱数とに基づき該通信トークンを生成して該ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、前記通信トークン認証手段は、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信手段により該識別子と関連付けて記録された所定の乱数とに基づき前記通信トークンの正当性を認証することができる。

【００１３】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記通信トークン料金送信手段は、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金と前記識別子送信手段により

送信された識別子とを送信し、前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００１４】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００１５】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。

【００１６】

この発明のプログラムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末が実行するプログラムであって、該情報処理部のコンピュータを、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段、前記移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信手段、前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段、前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログイン手段、前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段として機能させるためのプログラムであり、前記識別子送信手段により前記ウェブサーバへ送信された識別子は、該ウェブサーバにより、該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンは前記移動通信部を介して前記情報処理部へ送信され、該ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、該通信トークンの料金が送信されるものであり、前記ログイン手段により用いられた識別子及び通信トークンは、前記認証サーバにより前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された識別子及び通信トークンに基づき通信トークンの正当性が認証され、該通信トークンの正当性が認証された場合、該認証サーバにより、前記移動通信部を介して前記情報処理部へ該所定のネットワークの利用を認める通知が送信され、前記課金サーバにより、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額が該移動通信部側の請求先に課金され、該通信トークンの料金が他の請求先に課金されることを特徴とするプログラムである。

【００１７】

ここで、この発明のプログラムにおいて、前記移動情報端末が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記ウェブサーバ側から前記課金サーバ側へ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログイン手段は、前記移動情報端末の識別子及び前記ウェブサーバ側から送信された通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、前記通信

トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることができる。

【００１８】

ここで、この発明のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記識別子送信手段により送信された識別子とが送信され、前記課金サーバにより、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記ウェブサーバにより送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００１９】

この発明のプログラムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を課金する課金サーバが該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するためのプログラムであって、課金サーバのコンピュータを、前記移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバから前記課金サーバへ送信された該所定の期間における所定のネットワークの利用権を示す通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段として機能させるためのプログラムであり、前記移動情報端末により、該移動通信部を介して前記移動通信部側ネットワークに接続し、通信トークンの購入に際し該移動通信部の識別子が前記ウェブサーバへ送信され、該ウェブサーバにより、送信された該識別子が該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンが該移動通信部を介して該情報処理部へ送信され、前記課金サーバへ該通信トークンの料金が送信されるものであり、前記移動情報端末により、従前に接続された前記移動通信部側ネットワークとの接続が解除され、前記移動通信部の識別子及び前記ウェブサーバから送信された前記通信トークンを用い、該移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用が試みられ、該認証サーバにより、移動情報端末により用いられた該識別子及び該通信トークンが前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子及び該通信トークンに基づき該通信トークンの正当性が認証された場合、該移動通信部を介して該情報処理部へ該所定のネットワークの利用を認める通知が送信され、該移動情報端末により、該認証サーバを介して該所定のネットワークの利用が行なわれることを特徴とするプログラムである。

【００２０】

ここで、この発明のプログラムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記ウェブサーバから前記課金サーバへ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記移動情報端末により、前記移動通信部の識別子及び前記ウェブサーバ側から該移動通信部を介して該情報処理部へ送信された前記通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用が試みられ、前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部

へ前記所定のネットワークの利用を認める通知が送信されることができる。

【００２１】

ここで、この発明のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記移動情報端末により、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子が前記ウェブサーバへ送信され、前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記移動情報端末により送信された識別子とが送信され、前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００２２】

ここで、この発明のプログラムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００２３】

ここで、この発明のプログラムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。

【００２４】

この発明の記録媒体は、本発明のいずれかのプログラムを記録したコンピュータ読取り可能な記録媒体である。

【００２５】

この発明のデータ通信料金課金方法は、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金方法であって、前記移動情報端末が、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続ステップと、前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信ステップと、前記ウェブサーバが、前記ウェブサーバと接続され前記通信トークンを発行する通信トークン発行サーバへ、前記識別子送信ステップで送信された識別子を送信するウェブサーバ側識別子送信ステップと、前記記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信ステップと、前記ウェブサーバが、前記通信トークン送信ステップで送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信ステップと、前記ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金を送信する通信トークン料金送信ステップと、前記移動情報端末が、前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除ステップと、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログインステップと、前記認証サーバが、前記ログインステップで用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信ステップと、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する

通信トークン認証ステップと、前記認証サーバが、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知ステップと、前記移動情報端末が、前記利用通知ステップで前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して前記所定のネットワークの利用を行う所定のネットワーク利用ステップと、前記課金サーバが、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金ステップとを備えたことを特徴とする。

【００２６】

ここで、この発明のデータ通信料金課金方法において、前記移動通信部が無線ＬＡＮを介して該所定のネットワークの利用を行う場合、前記通信トークン料金送信ステップで送信された該通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログインステップは、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い前記無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、前記利用可通知ステップは、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報端末装置へ前記所定のネットワークの利用を認める通知を送信することができる。

【００２７】

ここで、この発明のデータ通信料金課金方法において、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバ側識別子送信ステップに先立ち、前記ウェブサーバが該認証を行うウェブサーバ側認証ステップをさらに備えることができる。

【００２８】

ここで、この発明のデータ通信料金課金方法において、前記通信トークン送信ステップは、前記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子と所定の鍵と所定の乱数とに基づき通信トークンを生成して前記ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、前記通信トークン認証ステップは、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信ステップで該識別子と関連付けて記録された所定の乱数とに基づき該通信トークンの正当性を認証することができる。

【００２９】

ここで、この発明のデータ通信料金課金方法において、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信ステップは、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記通信トークン料金送信ステップは、前記課金サーバへ前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金と前記識別子送信ステップで送信された識別子とを送信し、前記区分課金ステップは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信ステップで送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００３０】

ここで、この発明のデータ通信料金課金方法において、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００３１】
ここで、この発明のデータ通信料金課金方法において、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。
【発明の効果】
【００３２】
本発明のデータ通信料金課金システム等によれば、所定のネットワーク用の通信トークンを携帯電話コンテンツ用ネットワークに接続された配信サイトが稼動するウェブサーバ経由で購入するに際し、好適には携帯電話器およびＰＣから構成される移動情報端末のＰＣから携帯電話器を介して携帯電話器の識別子ＩＤをウェブサーバへ送信する。送信された識別子ＩＤはウェブサーバにより通信トークン発行サーバへ送信される。通信トークン発行サーバは送信された携帯電話器の識別子ＩＤに基づき通信トークンを生成し、この生成された通信トークンをウェブサーバへ送信する。生成した通信トークンは携帯電話器の識別子ＩＤと紐付けされた状態で記録しておく。送信された通信トークンはウェブサーバにより携帯電話器を介してＰＣへ送信される。その後、携帯電話コンテンツ用ネットワークとの接続を一旦解除した後、改めて携帯電話器の識別子ＩＤおよび上記通信トークンを用い、ＰＣ側から携帯電話器および認証サーバを介して所定のネットワークの利用を試みる。認証サーバは携帯電話器の識別子ＩＤおよび通信トークンを通信トークン発行サーバへ送信する。通信トークン発行サーバは送信された識別子ＩＤおよび通信トークンに基づき当該通信トークンの正当性を認証する。従前に、生成された通信トークンＴ（従前）は携帯電話器の識別子ＩＤ（従前）と紐付けされた状態で記録されているため、送信された識別子ＩＤおよび通信トークンと、記録されている識別子ＩＤ（従前）および通信トークン（従前）とが一致する場合、従前に携帯電話コンテンツ用ネットワークを介して通信トークン（従前）を購入する際に用いられた携帯電話器と、現在所定のネットワークの利用を試みようとしている際に用いられている携帯電話器とが同一であると認証することができる。認証結果はウェブサーバ側へ通知される。以上のように、上記通信トークン購入時における認証（コンテンツ認証）と購入後における認証（通信認証）とを対応させることができる。この結果、携帯電話コンテンツ用ネットワークから所定のネットワークへの通信の切替を行った場合であってもユーザ（携帯電話器）の対応が付けられる。このため、課金サーバは通信事業者側サーバから送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器のデータ通信に対する料金から、当該所定の期間におけるウェブサーバにより送信された通信トークンの料金を控除した額を携帯電話器側の請求先（携帯電話器の所有者または利用者であるユーザ）に課金し、当該通信トークンの料金を他の請求先（上記ユーザに対して所定の関係を有する側）に課金することができる。従って、ユーザが業務上、インターネット（所定のネットワークの一例）上のサーバへアクセスする場合であっても、上述した通信トークンを用いることにより容易に公私分計することができる。さらに、本発明のデータ通信料金課金システムはキャリヤ側の設備だけで実現することができるため、キャリヤ側からみて極めて信頼度の高いシステムである。この結果、携帯電話器の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することができるという効果がある。
【発明を実施するための最良の形態】
【００３３】
以下、各実施例について図面を参照して詳細に説明する。
【実施例１】
【００３４】
図１は、本発明の実施例１におけるデータ通信料金課金システム１を示す。図１において、符号９０は移動通信機能を有する移動通信部１０と情報処理機能を有する情報処理部

２０とを備えた移動情報端末である。移動情報端末９０は移動通信部１０と情報処理部２０とを備えた１台の装置として構成することができる。あるいは移動情報端末９０は、好適には移動通信部１０を携帯電話器１０とし、好適には情報処理部２０をパーソナルコンピュータＰＣ２０とし、携帯電話器１０とＰＣ２０とを脱着可能に接続した構成とすることもできる。以下では、移動情報端末９０は携帯電話器１０とＰＣ２０とが脱着可能に接続した構成であるものとする。携帯電話器１０のユーザは携帯電話器１０の所有者または利用者と想定する。携帯電話器１０とＰＣ２０との間の接続は脱着可能な接続方式、例えばＵＳＢ（Universal Serial Bus）ケーブル１１を用いることが好適である。しかし、ＵＳＢ等の接続方式に限定されるものではなく、無線等であってもよいことは勿論である。なお本明細書において、「携帯電話器」は携帯電話装置または携帯電話機と呼んでもよい。続いて、符号１３は移動体通信網、１４は移動体通信網１３に接続された通信事業者側サーバ、１２は移動体通信網１３に接続された基地局であり、携帯電話器１０は基地局１２のエリア内に在圏しているものと想定する。符号１５は通信事業者側サーバ１４と接続された携帯電話コンテンツ用ネットワーク（移動通信部側ネットワーク）、３０は携帯電話コンテンツ用ネットワーク１５に接続されソフトウェアの配信を行う配信サイトが稼動するウェブ（Ｗｅｂ）サーバである。通信事業者側サーバ１４は携帯電話器１０が携帯電話コンテンツ用ネットワーク１５に接続する際の認証課金を行う。続いて、符号４０はウェブサーバ３０と接続され所定のネットワーク１６の利用権を示す通信トークン（ワンタイム通信トークン）を発行する通信トークン発行サーバ、６０はウェブサーバ３０と接続され移動情報端末９０の携帯電話器１０に掛かるデータ通信料金を課金する課金サーバ、５０は所定のネットワーク１６に接続された認証サーバである。所定のネットワークとしては、携帯電話器１０のユーザが業務上使用する企業内ネットワーク、インターネット等が好適である。認証サーバ５０は通信トークン発行サーバ４０と接続されている。図１に示されるように、携帯電話器１０は移動体通信網１３および携帯電話コンテンツ用ネットワーク１５を介してウェブサーバ３０と接続されている。ウェブサーバ３０と通信トークン発行サーバ４０との間の接続、ウェブサーバ３０と課金サーバ６０との間の接続、通信事業者側サーバ１４と課金サーバ６０との間の接続、認証サーバ５０と通信トークン発行サーバ４０との間の各接続はＶＰＮ（Virtual Private Network）等の専用通信網によることが好適である。上述のように、移動通信部の例として携帯電話器１０を用いて説明するが、移動通信部１０は携帯電話器１０に限定されるものではなく、ＰＨＳ（Personal Handyphone System）等であってもよい。同様に、情報処理部２０の例としてＰＣ２０を用いて説明するが、ＰＣ２０に限定されるものではなく、ＰＤＡ（Personal Digital Assistant）等、携帯電話器１０と接続可能な情報処理装置であれば他の装置であってもよい。

【００３５】

図１において、符号２１はＰＣ２０が備える機能を示す機能ブロックである。機能ブロック２１において、符号２２は携帯電話器１０を介して携帯電話コンテンツ用ネットワーク１５に接続するネットワーク接続部（移動通信部側ネットワーク接続手段）、２３は、例えば携帯電話器１０のユーザが業務上必要とする所定のネットワーク１６用の通信トークンを自己が所有する携帯電話器１０を用いて上記配信サイト経由で購入するに際し、携帯電話器１０の識別子（例えば携帯電話器１０の電話番号等）をウェブサーバ３０へ送信する識別子送信部（識別子送信手段）、２４はウェブサーバ３０側から携帯電話器１０を介して通信トークンが携帯コンテンツとみなされて送信された後、ネットワーク接続部２２により接続された携帯電話コンテンツ用ネットワーク１５との接続を解除するネットワーク接続解除部（移動通信部側ネットワーク接続解除手段）、２５は携帯電話器１０の識別子およびウェブサーバ３０側から送信された通信トークンを用い、携帯電話器１０および認証サーバ５０を介して所定のネットワーク１６の利用を試みるログイン部（ログイン手段）、２６は認証サーバ５０から所定のネットワーク１６の利用を認める通知が送信された場合、認証サーバ５０を介して所定のネットワーク１６の利用を行う所定のネットワーク利用部（所定のネットワーク利用手段）である。以上のＰＣ２０が備える機能は、ＰＣ２０に配置されＰＣ２０のコンピュータに上述の各機能を実行させるための通信認証接

続ソフトウェアとして実現することができる。識別子送信部２３がウェブサーバ３０へ送信する識別子は、携帯電話器１０の識別子に限定されるものではなく、ＰＣ２０の識別子（例えばＰＣ２０の製造番号等）であってもよい。あるいは、携帯電話器１０およびＰＣ２０から構成される移動情報端末９０の識別子とすることもできる。

【００３６】

図１において、符号３１はウェブサーバ３０が備える機能を示す機能ブロックである。機能ブロック３１において、符号３２は識別子送信部２３により送信された識別子を通信トークン発行サーバ４０へ送信するウェブサーバ側識別子送信部（ウェブサーバ側識別子送信手段）、３４は通信トークン発行サーバ４０から送信された通信トークンを携帯電話器１０を介してＰＣ２０へ送信するウェブサーバ側通信トークン送信部（ウェブサーバ側通信トークン送信手段）、３６は課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金を送信する通信トークン料金送信部（通信トークン料金送信手段）である。携帯電話器１０のユーザが通信トークンを購入する時点では、通常、通信トークンの料金は予め定まっているが、未確定であってもよい。後述するように、課金サーバ６０が通信料金の公私分計を行うため、携帯電話器１０のユーザは業務上使用する通信トークンの料金を考慮する必要はない。

【００３７】

図１において、符号５１は認証サーバ５０が備える機能を示す機能ブロックである。機能ブロック５１において、符号５２はログイン部２５により用いられた携帯電話器１０の識別子および通信トークンを通信トークン発行サーバ４０へ送信する識別子・通信トークン送信部（識別子・通信トークン送信手段）、５４は通信トークン発行サーバ４０により上記通信トークンの正当性が認証された場合、携帯電話器１０を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知を送信する利用可通知部（利用可通知手段）である。

【００３８】

図１において、符号４１は通信トークン発行サーバ４０が備える機能を示す機能ブロックである。機能ブロック４１において、符号４２はウェブサーバ側識別子送信部３２により送信された携帯電話器１０の識別子に基づき上記通信トークンを生成し、この生成された通信トークンをウェブサーバ３０へ送信する通信トークン送信部（通信トークン送信手段）、４４は識別子・通信トークン送信部５２により送信された識別子および通信トークンに基づき当該通信トークンの正当性を認証する通信トークン認証部（通信トークン認証手段）である。通信トークン送信部４２は、生成した通信トークンを携帯電話器１０の識別子と紐付けされた状態で記録しておく。通信トークン認証部４４の認証結果は認証サーバ５０側へ通知される。

【００３９】

図１において、符号６１は課金サーバ６０が備える機能を示す機能ブロックである。機能ブロック６１において、符号６２は、通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ等）に課金し、当該通信トークンの料金を他の請求先（携帯電話器１０の所有者または利用者であるユーザに対して所定の関係を有する側等）に課金する区分課金部（区分課金手段）である。以上により、携帯電話器１０のユーザが業務上必要とする所定のネットワーク１６用の通信トークンを自己が所有する携帯電話器１０を用いて上記配信サイト経由で購入した場合、業務上用いた通信トークンの料金は上記他の請求先に課金されることになる。この結果、携帯電話器１０のユーザが私用で用いたデータ通信料金と業務上用いたデータ通信料金(通信トークンの料金)とが公私分計されることになる。所定の関係を有する側としては、例えばユーザが会社員である場合、当該会社員の雇用者、即ち会社であるものとすることができる。当該会社員が自社のネットワーク（所定のネットワーク１６）にログインする場合、業務上用いた当該自社のネットワークに関する通信トークンの料金

は会社側に課金されることになり、公私分計されることになる。あるいは、所定の関係を有する側としては、例えばユーザがコンシューマー向けの会員制情報提供サービスの会員である場合、当該コンシューマー向けの会員制情報提供サービスの提供者であるものとすることもできる。当該会員が当該会員制情報提供サービスのネットワーク（所定のネットワーク１６）にログインする場合、利用した当該会員制情報提供サービスのネットワークに関する通信トークンの料金は、当該会員制情報提供サービスの提供者側に課金されることになり、一種の分計が行なわれることになる。

【００４０】

図２は、データ通信料金課金システム１の構成要素であるＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０、課金サーバ６０で実行される各プログラムの流れまたはデータ通信料金課金方法をフローチャートで示す。図２において、左側からＰＣ２０で実行されるプログラム等のフローチャート、ウェブサーバ３０で実行されるプログラム等のフローチャート、通信トークン発行サーバ４０で実行されるプログラム等のフローチャート、認証サーバ５０で実行されるプログラム等のフローチャート、課金サーバ６０で実行されるプログラム等のフローチャートであり、各構成要素間の通信は点線で示す。

【００４１】

図２に示されるように、まず、ＰＣ２０が、携帯電話器１０を介して携帯電話コンテンツ用ネットワーク１５に接続する（移動通信部側ネットワーク接続ステップ。ステップＳ２２）。移動通信部側ネットワーク接続ステップ（ステップＳ２２）で接続された携帯電話コンテンツ用ネットワーク１５に接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバ３０へ、所定のネットワーク１６の利用権を示す通信トークンの購入を行うために、携帯電話器１０の識別子ＩＤを送信する（識別子送信ステップ。ステップＳ２３）。

【００４２】

次に、ウェブサーバ３０が、ウェブサーバ３０と接続され通信トークンを発行する通信トークン発行サーバ４０へ、識別子送信ステップ（ステップＳ２３）で送信された識別子ＩＤを送信する（ウェブサーバ側識別子送信ステップ。ステップＳ３２）。

【００４３】

続いて、通信トークン発行サーバ４０が、ウェブサーバ側識別子送信ステップ（ステップＳ３２）で送信された識別子ＩＤに基づき通信トークンＴを生成してウェブサーバ３０へ送信する（通信トークン送信ステップ。ステップＳ４２）。通信トークン発行サーバ４０は生成した通信トークンＴを携帯電話器１０の識別子ＩＤと紐付けした状態で記録しておく。

【００４４】

ウェブサーバ３０が、通信トークン送信ステップ（ステップＳ４２）で送信された通信トークンＴを携帯電話器１０を介してＰＣ２０へ送信する（ウェブサーバ側通信トークン送信ステップ。ステップＳ３４）。ウェブサーバ３０と接続され携帯電話器１０のデータ通信料金を課金する課金サーバ６０へ、ウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴの料金Ｂを送信する（通信トークン料金送信ステップ。ステップＳ３６）。

【００４５】

ＰＣ２０が、移動通信部側ネットワーク接続ステップ（ステップＳ２２）で接続された携帯電話コンテンツ用ネットワーク１５との接続を解除する（移動通信部側ネットワーク接続解除ステップ。ステップＳ２４）。携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴを用い、携帯電話器１０および所定のネットワーク１６に接続された認証サーバ５０を介して所定のネットワーク１６の利用を試みる（ログインステップ。ステップＳ２５）。

【００４６】

認証サーバ５０が、ログインステップ（ステップＳ２５）で用いられた識別子ＩＤおよ

び通信トークンＴを通信トークン発行サーバ４０へ送信する（識別子・通信トークン送信ステップ。ステップＳ５２）。

【００４７】

通信トークン発行サーバ４０が、識別子・通信トークン送信ステップ（ステップＳ５２）で送信された識別子ＩＤおよび通信トークンＴに基づき通信トークンＴの正当性を認証する（通信トークン認証ステップ。ステップＳ４４）。上述のように、通信トークンＴ（従前）は携帯電話器１０の識別子ＩＤ（従前）と紐付けされた状態で記録されているため、識別子・通信トークン送信ステップ（ステップＳ５２）で送信された識別子ＩＤおよび通信トークンＴと、記録されている識別子ＩＤ（従前）および通信トークンＴ（従前）とが一致する場合、通信トークン発行サーバ４０は従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴを購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。通信トークン認証ステップ（ステップＳ４４）において、上記認証結果Ｎは認証サーバ５０側へ通知される。

【００４８】

認証サーバ５０は、通信トークン認証ステップ（ステップＳ４４）で通信トークンＴの正当性が認証された場合、すなわち通知された認証結果Ｎが正当性を認証したことを示す場合、携帯電話器１０を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍを送信する（利用可通知ステップ。ステップＳ５４）。

【００４９】

ＰＣ２０は、認証サーバ５０から所定のネットワーク１６の利用を認める通知Ｍが送信された場合、認証サーバ５０を介して所定のネットワーク１６の利用を行う（所定のネットワーク利用ステップ。ステップＳ２６）。

【００５０】

課金サーバ６０は、携帯電話器１０が携帯電話コンテンツ用ネットワーク１５に接続する際の認証課金を行う通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信ステップ（ステップＳ３６）で送信された通信トークンＴの料金Ｂを控除した額を携帯電話器１０側の請求先に課金し、通信トークンＴの料金Ｙを他の請求先に課金する（区分課金ステップ。ステップＳ６２）。

【００５１】

以上より、本発明の実施例１によれば、識別子送信部２３は所定のネットワーク１６用の通信トークンＴを配信サイト経由で購入するに際し、携帯電話器１０の識別子ＩＤをウェブサーバ３０へ送信する。識別子送信部２３により送信された識別子ＩＤはウェブサーバ側識別子送信部３２により通信トークン発行サーバ４０へ送信される。通信トークン送信部４２はウェブサーバ側識別子送信部３２により送信された携帯電話器１０の識別子ＩＤに基づき通信トークンＴを生成し、この生成された通信トークンＴをウェブサーバ３０へ送信する。通信トークン送信部４２は生成した通信トークンＴを携帯電話器１０の識別子ＩＤと紐付けした状態で記録しておく。送信された通信トークンＴはウェブサーバ側通信トークン送信部３４により携帯電話器１０を介してＰＣ２０へ送信される。その後、ネットワーク接続解除部２４がネットワーク接続部２２により接続された携帯電話コンテンツ用ネットワーク１５との接続を解除する。携帯電話器１０とＰＣ２０との間は接続状態のままでよい。一旦携帯電話コンテンツ用ネットワーク１５との接続が解除された後、改めてログイン部２５が携帯電話器１０の識別子ＩＤおよび上記通信トークンＴを用い、携帯電話器１０および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。識別子・通信トークン送信部５２はログイン部２５により用いられた携帯電話器１０の識別子ＩＤおよび通信トークンＴを通信トークン発行サーバ４０へ送信する。通信トークン認証部４４は識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴに基づき当該通信トークンＴの正当性を認証する。従前に通信トークン送信部４２により生成された通信トークンＴ（従前）は携帯電話器１０の識別子ＩＤ（従前）と紐付

けされた状態で記録されているため、識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴと、記録されている識別子ＩＤ（従前）および通信トークンＴ（従前）とが一致する場合、通信トークン認証部４４は、従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴ（従前）を購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。通信トークン認証部４４の認証結果Ｎは認証サーバ５０側へ通知される。

【００５２】

以上のように、上記通信トークンＴ購入時における認証（コンテンツ認証）と購入後における認証（通信認証）とを対応させることができる。この結果、携帯電話コンテンツ用ネットワーク１５から所定のネットワーク１６への通信の切替を行った場合であってもユーザ（携帯電話器１０のユーザ）の対応が付けられる。このため、区分課金部６２は通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器１０のデータ通信に対する料金（＝Ａ）から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンＴの料金（＝Ｂ）を控除した額（＝Ａ－Ｂ）を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ）に課金し、当該通信トークンＴの料金（＝Ｂ）を他の請求先（上記ユーザに対して所定の関係を有する側、例えば雇用者側）に課金することができる。従って、ユーザが業務上、インターネット（所定のネットワーク１６の一例）上のサーバへアクセスする場合であっても、上述した通信トークンＴを用いることにより即時に公私分計することができる。さらに、本発明のデータ通信料金課金システム１はキャリヤ側の設備だけで実現することができるため、キャリヤ側からみて極めて信頼度の高いシステムである。この結果、携帯電話器１０の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ２０上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット１６上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することができる。

【実施例２】

【００５３】

実施例２では、携帯電話器１０が無線ＬＡＮを介して所定のネットワーク１６の利用を行う場合について説明する。

【００５４】

図３は、本発明の実施例２におけるデータ通信料金課金システム２を示す。図２で図１と同じ符号を付した箇所は同じ要素を示すため説明は省略する。図２に示されるデータ通信料金課金システム２が図１に示されるデータ通信料金課金システム１と異なる点は、ＰＣ２０が無線ＬＡＮ１７を介して所定のネットワーク１６の利用を行う場合のために、無線ＬＡＮ１７および無線ＬＡＮ１７に接続された無線ＬＡＮ基地局１８が追加された点と、当該追加に伴い、ＰＣ２０のログイン部２５の機能および認証サーバ５０の利用可通知部５４の機能が一部変更された点とである（各々、ログイン部２５’、利用可通知部５４’と示す）。

【００５５】

データ通信料金課金システム２では、通信トークン料金送信部３６により送信された通信トークンＴ’の料金Ｂ’には、実施例１で説明した所定のネットワーク１６の利用料に加えて無線ＬＡＮ１７の回線使用料金が含まれている。この無線ＬＡＮ１７の回線使用料金は、例えば無線ＬＡＮ基地局１８があるホットスポットの臨時課金である。ログイン部２５’は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信部３４により送信された通信トークンＴ’を用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。利用可通知部５４’は、通信トークン認証部４４により通信トークンＴ’の正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信する。他の処理

は実施例１と同様であるため説明は省略する。

【００５６】

実施例２のデータ通信料金課金方法は、上述した実施例１のデータ通信料金課金方法において、通信トークン料金送信ステップ（ステップＳ３６）で送信された通信トークンＴ’の料金Ｂ’が無線ＬＡＮ１７の回線使用料金を含み、ログインステップ（ステップＳ２５）は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴを用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みることになる。利用可通知ステップ（ステップＳ５４）は、通信トークン認証ステップ（ステップＳ４４）で通信トークンＴの正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信することになる。他の処理は図２に示される実施例１の処理と同様であるため説明は省略する。

【００５７】

以上より、本発明の実施例２によれば、データ通信料金課金システム２における通信トークンＴ’の料金Ｂに、所定のネットワーク１６の利用料に加えて無線ＬＡＮ１７の回線使用料金を含ませておく。ログイン部２５’は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信部３４により送信された通信トークンＴ’を用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。利用可通知部５４’は、通信トークン認証部４４により通信トークンＴ’の正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信する。この結果、携帯電話器１０は無線ＬＡＮ１７を介して所定のネットワーク１６の利用を行うことができる。区分課金部６２は、実施例１と同様に、通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器１０のデータ通信に対する料金（＝Ａ）から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンＴ’の料金（＝所定のネットワーク１６の利用料＋無線ＬＡＮ１７の回線使用料金＝Ｂ’）を控除した額（＝Ａ－Ｂ’）を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ）に課金し、当該通信トークンＴ’の料金（＝Ｂ’）を他の請求先（上記ユーザに対して所定の関係を有する側、例えば雇用者側）に課金することができる。従って、ユーザが業務上、ホットスポットにおいて臨時的にインターネット（所定のネットワーク１６の一例）上のサーバへアクセスする場合であっても、上述した通信トークンＴ’を用いることにより、実施例１と同様に即時に公私分計することができる。

【実施例３】

【００５８】

上述した実施例１および２の各データ通信料金課金システム１および２において、所定のネットワーク１６への接続が認証を必要とする場合のために、ウェブサーバ３０は当該認証（ユーザ認証）を行うウェブサーバ側認証部（ウェブサーバ側認証手段。不図示）をさらに備えることができる。所定のネットワーク１６が企業内ネットワーク等である場合、当該企業内ネットワーク等へログインするためにはユーザ認証を必要とする。あるいは、接続料金定額サービスの場合、通信時間またはパケット量の測定をしないケースもあるため、接続料金定額サービスを利用する場合にはユーザ認証を必要とする。本実施例３によれば、ウェブサーバ３０はユーザ認証を行うウェブサーバ側認証部を備えているため、所定のネットワーク１６への接続が認証を必要とする場合、当該認証を行うことができる。

【００５９】

実施例３のデータ通信料金課金方法は、上述した実施例１または２の各データ通信料金課金方法において、ウェブサーバ側識別子送信ステップ（ステップＳ３２）に先立ち、ウェブサーバ３０が上記認証を行うウェブサーバ側認証ステップ（不図示）をさらに備えればよい。他の処理は図２に示される実施例１の処理、上述した実施例２の処理と同様であるため説明は省略する。

【実施例４】
【００６０】
本実施例４では、上述した各実施例において通信トークンの生成の際に暗号化を用いる場合について説明する。暗号化以外については上述した各実施例と同様である。以下では、図１を適宜引用して説明する。
【００６１】
通信トークン送信部４２は、ウェブサーバ側識別子送信部３２により送信された識別子ＩＤと所定の鍵（秘密鍵等）Ｋと所定の乱数Ｒとに基づき通信トークンＴ＊（暗号化されたことを上付＊で示す。）を生成する。生成した通信トークンＴ＊をウェブサーバ３０へ送信する。通信トークン送信部４２は携帯電話器１０の識別子ＩＤと所定の乱数Ｒとを関連付け（紐付け）した状態で記録しておく。所定の鍵Ｋは携帯電話器１０によらず一定の鍵としておけばよいが、所定の鍵Ｋも識別子ＩＤと関連付けて記録しておいてもよいことは勿論である。通信トークン認証部４４は、識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴ＊と、所定の鍵Ｋと、通信トークン送信部４２により識別子ＩＤと関連付けて記録された所定の乱数Ｒとに基づき、通信トークンＴ＊の正当性を認証する。従前に通信トークン送信部４２により通信トークンＴ＊（従前）が生成された際、携帯電話器１０の識別子ＩＤ（従前）および所定の乱数Ｒとは紐付けされた状態で記録されている。このため、識別子・通信トークン送信部５２により送信された識別子ＩＤと同じ値の識別子ＩＤ（従前）を検索し、当該識別子ＩＤ（従前）に紐付けされている所定の乱数Ｒを求め、この所定の乱数Ｒと所定の鍵Ｋと識別子ＩＤとから通信トークンＴ＊（従前）を求める。この通信トークンＴ＊（従前）と識別子・通信トークン送信部５２により送信された通信トークンＴ＊とが一致した場合、通信トークン認証部４４は、従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴ＊（従前）を購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。
【００６２】
以上より、本発明の実施例４によれば、上述した各実施例で説明した機能に加えて、暗号化された通信トークンＴ＊を用いることができる。この結果、通信トークンＴ＊がコピーされていた場合、ＰＣ２０からのログイン要求を拒否することができる。この結果、上述した各実施例の効果に加えて、通信トークンＴ＊をコピーされないようにすることができるセキュリティ機能を有するデータ通信料金課金システムを構築することができる。
【実施例５】
【００６３】
上述したデータ通信料金課金システム１等では、携帯電話器１０の識別子は１つであることを想定していた。本実施例５では、携帯電話器１０は１つ以上の識別子を有し、上述した他の請求先も当該１つ以上の識別子に対応して１つ以上ある場合について説明する。
【００６４】
移動情報端末９０および課金サーバ６０は携帯電話器１０の１以上の識別子と当該１以上の識別子に各々対応する他の請求先との対応表１００（後述する図４参照）をさらに備えている。対応表１００は、例えばＰＣ２０および課金サーバ６０の記録装置７８ａ（図４参照）に記録されている。ＰＣ２０側では、識別子送信部２３’’（不図示）は、通信トークンの購入に際し対応表１００に基づき携帯電話器１０の１以上の識別子の内の一つの識別子をウェブサーバ３０へ送信する。ウェブサーバ３０側では、通信トークン料金送信部３６’’（不図示）は、課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金と識別子送信部２３’’により送信された識別子とを送信する。課金サーバ６０側では、区分課金部６２’’は、通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６’’により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先に課金し、上記通信トークンの料金を通信トークン料金送信部３６’’により送信された識別子に対応する対応表１００中の他の請求先に

課金する。

【００６５】

以上により、本発明の実施例５によれば、移動情報端末９０および課金サーバ６０は携帯電話器１０の１以上の識別子と当該１以上の識別子に各々対応する他の請求先との対応表１００をさらに備えている。識別子送信部２３’’は、通信トークンの購入に際し対応表１００に基づき携帯電話器１０の１以上の識別子の内の一つの識別子をウェブサーバ３０へ送信する。通信トークン料金送信部３６’’は、課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金と識別子送信部２３’’により送信された識別子とを送信する。区分課金部６２’’は、通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６’’により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先に課金し、上記通信トークンの料金を通信トークン料金送信部３６’’により送信された識別子に対応する対応表１００中の他の請求先に課金する。この結果、携帯電話器１０は複数の識別子を使い分けることにより、通信トークンの料金を複数の他の請求先へ課金させることができる。

【実施例６】

【００６６】

図４は、上述した各実施例を実現するための本発明のコンピュータ・プログラムを実行するＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０および課金サーバ６０のコンピュータの内部回路７０を示すブロック図である。図４に示されるように、ＣＰＵ７１、ＲＯＭ７２、ＲＡＭ７３、画像制御部７６、コントローラ７７、入力制御部７９、無線ＬＡＮ１７とのインタフェース機能を有する通信メディアインタフェース（Ｉ／Ｆ）部８１および入出力Ｉ／Ｆ部８２はバス８３に接続されている。図４において、上述の本発明のコンピュータ・プログラム（ＰＣ２０側のプログラム、課金サーバ６０側のプログラム等）は、ＲＯＭ７２、ＨＤ等の記録装置７８ａ、またはＤＶＤ若しくはＣＤ－ＲＯＭ７８ｎ等の記録媒体（脱着可能な記録媒体を含む）に記録されている。本発明のコンピュータ・プログラムは、ＲＯＭ７２からバス８３を介し、あるいは記録装置７８ａまたはＤＶＤ若しくはＣＤ－ＲＯＭ７８ｎ等の記録媒体からコントローラ７７を経由してバス８３を介しＲＡＭ７３へロードされる。内部回路７０がＰＣ２０および課金サーバ６０の場合、図４に示されるように記録装置７８ａには対応表１００が記録されている。入力制御部７９は、マウス、テンキー等の入力操作部８０と接続され入力制御等を行う。画像メモリであるＶＲＡＭ７５はＰＣ２０の表示部７４の少なくとも一画面分のデータ容量に相当する容量を有しており、画像制御部７６はＶＲＡＭ７５のデータを画像データへ変換して表示部７４へ送出する機能を有している。入出力Ｉ／Ｆ部８２は入出力インタフェース機能を有しており、ＵＳＢケーブル１１等により携帯電話器１０の入出力Ｉ／Ｆ部（不図示）と接続されている。

【００６７】

上述のようにＣＰＵ７１が本発明のコンピュータ・プログラムを実行することにより、本発明の目的を達成することができる。当該コンピュータ・プログラムは上述のようにＤＶＤまたはＣＤ－ＲＯＭ７８ｎ等の記録媒体の形態でコンピュータＣＰＵ７１に供給することができ、当該コンピュータ・プログラムを記録したＤＶＤまたはＣＤ－ＲＯＭ７８ｎ等の記録媒体も同様に本発明を構成することになる。当該コンピュータ・プログラムを記録した記録媒体としては上述された記録媒体の他に、例えばメモリ・カード、メモリ・スティック、光ディスク、ＦＤ等を用いることができる。

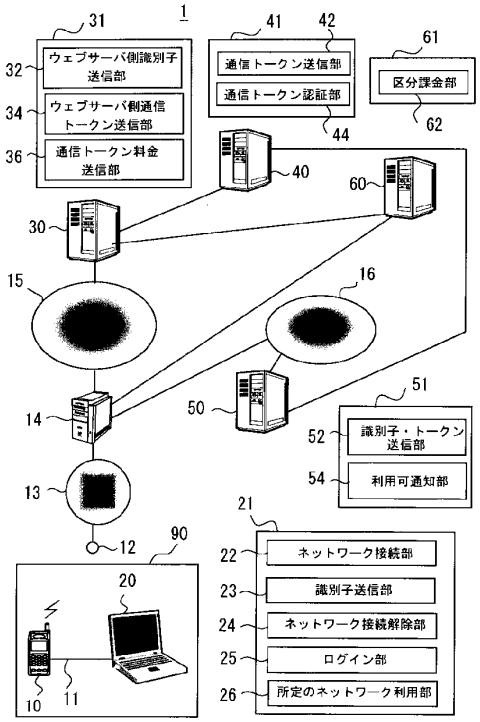
【産業上の利用可能性】

【００６８】

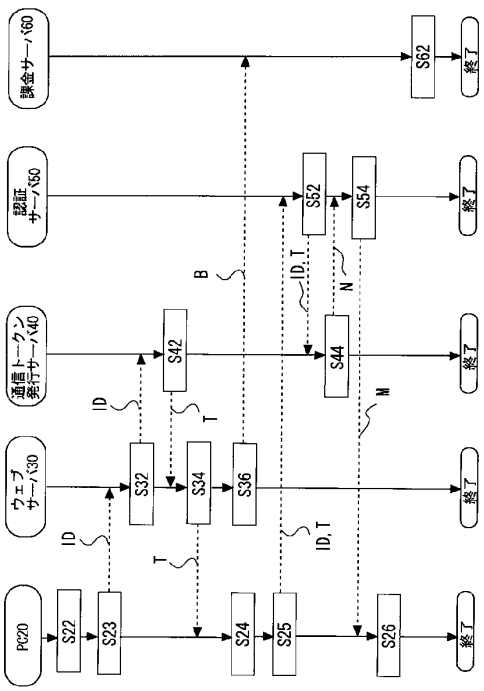
本発明の活用例として、上述のように公私分計を即時に行うことができるため、会社所有のＰＣおよび携帯電話器を用いた所定のネットワーク１６の利用に対する従来の会社側との割引契約に、個人所有のＰＣおよび携帯電話器を用いた場合における所定のネットワーク１６の利用に対しても即時に割引を適用するシステムへの応用が挙げられる。

【図面の簡単な説明】
【００６９】
【図１】本発明の実施例１におけるデータ通信料金課金システム１を示す図である。
【図２】データ通信料金課金システム１の構成要素であるＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０、課金サーバ６０で実行される各プログラムの流れまたはデータ通信料金課金方法を示すフローチャートである。
【図３】本発明の実施例２におけるデータ通信料金課金システム２を示す図である。
【図４】上述した各実施例を実現するための本発明のコンピュータ・プログラムを実行するＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０および課金サーバ６０のコンピュータの内部回路７０を示すブロック図である。
【符号の説明】
【００７０】
１、２　データ通信料金課金システム、　１０　携帯電話器、　１１　ＵＳＢケーブル、　１２　基地局、　１３　移動体通信網、　１４　通信事業者側サーバ、　１５　携帯電話コンテンツ用ネットワーク、　１６　所定のネットワーク、　１７　無線ＬＡＮ、　１８　無線ＬＡＮ基地局、　２０　ＰＣ、　２１、３１、４１、５１、６１　機能ブロック、　２２　ネットワーク接続部、　２３　識別子送信部、　２４　ネットワーク接続解除部、　２５、２５’　ログイン部、　２６　所定のネットワーク利用部、　３０　ウェブサーバ、　３２　ウェブサーバ側識別子送信部、　３４　ウェブサーバ側通信トークン送信部、　３６　通信トークン料金送信部、　４０　通信トークン発行サーバ、　４２　通信トークン送信部、　４４　通信トークン認証部、　５０　認証サーバ、　５２　識別子・通信トークン送信部、　５４、５４’　利用可通知部、　６０　課金サーバ、　６２　区分課金部、　７０　内部ブロック、　７１　ＣＰＵ、　７２　ＲＯＭ、　７３　ＲＡＭ、　７４　表示部、　７５　ＶＲＡＭ、　７６　画像制御部、　７７　コントローラ、　７８ａ　記録装置、　７８ｎ　記録媒体、　７９　入力制御部、　８０　入力操作部、　８１　通信メディアＩ／Ｆ部、　８２　入出力Ｉ／Ｆ部、　８３　バス、　９０　移動情報端末、　１００　対応表。

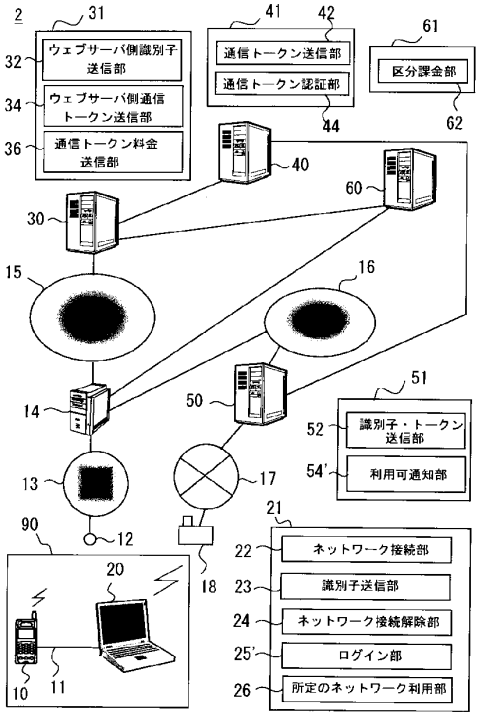
【図１】


1
31
ウェブサーバ側識別子送信部
32
ウェブサーバ側通信トークン送信部
34
通信トークン料金送信部
36
41
42
通信トークン送信部
通信トークン認証部
44
61
区分課金部
62
40
60
30
15
16
14
50
51
52
識別子・トークン送信部
54
利用可通知部
13
12
90
21
22
ネットワーク接続部
23
識別子送信部
24
ネットワーク接続解除部
25
ログイン部
26
所定のネットワーク利用部
20
10
11

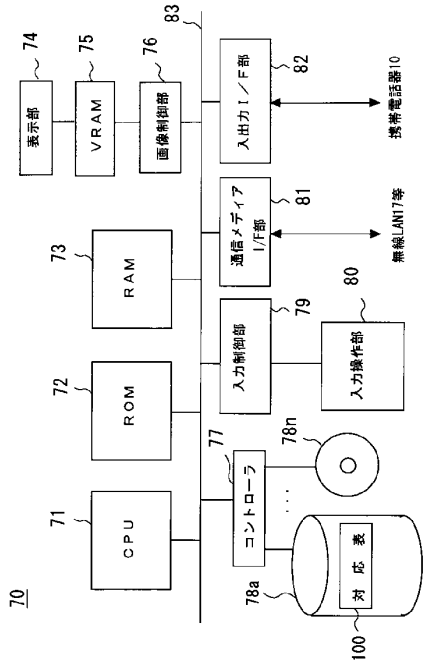
【図２】


課金サーバ60
認証サーバ50
通信トークン発行サーバ40
ウェブサーバ30
PC20
S22
S23
S24
S25
S26
S32
S34
S36
S42
S44
S52
S54
S62
終了
ID
T
ID,T
B
N
M

【図３】


2
31
ウェブサーバ側識別子送信部
32
ウェブサーバ側通信トークン送信部
34
通信トークン料金送信部
36
41
42
通信トークン送信部
通信トークン認証部
44
61
区分課金部
62
40
60
30
15
16
14
50
51
52
識別子・トークン送信部
54'
利用可通知部
13
17
18
90
12
21
22
ネットワーク接続部
23
識別子送信部
24
ネットワーク接続解除部
25'
ログイン部
26
所定のネットワーク利用部
20
10
11

【図４】


70
CPU
71
RAM
73
ROM
72
74
表示部
75
VRAM
76
画像制御部
77
コントローラ
78n
78a
対応表
100
79
入力制御部
80
入力操作部
81
通信メディアI/F部
82
入出力I/F部
83
携帯電話器10
無線LAN17等

フロントページの続き

Ｆターム(参考) 5K201 AA05 AA09 BD05 CB13 DC02 EA07 EC06 ED06 FA07

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2006 (02.02.2006)

PCT

(10) International Publication Number
WO 2006/012610 A2

(51) International Patent Classification[7]: H04L 29/08, 29/06

(21) International Application Number: PCT/US2005/026296

(22) International Filing Date: 22 July 2005 (22.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/590837	23 July 2004 (23.07.2004)	US
60/601431	13 August 2004 (13.08.2004)	US
60/607420	3 September 2004 (03.09.2004)	US
60/608814	10 September 2004 (10.09.2004)	US

(71) Applicant *(for all designated States except US)*: **CITRIX SYSTEMS, INC.** [US/GB]; 851 West Cypress Creek Road, Fort Lauderdale, FL 33309 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RAO, Goutham, P.** [US/US]; 6963 Starling Valley Drive, San Jose, CA 95120 (US). **BRUEGGEMANN, Eric** [US/US]; 5642 Stevens Creek Blvd., no.606, Cupertino, CA 95014 (US). **RODRIGUEZ, Robert** [US/US]; 5647 Wells Court, San Jose, CA 95123 (US).

(74) Agents: **LANZA, John, D.** et al.; Lahive & Cockfield, LLP, 28 State Street, Boston, MA 02109 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SYSTEMS AND METHODS FOR OPTIMIZING COMMUNICATIONS BETWEEN NETWORK NODES

(57) **Abstract:** The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. Additionally, the present invention provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access.

WO 2006/012610 A2

SYSTEMS AND METHODS FOR OPTIMIZING COMMUNICATIONS BETWEEN NETWORK NODES

Related Applications

This present application claims priority to U.S. Provisional Patent Application Number 60/590,837, entitled "Ad Hoc Distributed Networks And Remote Access Architecture", filed July 23, 2004, and U.S. Provisional Patent Application Number 60/601,431, entitled "System And Method For Assuring Redundancy In Remote Access Solution", filed August 13, 2004, and U.S. Provisional Patent Application Number 60/607,420, entitled "Virtual Network Bridging", filed September 3, 2004, and U.S. Provisional Patent Application Number 60/608,814, entitled "System And Method For Assuring Redundancy In Remote Access Solution", filed September 10, 2004, all of which are incorporated herein by reference.

Technical Field

The invention generally relates to optimizing network communications between nodes on a network.

Background Information

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, such as the Internet, to maintain privacy through the use of tunneling and security mechanisms. As such, a VPN provides for data encryption and security for corporate data traversing the public network. In addition to addressing secure access to corporate data via a public network, VPNs are also directed towards routing network traffic from two disconnected, otherwise non-routable networks. For example, a first private network with private internet protocol addresses in the range 10.0.0.0 – 10.255.255.255 may communicate via a VPN with a second private network with private internet protocol addresses in the range 192.168.0.0 – 192.168.255.255. The VPN allows a remote machine on the first private network to communicate with an internal machine on the second private network by tunneling network traffic from the remote machine and making the network traffic appear on the second private network. This may work well for client-server protocols where a remote computer is transacting with an enterprise server located on a remote network.

However, traditional VPNs may not work well in the case where two remote computers tunnel via a VPN gateway to communicate directly with each other, such as in peer-to-peer protocols. The VPN achieves this peer-to-peer computing by flattening the disjoint private network address spaces in which the two remote computers tunnel all peer-to-peer communications via the VPN gateway. As a result, network traffic from one of the peers flows through the VPN gateway and switches tunnels on the intranet to flow back out on the internet to the peer computer. The network traffic between the peer computers may travel longer and less optimal routes event though the peer computers may have a shorter direct path between then. It would be useful to allow remote computers to benefit from the security afforded by VPNs without incurring the drawback of longer data paths routes.

Other inefficiencies exist with direct communications over a network between two computers. For example, the network connection is susceptible to breakdown. For instance, a wireless connection between a client and a server is often unreliable. In other cases, the network connection is intermittent. A connection can be lost when one enters an elevator or tunnel and may only be restored following one's exit from the elevator or tunnel. In another example, a connection can be disrupted when a mobile computing device moves from network access point to network access point, such as in a wireless network topology.

If an established communication session between the client and the server computer abnormally terminates, the client generally has to re-establish the connection by starting a new communication session. To begin the new communication session, the user typically has to retransmit the authentication credentials, such as a login/password pair, to the server computer so that the server computer can authorize the user for the new communication session. This retransmission of the authentication credentials of a user across multiple communication sessions repeatedly exposes the authentication credentials of that user to potential attackers, thereby decreasing the level of security of the authentication credentials. In addition, this often is a slow process that also results in user frustration and inefficiency. Furthermore, in establishing a new communication session, the network may require the client obtains a new network identifier, such as an internet protocol address. The applications or programs on the client may need to be restarted because of the change in the client's network identifier. Thus, it would be desirable to shield the computing devices from network disruptions.

Another inefficiency associated with direct communication between peer computing devices is that the protocol used for communications may not be as efficient or secure as desired. As an example, the network communications may include real-time data communications such as voice over IP (VoIP) communications. The real-time data communications may be communicated via an unreliable protocol such as the user datagram protocol in order to reduce latency in the telephone call. However, the VoIP communication may traverse a TCP/IP network or secure SSL gateway, which provides a reliable protocol to the VoIP communications. This may increase the latency in the telephone call that the unreliable protocol was intended to reduce. Techniques are needed for transmitting data via a lossless protocol that is intended for communication using a lossy protocol.

Another inefficiency in direct communication result from the use of encryption. Encryption, such as SSL, may be used to provide secure network communications. Although the communication is secure, the encryption of the network traffic increases the size of the network packets, which can cause the packet payload to become too large for a single packet. This can result in packet fragmentation, causing more overhead for communication processing. Techniques for adjusting the maximum size of a packet to account for encryption overhead would be useful.

Another inefficiency result from the fact that a client typically sends network communications as they are generated by the activity of the user and applications of the client, and processes incoming network communications as they are received. For example, in one case, although an application is running in the foreground and currently in active use by the user, a network packet generated or received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground. In another example, the client may be running a VoIP application to provide a telephone call to a remote computing device. One or more other applications on the client may be running that are not related to the real-time data communication of VoIP. The network packets for these applications may be processed ahead of the real-time network packets of the VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication. It is desirable to provide application-aware, client-specific prioritization of packet traffic.

Summary of the Invention

The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present invention provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. Additionally, the present invention provides various techniques for optimizing peer-to-peer communications, including real-time communications such as voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging. The present invention provides the following peer to peer optimization techniques: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access, such as for mobile computing.

In one aspect, the present invention relates to a method for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network. The first network may be disconnected from and not routable to the second network. The method includes establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device. The third computing device may be a gateway, such as an SSL VPN gateway. The first computing device initiates a communication session to the second computing device via the third computing device, such as via a signaling protocol. A server receives a signal to establish the initiated communication session, and the server communicates to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session. The first computing device communicates a request to initiate a connection with the second computing device using the first network address. The method further

includes intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The third computing device communicates a request to the second computing device to allow a connection from the first computing device using the second network address, such as via a swimmer session traversing a firewall.

In one embodiment of the present invention, the first tunneling session or the second tunneling session is established using a Secure Socket Layer or a virtual private network The third computing device may be a remote access gateway. In another embodiment, the second computing device is located behind a firewall associated with the second network address.

In another embodiment, the method of the present invention includes providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session. In an additional embodiment, the method of includes providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

In a further embodiment of the present invention, the third computing device communicates a key to the first computing device and the second computing device. The first computing device and the second computing device may exchange keys. Additionally, the first and second computing device may check that the key received from the other computing device matches before transmitting data to the other computing device.

In some embodiments of the present invention, the method associates a first telecommunication device with the first computing device, and associates a second telecommunication device with the second computing device. The first telecommunication device or the second telecommunication device may include a software component or a hardware component, such as a hard or soft VoIP telephone. In one embodiment, the method of the present invention includes establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection between the first and second computing devices. The first telecommunication device and the second telecommunication device

may communicate over the telecommunication session without traversing the third computing device.

In another embodiment of the present invention, the method communicates a remote display protocol via the connection between the first computing device and the second computing device. The remote desktop protocol may include the Independent Computing Architecture protocol or the Remote Desktop Protocol. In yet a further embodiment, the method may include sharing a screen view or screen data of the first computing device with the second computing device via the connection.

In one aspect, the present invention relates to a method performed in a gateway for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network. The first network may be disconnected from and not routable to the second network. The method includes establishing a first tunneling session with the first computing device on a first network, and establishing a second tunneling session with the second computing device on the second network. The gateway receives a request by the first computing device to initiate a communication session with the second computing device. The first computing device provides a first network address for contacting the second computing device. The first network address identifies a network address of the second computing device associated with the second tunneling session. The gateway receives a request by the first computing device to initiate a connection with the second computing device using the first network address, intercepts the request to initiate the connection, and provides the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The gateway communicates to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address, such as via a swimmer session traversing a firewall.

In one embodiment, the first tunneling session or the second tunneling session via the gateway includes a Secure Socket Layer or a virtual private network. In another embodiment, the second computing device is located behind a firewall associated with the second network address. In a further embodiment, the method of the present invention provides the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling

session. Additionally, the gateway may communicate a key to the first computing device and to the second computing device.

In another aspect, the present invention is related to a system for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device. The first network may be disconnected from and not routable to the second network. The system includes a first computing device on the first network, and a second computing device on the second network. A third computing device establishes a first tunneling session with the first computing device and a second tunneling session with the second computing device. The system also includes a server accessible via the third computing device. In operation of the system, the server communicates via the third computing device to the first computing device a first network address identifying a network address of the second computing device associated with the second tunneling session. The first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address. The third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

In one embodiment of the system, the first tunneling session or the second tunneling session includes a Secure Socket Layer or a virtual private network. Furthermore, the third computing device may be a remote access gateway, such as an SSL VPN gateway. In another embodiment of the system, the second computing device is located behind a firewall associated with the second network address.

In an additional embodiment of the present invention, the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session, such as via an out of band TLS session. In one embodiment, the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

In a further embodiment of the system of the present invention, the third computing device communicates a key to the first computing device and the second computing device. The first computing device and the second computing device may exchange keys. Additionally, the first and second computing device may check that the key received from the other computing device matches before transmitting data.

In some embodiments of the present invention, the system includes a first telecommunication device associated with the first computing device, and a second telecommunication device associated with the second computing device. The first telecommunication device or the second telecommunication device may include a software component or a hardware component, such as a hard or soft VoIP telephone. In one embodiment, the system of the present invention includes establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection between the first and second computing devices. The first telecommunication device and the second telecommunication device may communicate over the telecommunication session without traversing the third computing device.

In another embodiment of the present invention, the first computing device and the second computing device communicate a remote display protocol via the connection. The remote desktop protocol may include the Independent Computing Architecture protocol or the Remote Desktop Protocol. In yet a further embodiment, the first computing device may share a screen view or screen data with the second computing device via the connection.

In another aspect, the present invention is related to a method for communicating via a lossless protocol a packet constructed to be transmitted via a lossy protocol. The method may be performed in one or more electronic devices, such as in a system, and by any suitable means and mechanisms. The method includes establishing a connection between a first computing device and a second computing device via a lossless protocol. In some embodiments, the second computing device may be a gateway, such as an SSL VPN gateway. The first computing device detects a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol. The first computing device communicates a false acknowledgement of receipt of the lossless protocol packet to the first computing device and/or the second computing device. The false acknowledgement of receipt of the lossless protocol packet prevents

employing the reliability algorithms and mechanisms of the lossless protocol. The first computing device communicates the lossless protocol packet to the second computing device. In some embodiments, the false acknowledgement of receipt of the lossless protocol packet is communicated prior to communicating the lossless protocol packet.

In one embodiment, the method of the present invention includes encrypting, by the first computing device, the one or more packets using a key. In some embodiments, the encryption key may be provided to the first computing device via an out of band transport security layer session between the first computing device and the second computing device. In a further embodiment, the method encrypts the one or more packets on a packet by packet basis.

In another embodiment of the method of the present invention, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by the first computing device and/or the second computing, the first computing device and/or the second computing prevents executing an operation associated with providing a lossless characteristic of the lossless protocol. In one embodiment, the lossless protocol is a transport control protocol.

In a further embodiment, the method of the present invention prevents the network stack of the first computing device and/or the second computing device from executing one or more of the following in connection with the lossless protocol: 1) a retransmit, 2) an ordering, 3) a flow control algorithm, 4) a naple's algorithm, and 5) a sliding window algorithm.

In one embodiment, the lossy protocol includes a user datagram protocol. In another embodiment, the method includes communicating, by the first computing device, the
lossless protocol packet via a secure socket layer or a transport security layer tunnel to the second computing device.

In another embodiment, the one or more packets of the payload comprises a real-time protocol. In an additional embodiment, the method includes communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

In one aspect, the present invention relates to a method for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The method includes receiving, at a first device, a first packet to be transmitted using an unreliable

transport protocol, and creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device. The first device transmits the first TCP packet to the second device. The method further includes receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol, and creating a second TCP packet including a second payload of the received second packet and the first TCP header information. Before receipt of an acknowledgement of the receipt of the first payload from the second device, the first device transmits the second TCP packet to the second device.

In one embodiment, the method of the present invention establishes the TCP connection with a port number associated with the unreliable transport protocol. In another embodiment, the method includes dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol. In some embodiments, the unreliable transport protocol is UDP.

In an additional embodiment, the method includes receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism. In some embodiments, the method establishes by the first device, the TCP connection with a VPN gateway device. In other embodiments, the method includes establishing peer-to-peer communications between the first device and the second device via the TCP connection. In another embodiment of the present invention, the method includes encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

In another aspect, the present invention relates to a method for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The method includes intercepting, at a second device, a first TCP packet created on a first device and received on the second device. The first TCP packet includes a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device. The intercepting of the method occurs before the first TCP packet is provided to a TCP stack on the second device. The method includes identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable

transport protocol, stripping the TCP header of information from the first TCP packet, and forwarding the first payload to an application using the unreliable data protocol.

In one embodiment, the unreliable protocol is UDP. In another embodiment, the step of identifying comprises identifying that the TCP header information includes a port number associated with the unreliable transport protocol. In some embodiments, the method includes intercepting, by the second device, the first TCP packet using a packet capture driver.

In some embodiments, the first device is a client device and the second device is a VPN gateway. Additionally, the method of the present invention includes performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

In a further aspect, the present invention relates to a system for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The system includes a first device and a second device. The first device has an application that generates a first and second packet. The first and second packet are intended to be transmitted using an unreliable transport protocol. The first device also has a filter process and a tunneling process. The filter process intercepts the first and second packets from the application and forwards the intercepted packets to the tunnel process. The tunnel process requests the opening of a TCP connection between the first device and a second device. The request to open the TCP connection indicates to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol. The tunnel process forwards the first and second packets as payloads in a first and second TCP packet to the second device. The tunnel process sends the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet.

The second device of the system of the present invention is in communication with the first device. The second device has second filter process and tunneling process. The second tunnel process opens the TCP connection requested by the first device, and identifies and forwards the source address of the TCP connection to the second filter process. The second filter process intercepts packets from the application received at the second device with the TCP connection source address in a header. The second filter process strips the TCP header from the received packets and forwards the stripped

packets to an intended destination, and circumventing the TCP/IP stack on the second device.

In one embodiment of the system of the present invention, the filter process on the first device and/or the second filter process of the second device is a packet capture driver. In some embodiments, the first device is a client device and the second device is a VPN gateway device. In one embodiment, the unreliable data protocol is UDP.

In another embodiment, the system also includes a third device to which the stripped packets are transmitted. Additionally, the second device may further include a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to the third device.

In a further aspect, the present invention is related to a method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation. The method may be performed in one or more electronic devices, such as in a system, and by any suitable means and mechanisms. The method includes establishing a session between a first computing device and a second computing device. The session may established by an agent of the first computing device. The first computing device has a first network stack. The method detects, by the first computing device, a network packet having an encrypted payload, and determines a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload. The method alters the maximum transmission unit (MTU) parameter of the first network stack to the determined setting. As such, the reported MTU parameter is reduced to account for the encryption.

In one embodiment, the method of the present invention includes communicating the network packet via a secure socket layer or a transport layer security tunnel to the second computing device. The second computing device may be a gateway, such as an SSL VPN gateway. In another embodiment, the payload comprises a real-time protocol.

Additionally, in one embodiment, the method may further comprise altering the maximum transmission unit parameter via a network driver interface specification (NDIS) level mechanism of the first network stack In another embodiment, the method determines the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device. In one embodiment, the agent of the first computing device communicates via an IOCTL

application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

In some embodiments, the method of the present invention establishes the session between the first computing device and the second computing device via a gateway. In other embodiments, the method communicates by the first computing device real-time voice, audio, or data to the second computing device via the payload of the network packet. In yet another embodiment, the method may include communicating a false acknowledgement of receipt of the network packet to the first computing device and/or the second computing device before communicating the network packet. In one embodiment, the network packet comprises a lossless protocol packet, such as a transport control protocol. In another embodiment, the payload comprises a lossy protocol packet, such as a user datagram protocol.

In an additional aspect, the present invention is related to a method for a client to prioritize network communications of the client associated with an application of the client. The method includes intercepting, by the client, one or more network packets associated with one or more applications of the client, and storing the one or more network packets to a queue. The client determines the queued one or more network packets is associated with a first application of the client. The client indicates a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client. The client
provides the prioritized one or more network packets for communications via a network stack of the client.

In one embodiment, the method of the present invention includes determining, by the client, the queued one or more networks packets of the first application comprises real-time data. The real-time data may include one of the following: 1) a real-time protocol, 2) a user datagram protocol, and 3) a representation of voice or audio.

In another embodiment, the method includes preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application. In a further embodiment, the method includes holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon

communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

In yet another embodiment of the present invention, the method includes intercepting, by the client, the one or more network packets transparently to the one or more applications on the client. In some embodiments, the first application is running in the foreground, and the second application is running in the background.

In one embodiment of the present invention, the method includes associating a priority with the first application higher than a priority associated with the second application. In another embodiment, a user may specify the priority of the first application or the second application. In a further embodiment, the client receives the one or more network packets from a computing device. Also, the one or more applications may provide the one or more network packets for communicating from the client to a computing device.

In another aspect, the present invention is related to a client for prioritizing network communications of the client associated with an application of the client. The client includes a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client. The client also includes a network driver for storing the one or more networks packets to a queue and communicating the one or more network packets via a network stack of the client. The client further includes an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

In one embodiment, the agent of the present invention determines the one or more networks packets of the first application comprises real-time data. The real-time data comprises one of the following: 1) a real-time protocol, 2) a user datagram protocol, and a 3) representation of voice or audio.

In a further embodiment, the agent or the network driver of the present invention prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application. In one embodiment, the network driver holds in the queue a network packet associated with the second application, and releases the held network packet upon communication

of the one or more network packets associated with the first application prioritized ahead of the held network packet.

In another embodiment, the present invention, via the mechanism, intercepts the one or more network packets transparently to the one or more applications on the client. In some embodiments, the first application is running in the foreground, and the second application is running in the background. Also, the first application may have a priority higher than the second application of the client. Furthermore, the client may include a configuration mechanism for a user to specify the priority. In some embodiments, the client receives the one or more network packets from a computing device. In other embodiments, the one or more applications provides the one or more network packets for communicating from the client to a computing device.

In an additional embodiment, the network driver includes a Network Driver Interface Specification (NDIS) driver. Also, the network driver may operate in kernel-mode of an operating system of the client. In some cases, the agent operates in user-mode of an operating system of the client. Furthermore, the agent or the network driver includes the mechanism for intercepting one or more network packets of the client.

In yet another aspect, the present invention is related to a method for shielding from a network disruption a session established via a first protocol. The method includes the steps of establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device. The network connection is associated with a network stack. A first portion of the network stack has one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack includes a layer for the first protocol and one or more layers of the network stack above the first protocol. The method includes detecting a disruption in the network connection causing the second portion of the network stack to be disestablished, and maintaining, by the agent, the session and the second portion of the network stack during the disruption. The method further includes re-establishing the first portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

In one embodiment, the method includes continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

In some embodiments, the method also includes dropping, by the first and/or second portion of the network stack, any network packets received during the disruption.

In another embodiment, the device comprises a remote access gateway or another computing device. In some cases, the method includes establishing the session via the first protocol of one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. Additionally, the method of the present invention may include communicating, by the agent, real-time data via the session between the client and the device. The real-time data may include a real-time protocol or the real-time data may represent voice or audio.

In some embodiments, the agent operates in user-mode of an operating system of the client. In one embodiment, the first portion of the network comprises one of a transport control protocol or an internet protocol. In another embodiment, the second portion of the network stack comprises one of 1) an internet protocol, 2) a user datagram protocol, or 3) a voice over internet protocol. Additionally, the client may communicate with the device via a remote display protocol. The remote display protocol may be an Independent Computing Architecture (ICA) protocol or a Remote Desktop Protocol (RDP).

In another embodiment, the method of the present invention is performed transparently to an application of the client communicating via the network connection. In one embodiment, the method includes intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application. In one embodiment, the method includes intercepting, by a network driver associated with the first portion of the stack, transparently to the application on the client one or more network packets associated with the application.

In an additional aspect, the present invention is related to a system for shielding from a network disruption a session established via a first protocol. The system has an agent of a client establishing a session between the client and a device over a network connection via a first protocol. The system includes a network stack having a first portion and a second portion, such as the network stack of the client. The second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol, and a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol. The system includes a detector for detecting a disruption in the network

connection causing the first portion of the network stack to be disestablished. In operation of the system and upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption. The client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

In one embodiment of the system of the present invention, the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack. In some embodiments, the first and/or second portion of the network stack drops any network packets received during the disruption.

In one embodiment, the device of the system is a remote access gateway or another computing device The first protocol used by the system of the present invention may include one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. In another embodiment, the agent of the present invention communicates real-time data via the session between the client and the device. The real-time data may include a real-time protocol, or a representation of voice or audio.

In some embodiments of the system, the agent operates in user-mode of an operating system of the client. In one system embodiment, the first portion of the network comprises a transport control protocol and/or or an internet protocol. In another embodiment, the second portion of the network stack includes one of 1) an internet protocol, 2) a user datagram protocol, or 3) a voice over internet protocol. Additionally, the client may communicate with the device via a remote display protocol, which may be an Independent Computing Architecture (ICA) protocol or a Remote Desktop Protocol (RDP).

In another embodiment, the system of the present invention maintains the second portion of the network stack and re-establishes the first portion of the network stack transparently to an application of the client communicating via the network connection. In one embodiment, the agent intercepts network packets transparently to an application of the client one or more network packets associated with the application. In one embodiment, the system also includes intercepting, by a network driver associated with

the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

The details of various embodiments of the invention are set forth in the accompanying drawings and the description below.

Brief Description of the Drawings

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent and may be better understood by referring to the following description taken in conjunction with the accompanying drawings, in which:

Figure 1A is a block diagram depicting an embodiment for practicing the operations of the present invention via a gateway in a network environment;

Figure 1B is a block diagram depicting another embodiment for practicing the operations of the present invention in a peer-to-peer network environment;

Figure 1C is a block diagram depicting an embodiment of a remote access client of the present invention for network communications;

Figures 1D and 1E are block diagrams depicting embodiments of a computing device useful in practicing an embodiment of the present invention;

Figure 2A is a block diagram depicting an embodiment of a peer-to-peer network environment for practicing an embodiment of the technique of the present invention for establishing a peer-to-peer communication route;

Figure 2B is a flow diagram depicting an embodiment of the steps performed to optimize peer-to-peer route optimization technique of the present invention;

Figure 3A is a block diagram depicting an embodiment of network stacks of any of the computing devices of illustrative environments depicted in Figures 1A-1C;

Figure 3B is a flow diagram depicting an embodiment of the steps performed to use a false acknowledgement of receipt of network packets to communicate via a lossless protocol packets constructed for transmission via a lossy protocol;

Figure 3C is a flow diagram depicting an embodiment of the steps performed to communicate via a lossless protocol packets constructed for transmission via a lossy protocol;

Figure 4 is a flow diagram depicting one embodiment of steps performed for adjusting the maximum transmission unit parameter;

Figure 5A is a block diagram depicting an environment of a client for providing client-side application-aware prioritization techniques;

Figure 5B is a flow diagram depicting one embodiment of the steps performed to provide client-side application-aware prioritization;

Figure 6A is a block diagram depicting an environment of an apparatus for shielding a network disruption from a device; and

Figure 6B is a flow diagram depicting one embodiment of the steps performed in to shield network disruption from a device.

Description

Certain illustrative embodiments of the present invention are described below. It is, however, expressly noted that the present invention is not limited to these embodiments, but rather the intention is that additions and modifications to what is expressly described herein also are included within the scope of the invention. Moreover, it is to be understood that the features of the various embodiments described herein are not mutually exclusive and can exist in various combinations and permutations, even if such combinations or permutations are not expressly made herein, without departing from the spirit and scope of the invention.

The illustrative embodiments of the present invention are generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one illustrative embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. The present invention also provides various techniques for optimizing the peer-to-peer communications established with or without the gateway. The peer-to-peer communications may include real-time communications such as voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging. In addition to establishing a peer-to-peer connection via gateway, the present invention also provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol packets constructed for transmission via a lossy protocol, 2) payload shifting of

network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access, such as for mobile clients. These techniques may be practiced in peer-to-peer communications between two clients in some embodiments, or in other embodiments, in communications between a client and a gateway or between one computing device via a gateway to another computing device, such as via an SSL VPN gateway of an illustrative embodiment of the present invention.

In the illustrative embodiments of the present invention, the peer-to-peer route optimization technique determines a more optimal route to a resource a client may be trying to access via a gateway. The client and the resource accessed by the client, such as a server or a peer computer, may have a more direct route than via the gateway. For example, the client and the server may be located near each other but distant from the gateway, and thus, are closer to each other than via the gateway. Furthermore, using a gateway causes at least one additional hop in the end-to-end network communications between the client and the server. Instead of the client and server communicating via the gateway using their virtual private network (VPN) assigned internet protocol (IP) network addresses, the gateway and remote access architecture of the present invention facilitates the client and server communicating to each other via a direct route in a peer-to-peer fashion without using the gateway. In some cases, however, the client and server may not have a direct path between each other as either the client and/or server may be behind a firewall, such as a Network Address Translation (NAT) firewall. The peer-to-peer route optimization techniques and remote access architecture of the present invention also provide techniques for the client and server to communicate directly via traversal of the firewall. As such, the peer-to-peer route optimization techniques of the present invention provides a shorter more optimal route between peer computers than via the gateway.

In the illustrative embodiments of the present invention, the false acknowledgement technique of an embodiment of the present invention enables a packet constructed to be transmitted via a lossy protocol to be communicated via lossless protocol. For example, a real time protocol (RTP) may be implemented over a user

datagram protocol (UDP) for voice over IP (VoIP) communications. A lossy or unreliable protocol, such as UDP, may be used for voice communications because, in some real-time voice applications, it may be more important to get network packets to a recipient on time rather than getting the network packets in order or guaranteeing the delivery of network packets. However, by way of virtual private network and remote access solutions using a secure communication and/or tunneling protocol, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS), a real-time application data constructed to be transmitted via a lossy protocol, such as UDP, may be communicated via a lossless or reliable protocol such as a transport control protocol (TCP). The techniques of the present invention allow a lossy protocol, such as RTP over UDP, to be communicated via a lossless protocol such as TCP, while avoiding one or more of the lossless characteristics of the lossless protocol from being applied to the communication. In the illustrative embodiment of the present invention, this technique communicates a false acknowledgement of receipt of the lossless protocol network packet to the corresponding network stacks to prevent the lossless protocol from executing algorithms that provide for reliability of the protocol. Using this technique, the lossy protocol can be communicated over a lossless protocol, such as via TCP, SSL or via a tunneling protocol of a gateway, for example, to make the communication secure, and have the lossy protocol network packets get to the recipient on time rather than getting to the recipient reliably. In one embodiment, this technique can be used to securely communicate real-time data communications such as VoIP over SSL or TLS between peers or via a gateway.

The illustrative embodiments of the present invention also provide another technique of payload shifting that enables a packet constructed to be transmitted via a lossy protocol to be communicated via lossless protocol. A first computing device receives a first packet to be transmitted using an unreliable transport protocol, and creates a first TCP packet including a first payload of the received first packet. The first TCP packet is created with a TCP header having information associated with a TCP connection established between the first and a second computing device. The first TCP packet is transmitted to the second computing device. A second packet to be transmitted using an unreliable transport protocol is received by the first computing, which in turn creates a second TCP packet including the payload of the received second packet but with the TCP header information of the first TCP packet. The second TCP packet is

transmitted to the second computing device before receiving an acknowledgement of the receipt of the first TCP packet from the second device. As such, the payload shifting technique communicates multiple unreliable transport protocol payloads under a TCP header until an acknowledgement of receipt is received.

In the illustrative embodiments of the present invention, the maximum transmission unit adjustment technique reduces the reported size of the maximum transmission unit (MTU) parameter of a network stack of a client to take into consideration the effect of the network packet size due to encryption of a payload. Encryption of the payload of a network packet increases the size of the network packet communicated to or by the client, and may cause a network packet to be fragmented. For example, a server may communicate to the client a network packet via an SSL gateway to the client. Although the server sends a network packet that should meet the MTU size the network stack of the client can handle, the encryption provided by the gateway increases the size of the network packet before it reaches the client. This may cause the network packet communicated from the server to the client via the gateway to be fragmented as the increased packet size from encryption may be too large for the MTU size of the client. The technique of the present invention adjusts the client's reported MTU size to report a smaller size to take in account for the overhead of the encryption. This technique reduces network fragmentation or otherwise prevents non-optimal fragmentation.

In the illustrative embodiments of the present invention, the prioritization technique provides for client-side and application-aware prioritization of network communications. That is, the remote access client of the present invention manages and controls network communication prioritizations on the client. The prioritizations are based on priorities of the application on the client. The remote access client transparently intercepts network communications associated with applications executing on the client, detects the network communication is associated with an application, and determines priorities for the network communications based on a priority for the application. For example, an application on the client may be communicating real-time data communications, such as VoIP, to a peer client or via a gateway. The remote access client may intercept a network packet, and detect, for example, the network packet contains real-time data or is from a VoIP application. The remote access client may indicate a priority for this network packet such that the network packet may be

communicated ahead of non-real-time data communications or ahead of network communications from other applications. As such, the prioritization techniques of the present invention may improve or increase the performance, operational characteristics, and user experience on the client based on the applications running on the client.

In the illustrative embodiments of the present invention, the network disruption shielding technique provides a persistent and reliable connection of a client to a network, such as a peer-to-peer communication session or a connection to a gateway. For example, a mobile client, such as a laptop with a software based IP telephone, may connect to a network for VoIP communications. A temporary disruption in a network connection may occur when the mobile client roams between different access points in the same network, or when the client switches between networks (*e.g.*, from a wired network to a wireless network). This disrupts the network service to the client and may drop the VoIP telephone call. Additionally, as the mobile client moves between access points, the mobile client may obtain a different IP network address, such as from a new Dynamic Host Configuration Protocol (DHCP) lease. This can also cause network connectivity and VoIP telephone communication disruption. The techniques of the present invention detects a disruption in the network and shields a portion of the network stack from the network disruption. The shielded portion of the network stack is maintained while the other portion of the network stack is reestablished and reconnected to the network. Once the network is available, the present invention continues with the client's network communications. In some embodiments, the network communications are queued during the network disruption and transmitted once the network is available. In other embodiments, such as for real-time data communications, network packets are dropped during the disruption to prevent the queuing of network packets that may cause latency in the real-time communication, such as VoIP telephone call.

Although the illustrative embodiments of the present invention may be generally described in connection with an internet protocol (IP) based protocol, such as a transport control protocol (TCP) or user datagram protocol (UDP), the techniques of the present invention may be used in any other types of networking environments with other networking protocols, such as any Internetwork Packet Exchange (IPX) protocol based networks using a Sequenced Packet Exchange (SPX) protocol. Also, although a lossy or unreliable protocol such as UDP and a lossless or reliable protocol such as TCP may be used for illustrating an embodiment of the present invention, any lossless/reliable and

lossy/unreliable protocol as known to those ordinarily skilled in the art may be used in practicing the operations of the present invention described herein. Furthermore, although some of the illustrative embodiments of the present invention may be described below in relation to real-time data communications, such as VoIP, the techniques of the present invention may be applied for non-real-time data communications as one ordinarily skilled in the art will also recognize and appreciate.

Additionally, at times, the illustrative embodiments of the present invention may be described in regards to peer-to-peer communications. In one aspect, a peer-to-peer model comprises a type of network in which any computer can act as both a server by providing access to its resources to other computers, and can act as a client by accessing shared resources from other computers. Although in another aspect, a peer-to-peer model may not comprise a notion of a client and a server, a client and a server may provide peer-to-peer communications as well as client to client, server to server, or a client/server to a computing device such as a gateway. In an additional aspect, peer-to-peer communications comprises a process whereby computers can exchange information between each other directly without the assistance of a third party network or a device, such as a gateway. Although peer-to-peer communications may be generally described as direct communication between computers, there may be other network elements between the computing devices to facilitate the transmission and/or communication, such as for example, a network hub.

Furthermore, although the illustrative embodiments of the present invention may be described peer-to-peer, point-to-point, client to server, or otherwise, one ordinarily skilled in the art will recognize and appreciate that the present invention may be practiced between computing devices in any manner via any network topology, and that any reference to peer-to-peer, client/server, or otherwise is not intended to limit the present invention in any way.

In one aspect, the present invention is related to a remote access architecture having a remote access client for communicating to a network via a gateway or peer-to-peer to another remote access client or another computing device. The remote access architecture of the present invention provides systems and methods for securely communicating network traffic transmitted between a private network behind a gateway to a client on an external network, such as public network. The remote access architecture of the present invention enables separation of the client from the private

network by providing network address translation (NAT) functionality on the gateway. A VPN gateway that uses Network Address Translation (NAT(provides masquerading of IP addresses of a client to shield the private network from direct layer-2 access by the client.

Referring now to Figure 1A, the environment 180 depicts a system for deploying the remote access architecture in an illustrative embodiment of the present invention. In brief overview, the environment 180 includes multiple computing devices 102a-102c (herein also referred to as clients 105a-105c) connected to a network 104 via one or more network connections 341a-341n. One or more of the clients 105a-105n may connect to a server 102a, a server farm 102e, or a peer computing devices 102d via a gateway 350.

Each client 105a-105n includes a remote access client 120a-120c, which will be described in more details in connection with Figure 1C, and one or more applications 338a-338n. Each of the clients 105a-105n communicate over the network 104 to the gateway 340 via a tunneling or gateway connections 341a-341n using any type and/or form of suitable tunneling or gateway protocols. In some embodiments, the gateway connections 341a-341n may be used for communicating securely, such as via encapsulating and encryption, or otherwise may use any other protocols, such as any real-time, lossless, or lossy protocol. In other embodiments, the gateway 340 provides a virtual private network connection between one or more of the clients 105a-105n and any of the computing devices 102d-102n.

The client 105 can be any type and/or form of computing device 102 that can run one or more applications 338 that access a network, such as network 104. The application 338 can be any type and/or form of application such as any type and/or form of web browser, web-based client, client-server application, a thin-client computing client, an ActiveX control, or a Java applet, or any other type and/or form of executable instructions capable of executing on client 105 or communicating via a network 104. The application 338 can use any type of protocol and it can be, for example, an HTTP client, an FTP client, an Oscar client, or a Telnet client. In some embodiments, the application 338 uses a remote display or presentation level protocol. In one embodiment, the application 338 is an ICA client, developed by Citrix Systems, Inc. of Fort Lauderdale, Florida. In other embodiments, the application 338 includes a Remote Desktop (RDP) client, developed by Microsoft Corporation of Redmond, Washington.

In other embodiments, the application 338 comprises any type of software related to VoIP communications, such as a soft IP telephone. In further embodiments, the application 338 comprises any application related to real-time data communications, such as applications for streaming video and/or audio.

The clients 105a-105n may access any of the resources provided via computing devices 102d-102n which may be on the same network 104, or which may be on a separate network, such as a private network. In some embodiments, computing devices 102a-102n may be on a network disconnected and not routable from the network 104 of the clients 105a-105n. In one embodiment, any of the clients 105a-105n may communicate with a peer computing device 102d having a remote access client 102n and application 338d. For example, the application 338d may comprise a portion of a client/server or distributed application corresponding to any of the applications 338a-338c on clients 105a-105n. In some embodiments, any of the remote access clients 120a-120n may communicate with the remote access client 120n via the gateway 340.

In another embodiment, any of the clients 105a may communicate via the gateway 340 to a server 102e running an application 338e, which for example, may be an application server providing email services such as Microsoft Exchange manufactured by the Microsoft Corporation of Redmond, Washington, a web or Internet server, or a desktop sharing server, or a collaboration server. In some embodiments, any of the application 338e may comprise any type of hosted service, such as GoToMeeting.com provided by Citrix Systems, Inc. of Ft. Lauderdale, Florida, WebEx.com provided by WebEx, Inc. of Santa Clara, California, or LiveMeeting.com provided by Microsoft Corporation of Redmond, Washington.

In another embodiment, any of the clients 105a may communicate via the gateway 340 to a server farm 102n or server network, which is a logical group of one or more servers that are administered as a single entity. The server farm 102n may be running one or more applications 338N, such as an application 338f providing a thin-client computing or remote display presentation application. In one embodiment, the server 102e or server farm 102n executes as an application 338e-338n, any portion of the Citrix Access Suite™ by Citrix Systems, Inc., such as the MetaFrame or Citrix Presentation Server™, and/or any of the Microsoft Windows Terminal Services manufactured by the Microsoft Corporation.

Still referring to Figure 1A, the gateway 340 may comprise any type and/or form of gateway, such as a remote access server, that may be used to connect one or more computing devices on one network to other networks. In another aspect, the gateway 340 may be used to provide a virtual private network connection to give a client 105a-105c access to a private network. In a further aspect, the gateway 340 may be a hardware or software set-up that translates between two dissimilar protocols or disjoint or disconnected networks or systems. The gateway 340 may comprise a specialized hardware or networking device, or may be a computing device configured to act as a gateway. As such, the gateway 340 may comprise software, hardware, or any combination of software and hardware. In one embodiment, the client 105 and the gateway 340 communicate via any type and/or form of gateway or tunneling protocol 341a-341n, such as SSL or TLS, or the Citrix Gateway Protocol manufactured by Citrix Systems, Inc. of Ft. Lauderdale, Florida.

In some embodiments, the gateway 340 may decrypt encrypted packets received from a client 105a-105c, and may encrypt packets communicated to a client 105a-105n. The gateway 340 may be used to protect a private network, such as network 104. In some embodiments, the gateway 340 associates a client 105a-105c with a private IP address or an IP address of the private network. In one of these embodiments, when the gateway 340 receives a packet from the client 105a-105c, the gateway 340 transforms the IP address of the packet to the IP address associated with the client 105a-105c for the private network. In some embodiments, the gateway 340 may apply access control policies to network traffic to and/or from a client 105a-105c. For example, access controls policies may be applied to a packet received from the client prior to routing the packet to a final destination.

In one embodiment of the gateway 340, once a frame enters the gateway 340 via an SSL tunnel, the packet and its payload are dispatched via callbacks into a handlers executing in user mode, which provide functionality for SSL decryption. In another embodiment, openSSL may be used. In other embodiments, a hardware accelerator is used. In a further embodiment, the gateway 340 comprises one or more blades for providing remote access. Once the packet is decrypted, it is injected into an HTTP network stack where headers are assembled and passed on to the remote access blade. In a remote access blade, a packet is classified by the type of data contained within the packet. In one embodiment, the packet contains an HTTP header requesting login and

registration. In another embodiment, the packet seeks TCP/UDP/RAW/OTHER connection establishment. In still another embodiment, the packet contains connection-specific data. In yet another embodiment, the packet contains a special feature request such as collaboration with other users, fetching of user directory and presence or requesting telephony functionality such as conferencing and web cast. The remote access module dispatches the packet appropriately to the corresponding sub handler. For example, the client 105 may request that a connection be set up to a specific machine on the private network behind the gateway 340. The remote access module may consult with the access control module and if a positive response is returned, the remote access module may grant the request. In some embodiments, the remote access module 120 may grant the request by injecting subsequent frames on the private network using a frame forwarding module utilizing NAT/PAT to correlate incoming frames to corresponding SSL tunnels 341a-341n to a client 105a-105c.

The network 104 as illustrated in Figure 1A can be any type of network. The network 104 can be a local-area network (LAN), such as a company Intranet, a metropolitan area network (MAN), or a wide area network (WAN), such as the Internet or the World Wide Web. The topology of the network 104 may be a bus, star, or ring network topology. The network 104 and network topology may be of any such network or network topology capable of supporting the operations of the present invention described herein. The client 108 and gateway 340 can connect to one or more networks 104 through a variety of connections including standard telephone lines, LAN or WAN links (e.g., T1, T3, 56 kb, X.25, SNA, DECNET), broadband connections (ISDN, Frame Relay, ATM, Gigabit Ethernet, Ethernet-over-SONET), and wireless connections or any combination thereof. Connections can be established using a variety of communication protocols (e.g., TCP/IP, IPX, SPX, NetBIOS, Ethernet, ARCNET, Fiber Distributed Data Interface (FDDI), RS232, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and direct asynchronous connections).

In one embodiment of the present invention, the gateway 340 illustrated in Figure 1A is used to facilitate a direct peer-to-peer connection between computing devices 102a-102n. For example, client 105a may establish a tunneling session with the gateway 340 to access the peer computing device 102d. The gateway 340 negotiates with the remote access client 120a of client 105a and the remote access client 120n of computing device 102d to enable the client 105a to directly connect to the computing

device 102d without traversing the gateway 340. Once the network connection between the client 105a and computing device 102d is established, the client 105a can communicate in a peer-to-peer manner with computing device 102d. The gateway 340 of the present invention can facilitate a direct peer-to-peer connection between any of the computing devices 102a-102n illustrated in the environment 180. In one embodiment, the gateway 340 can facilitate a peer-to-peer connection between any of the clients 105a-105n, for example between client 105a and client 105b or between client 105b and client 105c. In another embodiment, the gateway 340 facilitates a peer-to-peer connection between computing devices 102d-120n, for example, between computing device 102d and server 102e or server farm 102n. In other embodiments, the gateway 340 facilitates a peer-to-peer connection between one of the clients 105a-105n and one of the computing devices 102d-102n. The techniques of facilitating a peer-to-peer connection via the gateway 340 will be discussed in more detail below in conjunction with Figures 2A and 2B.

Referring now to Figure 1B, the remote access client 120 of the present invention may be used in an illustrative embodiment of a peer-to-peer connection without a gateway 304. For example, the gateway 340 may facilitate a peer-to-peer connection between any of the computing device 102a-102n illustrated in Figure 1, and thereafter the computing devices 102a-102n communicate directly to each other in a peer-to-peer manner. In other embodiments, any computing device 102a may communicate directly to another computing device 102b or 102c via a network 104 without a gateway 340 facilitating the connection.

In brief overview of Figure 1B, the remote access client 120a may be deployed on a client 102a running one or more application 338a. The computing device 102a may connect over the network 104 to computing device 102b and/or computing device 102c. Computing device 102b may be a peer or client computing device also comprising a remote access client 120b. In some embodiments, remote access client 120a and 120b may communicate with each other via network 104, and may work in conjunction with each other for application 338a to communicate to application 338b, such as for a web-based or client/server application. In other embodiments, the remote access client 120a may communicate with computing device 120c which may be a server that does not execute a remote access client 120.

Figure 1C depicts a block diagram illustrating a system having a remote access client 120 for routing network packets from a client 105 to a network 104. In brief overview, the system includes a computing device102 (herein also referred to as a client 105) having an operating system that includes a user mode 332, also referred to as an application or user space, and a kernel-mode 334, which may be also referred to as the kernel or system level space. The client 105 runs an agent 326 that in one embodiment, may run in user-mode 332. The client 105 also runs a filter 322, which may, in one embodiment, execute in kernel-mode or the kernel space 334. In one embodiment, the filter 322 and the agent 326 form the remote access client 120 for routing packets via a network, or for otherwise providing remote access connectivity in accordance with the operations of the present invention described herein. The remote access client 120, or any portion thereof, such as the agent 326 or the filter 322, may execute in user-mode 332 or kernel-mode 334.

The client 105 may also have a network stack 310, which may comprise one or more network layers, such as any networks layers of the Open Systems Interconnection (OSI) communications model as those skilled in the art will recognize and appreciate. The network stack 310 may comprise one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol, such as IEEE 802.11, as those skilled in the art will recognize and appreciate. Furthermore, the network stack 310 may include one or more network drivers supporting the one or more layers, such as a TCP driver or a network layer driver. The network drivers may be included as part of the operating system of the computing device 102 or as part of any network interface cards or other network access components of the computing device 102. Additionally, any of the network drivers of the network stack 310 may be customized, modified or adapted to provide a custom or modified portion of the network stack 310 in support of any of the techniques of the present invention described herein. Additionally, some portions of the network stack 310 may operate in kernel-mode 334 while other portions run in user-mode 332, such as an application layer of the network stack 310.

The filter 322 may include a packet capturing mechanism 365, and the filter 322 and/or packet capturing mechanism 365 may comprise a network driver, such as a network driver operating at any layer, or portion thereof, of a network stack 310 of the client 105. The filter 322 and/or the packet capture mechanism 365 may comprise a driver complying with the Network Driver Interface Specification (NDIS), or a NDIS

driver. In another embodiment, the filter 322 and/or the packet capture mechanism 365 may comprise a min-filter or a mini-port driver. The packet capture mechanism 365 may also in some embodiments operate in kernel mode 334. Although the packet capture mechanism 365 is illustrated as part of the filter 322, the packet capture mechanism 365 may be separate from the filter 322. Additionally, the filter 322 and the packet capture mechanism 365 may operate at different layers, or portions thereof, of a network stack of the client 105.

The filter 322 may use a filter table for filtering packets. The filtering table is used to determine what action to take against packets, such as packets intercepted by the packet capture mechanism 365. The filter 322 can inspect the contents of the packets, such as routing information, to determine the action to take based on the filtering table. In some embodiments, the filter 322 may drop or accept the network packets depending on their content. In other embodiments, the filter 322 may route the network packets to the agent 326 based on the packets content and/or the filtering table. The filter table may also be used to ensure that unwanted packets are discarded. The filter 322 may be used to deny access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses.

In some embodiments, the filtering table includes information about a private network. In other embodiments, a filter 322 on a client computing device 102 receives the filtering table. In one of these embodiments, the filter 322 receives the filtering table from an application 338 or an agent 326 on the computing device 102. In another of these embodiments, the filter 322 receives configuration settings from the agent 326 and stores the configuration settings in a filtering table.

The packet capture mechanism 365 may intercept any of the network traffic of the client 105, such as network packets associated with the application 338. In some embodiments, the packet capture mechanism 365 intercepts network traffic transparently to the application 338, the agent 326, the gateway 340, or to any portion of the network stack 310 of the client 105, such as any other driver or layer operating at a layer above or below the layer the packet capture mechanism 365 operates. In this manner, the present invention can be used with and support any of the techniques described herein and for any application and any protocol used by the application. In one embodiment, the packet capture mechanism 365 intercepts outbound packet traffic, such as any network traffic communicated via network 104 and/or gateway 340. The packet capture

mechanism 365 may forward the packets to the agent 325 or a frame monitor mechanism 360 of the agent 326. In some embodiments, the filter 322 communicates with the agent 326 via asynchronous I/O control messages. In one of these embodiments, the packet capture mechanism 365 may forward packets addressed to a private network behind a gateway 340 via asynchronous I/O control messages. In other embodiments, the filter 322 communicates with the agent 326 running in the user space 334 via UDP packets. In one embodiment, the filter 322 receives configuration settings from the agent 326 driver via asynchronous I/O control messages. The configuration settings may include information regarding which networks, protocols, or types of packets to filter. In one embodiment, the filter 322 stores the configuration settings in a filtering table. In another embodiment, the filter 322 receives a filtering table including the configuration settings.

In one embodiment, the filter 322 intercepts all outbound packets of the client 105 for inspection. For example, in some embodiments, the filter intercepts a packet generated by an application 338 executing in user-mode 332 for transmission by the client 105. If the packet satisfies a condition listed in the filtering table, the filter 322 may transmit the packet to the agent 326 and not to the original destination of the packet. The filter 322 may use an asynchronous I/O control message to forward the packet to the agent 326. The filter 322 may transmit the packet to the agent 326 in accordance with or responsive to a routing table .

In some embodiments, the agent 326 and the filter 322 communicate via an IOCTL application programming interface (API), such as any IOCTL libraries and function calls provided by the Microsoft Windows family of operating systems. In other embodiments, the IOCTL based interface between the agent 326 and the filter 322 may be provided by any portion of the operating system running on the client 105. Although discussed in terms of I/O control message and the IOCTL interface, the agent 326 and the filter 322 may communicate via any suitable mechanism and/or means.

The kernel 334 of client 105 may include an NDIS interface. In some embodiments, the NDIS interface includes a plurality of intermediate filters. In one embodiment, a packet passes through the NDIS interface and may be inspected by the plurality of intermediate filters. Although the filter 322 may be provided as an NDIS driver, the filter 322 may also be a process or other set or type of executable instructions executing in the kernel 334.

The agent 326 of the present invention may execute in the application space 332 or user-mode on the client 105. In other embodiments, the agent 326 operates in kernel-mode 334. In some embodiments, the agent 326 provides functionality for receiving packets from the filter 322. In other embodiments, the agent 326 provides functionality for applying a policy to a received packet. In still other embodiments, the agent 326 provides functionality for managing an SSL tunnel to the gateway 340. In yet other embodiments, the agent 326 provides functionality for encrypting and transmitting a packet to the gateway 340. The agent 326 may include frame monitor mechanism 360. The frame monitor 360 may include policies and logic for applying a policy to a received packet. The agent 326 may transmit a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360.

In some embodiments, the frame monitor 360 may apply a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet. In other embodiments, the frame monitor 360 may identify an application 338 that generated the packet. In some of these embodiments, the frame monitor 360 may make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application 338. In another embodiment, the frame monitor 360 may perform a checksum on the packet to verify that the identified application actually generated the packet.

In other embodiments, the packet capture mechanism 365 may be included in the agent 326 instead of or in addition to the filter 322. As such, the agent 326 may intercept network traffic. The packet capture mechanism 365 may use any hooking application programming interface (API) to intercept, hook, or otherwise obtain inbound and/or outbound packets of the client 105, such as the network traffic associated with application 338.

In one embodiment, a TCP connection is initiated by an application 338 executing on the client 105 for transmission of IP packets to a target computing device, such as computing device 102c of Figure 1B or the gateway 340 in Figure 1A. The remote access client 120 may intercept or capture the IP packets generated by the application 338. The remote access client 120 may send a TCP acknowledgement packet to the application 338 and terminate the TCP connection initiated by the application 338. Then, the remote access client 120 creates a second TCP connection to the second computing device 102c or the gateway 340 and transmits the captured IP

packets via the second TCP connection. In some embodiments, the remote access client 120 may store a captured IP packet in a buffer. In these embodiments, the remote access client 120 may transmit the buffered IP packets via the second TCP connection to the second computing device 102c. Storing the captured IP packets in a buffer enables preservation of the packets in the event of a disruption in the network connection.

In one embodiment, upon receipt of the captured IP packets, the gateway 340 may create a third TCP connection between the gateway 340 and the targeted computing device 102d, such as in Figure 1A. The gateway 340 may maintain a port-mapped Network Address Translation (NAT) table, enabling the gateway 340 to transmit response packets from the target computing device 102d to the port monitored by the application 338 that originally generated the IP packet on the client 105. Because the client 105 communicates only with a public network address of the gateway 3400, the client 105 is unaware of the network address of the target computing device 102d, increasing security to the network on which the target computing device 102d resides. Similarly, since the gateway 340 originates the TCP connection to the target computing device 102d, the target computing device 102d does not receive the address information of the client 105, protecting the client 105 and the network on which it resides. Additionally, since the gateway 340 receives the IP packets, the gateway 340 may make a determination responsive to a policy or security check as to whether or not to transmit the IP packets to the target computing device 102d, further increasing protection to the network on which the target computing device 102d resides.

In one embodiment, the present invention provides a method for securing a packet transmitted from a private, secured network behind a gateway 340 to a client 105 on an external network 104. The invention enables separation of the client 105 from the private network by providing network address translation (NAT) functionality on the gateway 340. A VPN gateway that uses NAT provides masquerading of IP addresses of a client 105 to shield the private network from direct layer-2 access by the client 105.

In one aspect, any portion of the remote access client 120, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365, or any portion thereof may comprise software, hardware, such as an ASIC or an FPGA, or any

combination of software and/or hardware. In some embodiments, portions of the remote access client 120 may be provided via one or more blades on the client 105.

Although the remote access client 120 is illustrated with multiple components, such as an agent 326 and a filter 322, one ordinarily skilled in the art will recognize and appreciate that the operations and functionality of the remote access client 120 described herein may be practiced in a single mechanism or single component. For example, in some embodiments, the operations and functionality of the remote access client 120 may be included within an application 338. In one embodiment for example, the functionality and operations of the remote access client 120 may be provided just as an agent 326, and in another embodiment, just as a network driver, such as the filter 322.

In some embodiments, the remote access client 120, or any portion thereof, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365 may comprise an application, module, service, computer program, software component, web service, web component, library, function, process, task, thread, or any other type and/or form of executable instruction which is designed to and capable of executing the functionality of the present invention as described herein, and which may operate in any portion or combination of user-mode 332 and/or kernel-mode 334.

As illustrated in Figures 1A-1C, the remote access client 120 of the present invention may be deployed and used in a variety of ways to communicate and provided remote access over a network to other computing devices, such as via a gateway 340 or directly between peer computing devices. In these variety of environments, the remote access client 120 may be used to practice one or more of the optimization techniques of the present invention as described in more detail below. For example, the remote access client 120 may be used for optimizing any real-time data communications, such as VoIP, desktop sharing, or web conferencing in any of the illustrative environments of Figures 1A-1C.

In the illustrative embodiments of Figures 1A-1C, the computing devices 102a-120n, such as for any of the clients 105, server, or the gateway 340, may be provided as any type and/or form of computing device such as a personal computer or computer server of the sort manufactured by the Hewlett-Packard Corporation of Palo Alto, California or the Dell Corporation of Round Rock, TX. Figures 1D and 1E depict block diagrams of a computing device 102 useful for practicing an embodiment of the present invention. As shown in Figures 1D and 1E, each computing device 102 includes a

central processing unit 102, and a main memory unit 104. As shown in Figure 1D, a typical computing device 102 may include a visual display device 124, a keyboard 126 and/or a pointing device 127, such as a mouse. Each computing device 102 may also include additional optional elements, such as one or more input/output devices 130a-130b (generally referred to using reference numeral 130), and a cache memory 140 in communication with the central processing unit 102.

The central processing unit 102 is any logic circuitry that responds to and processes instructions fetched from the main memory unit 104. In many embodiments, the central processing unit is provided by a microprocessor unit, such as: the 8088, the 80286, the 80386, the 80486, the Pentium, Pentium Pro, the Pentium II, the Celeron, or the Xeon processor, all of which are manufactured by Intel Corporation of Mountain View, California; the 68000, the 68010, the 68020, the 68030, the 68040, the PowerPC 601, the PowerPC604, the PowerPC604e, the MPC603e, the MPC603ei, the MPC603ev, the MPC603r, the MPC603p, the MPC740, the MPC745, the MPC750, the MPC755, the MPC7400, the MPC7410, the MPC7441, the MPC7445, the MPC7447, the MPC7450, the MPC7451, the MPC7455, or the MPC7457 processor, all of which are manufactured by Motorola Corporation of Schaumburg, Illinois; the Crusoe TM5800, the Crusoe TM5600, the Crusoe TM5500, the Crusoe TM5400, the Efficeon TM8600, the Efficeon TM8300, or the Efficeon TM8620 processor, manufactured by Transmeta Corporation of Santa Clara, California; the RS/6000 processor, the RS64, the RS 64 II, the P2SC, the POWER3, the RS64 III, the POWER3-II, the RS 64 IV, the POWER4, the POWER4+, the POWER5, or the POWER6 processor, all of which are manufactured by International Business Machines of White Plains, New York; or the AMD Opteron, the AMD Athlon 64 FX, the AMD Athlon, or the AMD Duron processor, manufactured by Advanced Micro Devices of Sunnyvale, California. The computing device 102 may be based on any of the above described processors, or any other processor capable of operating as described herein.

Main memory unit 104 may be one or more memory chips capable of storing data and allowing any storage location to be directly accessed by the microprocessor 100, such as Static random access memory (SRAM), Burst SRAM or SynchBurst SRAM (BSRAM), Dynamic random access memory (DRAM), Fast Page Mode DRAM (FPM DRAM), Enhanced DRAM (EDRAM), Extended Data Output RAM (EDO RAM), Extended Data Output DRAM (EDO DRAM), Burst Extended Data Output

DRAM (BEDO DRAM), Enhanced DRAM (EDRAM), synchronous DRAM (SDRAM), JEDEC SRAM, PC100 SDRAM, Double Data Rate SDRAM (DDR SDRAM), Enhanced SDRAM (ESDRAM), SyncLink DRAM (SLDRAM), Direct Rambus DRAM (DRDRAM), or Ferroelectric RAM (FRAM). The main memory 104 may be based on any of the above described memory chips, or any other available memory chips capable of operating as described herein. In the embodiment shown in Figure 1E, the processor 100 communicates with main memory 104 via a system bus 150 (described in more detail below). Figure 1E depicts an embodiment of a computing device 102 in which the processor communicates directly with main memory 104 via a memory port 103. For example, in Figure 1E the main memory 104 may be DRDRAM.

Figures 1D and 1E depict embodiments in which the main processor 100 communicates directly with cache memory 140 via a secondary bus, sometimes referred to as a backside bus. In other embodiments, the main processor 100 communicates with cache memory 140 using the system bus 150. Cache memory 140 typically has a faster response time than main memory 104 and is typically provided by SRAM, BSRAM, or EDRAM.

In the embodiment shown in Figure 1D, the processor 100 communicates with various I/O devices 130 via a local system bus 150. Various busses may be used to connect the central processing unit 102 to any of the I/O devices 130, including a VESA VL bus, an ISA bus, an EISA bus, a MicroChannel Architecture (MCA) bus, a PCI bus, a PCI-X bus, a PCI-Express bus, or a NuBus. For embodiments in which the I/O device is a video display 124, the processor 100 may use an Advanced Graphics Port (AGP) to communicate with the display 124. Figure 1E depicts an embodiment of a computer 102 in which the main processor 100 communicates directly with I/O device 130b via HyperTransport, Rapid I/O, or InfiniBand. Figure 1E also depicts an embodiment in which local busses and direct communication are mixed: the processor 100 communicates with I/O device 130a using a local interconnect bus while communicating with I/O device 130b directly.

The computing device 102 may support any suitable installation device 116, such as a floppy disk drive for receiving floppy disks such as 3.5-inch, 5.25-inch disks or ZIP disks, a CD-ROM drive, a CD-R/RW drive, a DVD-ROM drive, tape drives of various formats, USB device, hard-drive or any other device suitable for installing software and programs such as the remote access client software 120 related to the present invention.

The computing device 102 may further comprise a storage device 128, such as one or more hard disk drives or redundant arrays of independent disks, for storing an operating system and other related software, and for storing application software programs such as any program related to the remote access client 120 of the present invention. Optionally, any of the installation devices 118 could also be used as the storage device 128. Additionally, the operating system and the proxy software 120 can be run from a bootable medium, for example, a bootable CD, such as KNOPPIX®, a bootable CD for GNU/Linux that is available as a GNU/Linux distribution from knoppix.net.

Furthermore, the computing device 102 may include a network interface 118 to interface to a Local Area Network (LAN), Wide Area Network (WAN) or the Internet through a variety of connections including, but not limited to, standard telephone lines, LAN or WAN links (*e.g.*, 802.11, T1, T3, 56kb, X.25), broadband connections (*e.g.*, ISDN, Frame Relay, ATM), wireless connections, or some combination of any or all of the above. The network interface 118 may comprise a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the computing device 102 to any type of network capable of communication and performing the operations described herein.

A wide variety of I/O devices 130a-130n may be present in the computing device 102. Input devices include keyboards, mice, trackpads, trackballs, microphones, and drawing tablets. Output devices include video displays, speakers, inkjet printers, laser printers, and dye-sublimation printers. The I/O devices may be controlled by an I/O controller 123 as shown in Figure 1D. The I/O controller may control one or more I/O devices such as a keyboard 126 and a pointing device 127, e.g., a mouse or optical pen. Furthermore, an I/O device may also provide storage 128 and/or an installation medium 118 for the computing device 102. In still other embodiments, the computing device 102 may provide USB connections to receive handheld USB storage devices such as the USB Flash Drive line of devices manufactured by Twintech Industry, Inc. of Los Alamitos, California.

In further embodiments, an I/O device 130 may be a bridge 170 between the system bus 150 and an external communication bus, such as a USB bus, an Apple Desktop Bus, an RS-232 serial connection, a SCSI bus, a FireWire bus, a FireWire 800

bus, an Ethernet bus, an AppleTalk bus, a Gigabit Ethernet bus, an Asynchronous Transfer Mode bus, a HIPPI bus, a Super HIPPI bus, a SerialPlus bus, a SCI/LAMP bus, a FibreChannel bus, or a Serial Attached small computer system interface bus.

A computing device 102 of the sort depicted in Figures 1D and 1E typically operate under the control of operating systems, which control scheduling of tasks and access to system resources. The computing device 102 can be running any operating system such as any of the versions of the Microsoft® Windows operating systems, the different releases of the Unix and Linux operating systems, any version of the MacOS® for Macintosh computers, any embedded operating system, any real-time operating system, any open source operating system, any proprietary operating system, any operating systems for mobile computing devices, or any other operating system capable of running on the computing device and performing the operations described herein. Typical operating systems include: WINDOWS 3.x, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS NT 3.51, WINDOWS NT 4.0, WINDOWS CE, and WINDOWS XP, all of which are manufactured by Microsoft Corporation of Redmond, Washington; MacOS, manufactured by Apple Computer of Cupertino, California; OS/2, manufactured by International Business Machines of Armonk, New York; and Linux, a freely-available operating system distributed by Caldera Corp. of Salt Lake City, Utah, Java or Unix, among others.

In other embodiments, the computing device 102 may have different processors, operating systems, and input devices consistent with the device. For example, in one embodiment the computer 102 is a Zire 71 personal digital assistant manufactured by Palm, Inc. In this embodiment, the Zire 71 operated under the control of the PalmOS operating system and includes a stylus input device as well as a five-way navigator device.

Moreover, the computing device 102 can be any workstation, desktop computer, laptop or notebook computer, server, handheld computer, mobile telephone, any other computer, or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described herein.

In one aspect, the present invention is related to providing various techniques for optimizing communications between computing devices, such as depicted in any of the illustrative environments Figures 1A-1C. The present invention provides the following

techniques, which may be practiced stand-alone or in any combination: 1) peer-to-peer route optimization, 2) communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reducing network fragmentation by adjusting maximum transmission unit (MTU) adjustment to account for encryption, 4) client-side application-aware network communication prioritization, and 5) shielding a device from network disruption. The peer-to-peer route optimization technique will be discussed in conjunction with Figures 2A and 2B, techniques for communications via a lossless protocol of packets constructed for transmission via a lossy protocol are discussed in conjunction with Figures 3A and 3B, the MTU adjustment technique in conjunction with Figure 4, the client-side application-aware prioritization technique in conjunction with Figures 5A and 5B, and the network disruption shielding in conjunction with Figures 6A and 6B.

In one aspect, the present invention is related to providing a peer-to-peer route optimization technique between a first computing device accessing a second computing device via a gateway, such as the gateway 340 illustrated in Figure 1A. The peer-to-peer routing techniques provides a more optimal and direct communication between computing devices establishing or attempting to establish a communication session via a gateway. The illustrative method 260 of an embodiment of the present invention will be discussed in view of the illustrative environment 200 of Figure 2A. In brief overview, the environment 200 includes a gateway 340 providing remote access connectivity to a private network, such as a network with IP address ranges 10.10.10.XXX. The gateway 340 in association with the private network may have assigned an IP address of 10.10.10.2 for communications on the private network. This private network may include a server 102c. Also, the private network comprises a telecommunication device 210c, such as any type and/or form of VoIP telephone. The telecommunication device 210c is assigned IP address 10.10.10.100 on the private network.

In one embodiment, the server 102 comprises a signaling server, which may provide any type and/or form of signaling services for establishing a communication session between computing devices, such as a first computing device 102a and a second computing device 102b. In one embodiment, the server 102c supports a Session Initiation Protocol, SIP, which is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. In one embodiment, SIP works in the

application layer of the Open Systems Interconnection (OSI) communications model. In some embodiments, the first computing device 102a initiates a session via signaling, such as via the SIP protocol, to the signaling server 102c via signaling path 220. In one embodiment, the signaling server 102c in conjunction with the gateway 340 is used for establishing a media path 225 between the first computing device 102a and the second computing device 102b, such as for a VoIP telecommunication session between telephones 210a and 210b.

The first computing device 102a of environment 200 may be part of a network, private or public, accessing the gateway 340 via network 104 over the connection 341a and traversing the firewall 205a. The firewall 205a provides access to and traversal of a public network, and has assigned the IP address of 24.24.24.100. The first computing device 102a may be in communication with, or interfaced or coupled to a telecommunication device 210a, such as a VoIP communication device, or any other real-time data communication device. The second computing device 102b may be part of a private network and have assigned the IP address of 192.168.20.20. Additionally, the second computing device 102b may include a software based telecommunication device 210b, such as software-based VoIP telecommunication device or program. The second computing device 102b may access the gateway 340 via network 104 over connection 341b and traversing firewall 205b having a public network IP address of 216.216.10.10. The firewalls 205a and 205b may be any type and/or form of firewall as known to those ordinarily skilled in the art, such as a NAT firewall.

The first computing device 102a and second computing device 102b of Figure 2A includes and uses the remote access client 120 of the present invention to provide an ad-hoc peer-to-peer virtual network connectivity in the environment 200. In addition to maintaining a tunnel and virtual private connection, such as an SSL VPN connection, to the gateway 340, the remote access client 120 of the present invention also has logic, functionality, and operations to establish a direct ad-hoc connection, such as an SSL VPN connection, to a peer it is trying to reach. In view of Figure 2A, the illustrative method 260 of Figure 2B will be used to discuss how a peer-to-peer secure communication session is established for the media path 225 in one illustrative embodiment of the present invention. The peer-to-peer routing technique of the present invention as illustrated by method 260 provides better voice quality and reduces latency related to VoIP communications as well as other real-time data communications.

In brief overview of illustrative method 260, at step 262, the computing devices 102a and 102b establish tunneling sessions with the gateway 340. At step 264, the first computing device 102a initiates a session to second computing device 102b via gateway 340 using signaling protocol via the signaling path 220 to signaling server 102b. The session may be initiated by the telecommunication device 102a in communication with the first computing device 102a. At step 266, a signaling server 102c sets up the telecommunication session, and at step 268, provides the first computing device 102a with a first network identifier of the second computing device 102b. The first network identifier comprises the network address, such as a host name or IP address, of the second computing device 102b based on its IP address established via the tunnel 341b with the gateway 340. At step 270, the first computing device 102a communicates to the second computing device 102b using the first network identifier to establish a connection or communication session.

In further overview, at step 272, the gateway 340 intercepts the communications by the first computing device 102a and provides the first computing device 102a a second network identifier for the second computing device 102b. The second network identifier comprises an IP address or host name of the second computing device 102a directly or publicly accessible by the first computing device 102a, such as the last known public IP address of the second computing device 102b. At step 274, in one embodiment, the gateway 340 communicates to the second computing device 102b to request the second computing device 102b establish a swimmer session for first computing device 102a to connect to the second computing device 102b via firewall 205b. In some embodiments, the gateway 340, at step 276, may negotiate or otherwise provide encryptions keys for the first computing device 102a and second computing device 102b. At step 278, the first computing device 102a establishes a direct connection, communication session, or media path 225 to the second computing device 102b. In other embodiments, at step 280, the first computing device 102a and/or second computing device 102b match encryption keys received by the other computing device before allowing communications.

In some embodiments of illustrative step 262, the computing device 102a and 102b may establish a connection with the gateway 340 by any suitable means and/or mechanisms, such as by any type and/or form of tunneling or gateway protocol. In some embodiments, the connections 341a and 341b to the gateway 340 may form a virtual

private network connection, and in other embodiments, may use SSL or TLS to provide secure communications to the private network, such as the private network identified by the IP range 10.10.10.XXX in illustrative Figure 2A. In one embodiment, the computing devices 102a and 102b connect to the gateway 340 by traversing a firewall 205a-205b via a public network, while, in other embodiments, the computing devices 102a and 102b may connect to the gateway 340 via a private network, and may not traverse a firewall 205a-205b. One ordinarily skilled in the art will recognize and appreciate the variety of ways the computing devices 102a-102b may connect to and communicate with the gateway 340.

At illustrative step 264, in one embodiment, the telecommunication device 210a, such as a hard IP phone, initiates a telecommunication session, such as a telephone call, to the telecommunication device 210b, such as a soft IP phone. In some embodiments, the telecommunication device 210a initiates the telephone call by indicating the extension of the telecommunication device 210b. When the telecommunication device 210a initiates the telecommunication session, this initiation, indication, or request to establish a telecommunication session or media session may be sent to the signaling server 102a via SIP protocol, a proprietary signaling protocol, or any other type of protocol suitable for signaling. The signals are communicated via signaling path 220 via the tunneling session 341a to the gateway 230 and reach the signaling server 102c via the intranet routes of the private network behind the gateway 340.

Although the illustrative embodiment of method 260 is discussed in view of VoIP or telecommunication signaling and sessions, one ordinarily skilled in the art will recognize and appreciate that the present invention may be used for initiating any type and/or form of communication session, real-time or otherwise, such as an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. As such, the telecommunication devices 210a-210b, signaling/signal path 220, and signaling server 120a may accordingly and suitably comprise the type and/or form of device, signaling, protocols, and communications corresponding to the type and/or form of communication session.

In some embodiments of illustrative step 266, the signal server 102c may set up, negotiate, or establish any type and/or form of communication session, and in one embodiment the signaling server 102c sets up a telecommunication session, such as the VoIP telephone call initiated by the telecommunication device 210a. When setting up

the telecommunication or other media session, the signaling server 102c, at step 270, instructs, requests, signals or otherwise communicates to the initiating telecommunication device 210a and/or first computing device 102a to contact, signal, connect, or otherwise communicate to the peer telecommunication device 210b via a certain network address. In some embodiments, the network address provided by the signaling server 102c to the initiating telecommunication device 210a comprises the network address for the computing device 102b on the private network, i.e., 10.10.10.XXX, behind the gateway 340. In one embodiment, the network address for the peer telecommunication device 210b may comprise an enterprise private network address.

At this point, instead of contacting the peer telecommunication device 210b via its VPN private IP address, the illustrative method of 260, via the remote access client 120 facilities the telecommunication device 210a and/or the first computing device 102a to directly contact the peer or target telecommunication device 210b or the second computing device 102b. The techniques of the present invention is not specific to any VoIP protocol, and may be applied to any other protocols, such as any peer-to-peer protocol between computing devices. The techniques of the present invention makes decisions by way of the IP address of the resource a client is trying to connect with.

At step 270, when the telecommunication device 210a initiates a data connection to the telecommunication device 210b with the first network address provided by the signaling server 120c at step 268, such as the VPN private IP address of the soft IP phone, the gateway 340 intercepts the communication to provide the telecommunication device 210 and/or first computing device 102b with a second network address for contacting the telecommunication device 210b. In one embodiment, the gateway 340 intervenes and sends an out of band signal over the same established VPN tunnel 341a to the first computing device 102a that is facilitating traffic for the hard IP phone 210a. One ordinarily skilled in the art will recognize and appreciate that the gateway 340 may communicate to the telecommunication device 210 and/or computing device 102a that network address for contacting the computing device 102b and/or telecommunication device 210b directly by any suitable means and/or mechanisms. For example, the gateway 340 may communicate the second network address to the first computing device 102a via a second tunneling session.

In some embodiments, the gateway indicates to the first computing device 102a of the last known public IP address that the second computing device 102b which is running the soft IP phone 210b used to contact the gateway 340. In other embodiments, this public IP may not be the actual IP address of the second computing device but may be the IP address of the firewall 205b that the second computing device 102b is behind. If the computing device 210a contacts the public IP address of the firewall 205b directly, packets may be rejected by the firewall 205b. In these embodiments, the gateway 340 instructs the computing device 102b to establish what is known to those skilled in art as a swimmer session to the first computing device 102a. A forward hole is punched in the firewall 205b via which the first computing device 102a can traverse or get back in. In other embodiments, any suitable means and/or mechanism may be used to allow the first computing device 102a to traverse the firewall 205b to connect and communicate with the second computing device 102b.

Although illustrative method 260 is discussed in conjunction with environment 200 of Figure 2A having the second computing device 102n behind a firewall 205a, as one ordinarily skilled in the art will recognize and appreciate, the illustrative method 260 can be used in environments where the second computing device 102b is directly accessible without traversing a firewall 205a. As such, the illustrative method 260 may not need to at step 274 instruct the second computing device 102b to provide a swimmer session or other mechanism for the first computing device 102a to connect to the second computing device 102b.

In some embodiments, the gateway 340, at step 276, may negotiate a secret key between the computing devices 102a-103b for secure communications. The remote access client 120 on the computing devices 102a-102b may use this key for secure and encrypted communicates, and/or to authenticate or authorize the other computing device. In other embodiments, to ensure that malicious computing devices do not take advantage of this open hole, the gateway 340 at step 276 negotiates a secret key between the two computing devices 102a and 102b and the respective remote access clients 120 ensure that the keys match before allowing data communication. For example, in the embodiment of establishing a swimmer session, this key ensures that the packets coming in the open hole are from the computing device that the swimmer session was meant for.

In other embodiments, the gateway 340 does not perform step 276 to provide a secure mechanism of peer-to-peer communication sessions between the computing

devices 102a-102b. For example, the computing devices 102a-102b may be in the same private enterprise network and therefore, may be trusted. In further embodiments, instead of the gateway 340 negotiating a secret key, the computing devices 102a-102b use any suitable means and/or mechanism for authenticating and/or authorizing the other computing device for peer-to-peer communications. In some embodiments, the computing devices 102a-102b may authenticate and/or authorize via the gateway tunneling sessions, such as via path 341a, or at step 280, via the media path 225 established at step 278. For example, the remote access clients 120 of each computing device 102a-102b may check for matching keys over established media path 225 before allowing any data to be communication over the connection 225.

At step 278, the direct media path 224 for any type and/or form of communications is established between the computing devices 102a-102b without traversing the gateway 340, and, in some embodiments, not using the respective VPN assigned IP addresses of the computing devices 102a-102b but instead their public IP address or the IP address assigned to them by their resident network. Using the techniques of the present invention, the respective remote access client 120 of computing devices 102a-102b act as temporary peer-to-peer SSL gateways to each other, decrypting each other's SSL session directly without communicating via the gateway 340. The direct peer-to-peer communication session via path 225 avoids the extra-hop via the gateway 340. This will reduce any latency due to taking a longer route via the gateway 340, and will improve the quality, performance, and experience of real-time data communications, such as the VoIP communications illustrated in Figure 2A.

In some embodiments, the gateway 340 may be configured to automatically perform the techniques of illustrative method 260 every time a computing device 102 is trying to establish a peer-to-peer communication session or otherwise access a resource via the gateway 340. In other embodiments, the gateway 340 may be configured to automatically perform the techniques of the illustrative method 260 only for a certain IP address range either for a source IP address, a destination IP address, or any combinations thereof. In further embodiments, the gateway 340 may perform this technique based on the type of application and/or resource being accessed via the gateway 340. For example, in one embodiment, the gateway 340 may automatically perform this technique for any type of desktop or screen sharing application sharing screen data via the gateway 340. In other embodiments, the gateway 340 may determine

to perform this technique based on any type and/or form of business rules, access control policies, or other configuration, algorithm, and statistics. For example, the gateway 340 may perform this technique based on ping-based timing statistics between peer computing devices. If the peer computing devices are closer to each other than the gateway 340, the gateway performs the peer-to-peer routing technique. One ordinarily skilled in the art will recognize and appreciate the various ways the gateway of the present invention may be adapted or otherwise configured to perform the peer-to-peer routing technique of the present invention.

In one aspect, the present invention is related to allowing communications via a lossless protocol packets constructed for transmission via a lossy protocol. In one technique illustrated in Figure 3B, the present invention use a false acknowledgement technique when communicating a lossy or unreliable protocol via a lossless or reliable protocol, such as, for example, communicating RTP over UDP via a TCP or SSL/TCP connection. In another technique illustrated in Figure 3C, the present invention uses payload shifting to communicate via a lossless protocol packets constructed for transmission via a lossy protocol. In some embodiments, these techniques of the present invention helps achieve Transport Layer Security (TLS) at a UDP level as one ordinarily skilled in the art will recognize and appreciate in view of the description below.

The illustrative method 360 of the embodiment of the present invention for practicing the false acknowledgement technique will be discussed in view of the illustrative environment 300 of Figure 3A and additionally in view of Figures 1A-1E. In brief overview, the environment 300 comprises a client 105a of computing device 102a in communications with a peer client 105b of computing device 102b or alternatively, the gateway 340 via network 104. In some embodiments, the client 105a may traverse IP routers 305a-305b or the network 104 may have IP routers 305a-305b. Although, in other embodiments, the computing devices 102a-102b and gateway 340 may be on the same network 104. Additionally, a telecommunication device 210a may be associated with client 105a and a second telecommunication device 210b may be associated with the peer client 105b or the gateway 340.

Client 105a may comprise a first network stack 310a, and the client 105 or gateway 340 may comprise a second network stack 310b. The network stacks 3201a-310a may comprise one or more network layers, such as any networks layers of Open Systems Interconnection (OSI) communications model. For example, as illustrated in

Figure 3A, the network stacks 310a-310b comprises a TCP/IP 343a-343 communication layer communication on top of the frame layer that is suitable as known to those skilled in art for a TCP/IP based network 104. The TCP layer 343a-343b comprises an illustrative embodiments of a reliable or lossless protocol. For example, in TCP 343a-343b as known to those ordinarily skilled in the art, the network stack 310a-310b or any drivers or mechanisms thereof, such as a TCP driver, may perform algorithms and operations, and comprise logic or functionality to provide one or more of the lossless or reliable characteristics of the protocol. For example, to support TCP 343a-343b, the network stack 310a-320b may perform packet ordering, packet retransmission, acknowledgements of receipt of packet, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm, and any other reliability related operations and algorithms as one ordinarily skilled in the art will recognize and appreciate in view of TCP 343a-343b or any other lossless protocol.

Additionally, the networks stacks 310a-310b may comprise an SSL 341a-341b layer for supporting SSL or SSL VPN communications. For example, the SSL layer 341a-341b may be used for a gateway or tunneling session between remote access clients 120 or between a remote access client 120 and a gateway 340. As illustrated in Figure 3A, the network stacks 310a-310b may also provides a layer for a lossy protocol 342a-342b, such as UDP, to be communicated over the lossless protocol 343a-343b, such as TCP. In some embodiments, the lossy or unreliable protocol 342a-342b may comprises Real Time Protocol (RTP) over UDP, and may comprise a payload have any type and/or form of real-time data, such any representation of voice or audio. In other embodiments, the lossy protocol 342a-342b may carry the VoIP over communications to and from the client 105a in an established VoIP session, such as a session established via illustrative method 260 discussed above in connection with Figures 2A and 2B. A lossless protocol, such as UDP 342a-342b may be chosen for real-time applications like voice, because it may be more important to get packets to the recipient, such as peer client 105b, on time rather than getting the packets in a reliable manner, such as via a lossless protocol.

The network stacks 310a-310b also include a shim 322a-322b of the remote access client 120 of the present invention. The shim 322a-322b may comprise any portion of the remote access client 120, and in some embodiments, comprises a network driver, network driver interface, or other network layer related mechanism for providing

the false acknowledgement technique of the present invention as described herein. The shim 322a-322b may comprise software, hardware, or any combination of software and hardware. In one embodiment, the shim 322a-322b may operate at the IP layer of the network stack prior to a network packet reaching the TCP layer 343a. In other embodiments, the shim 322a-322b may operate at the TCP layer 343a-343b. One ordinarily skilled in the art will recognize and appreciate that the shim 322a-322b may operate in any manner associated with the layer of operations of the lossless protocol in the network stack 310a-310b, including in or adjacent to the layer of the lossless protocol.

The false acknowledgement technique of the present invention as illustrated by method 360 of Figure 3B allows a lossy protocol, such as UDP 342a-343b, to be communicated via a lossless protocol, such as TCP 343a-343b. By the shim 322a-322b issuing a false acknowledgement of receipt of a TCP packet, the technique of the present inventions prevents or avoid the reliability mechanisms, operations and algorithms of the lossless protocol, such as in the example of TCP 343a-343b, any of the packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. As such, the lossy protocol 342a-342b can be communicated over a lossless protocol 343a-343b but maintain its lossy or unreliable characteristics which may be desired such as in real-time data communications. This technique also enables the lossy protocol to be communicated securely, or traverse a gateway via a tunneling protocol, or simply via TCP/IP while not applying the lossless characteristics of the lossless protocol to the lossy protocol communications.

In brief overview of illustrative method 360, at step 365, the computing devices 102a and 102b or the gateway 340 establish a lossless protocol based connection, such as a TCP connection, by which lossless protocol packets are communicated. At step 370, the remote access client 120 of the present invention may detect that the payload of a lossless protocol packet comprises a lossy protocol, such as RTP or UDP, or otherwise comprises real-time data. In one embodiment, at step 375, the illustrative method 360 may encrypt the payload with a key, such as a key provided via an out of band TLS or SSL session of step 367. At step 380, a false acknowledgement of receipt of the lossless protocol packet may be communicated or otherwise provided to the network stacks 310a-310b, such as by the shim 322a-322b. In response to the receipt of the false acknowledgement of receipt of the lossless protocol packet, at step 385, the respective

network stacks 310a-310b do not execute one or more, or all of the algorithms and operations that provide the reliable or lossless characteristics of the lossless protocol. At step 390, the lossless protocol packet with the lossy protocol payload is communicated between the network stacks 310a-310b.

At step 365 of illustrative method 360, the lossless protocol connection may be established via any suitable means and/or mechanisms using an type and/or form of lossless protocol. In one embodiment, the network stack 310a of a client 105a establishes a lossless protocol connection, such as TCP, to a peer client 105a having network stack 310b. In another embodiment, the network stack 310a of client 105a establishes a lossless protocol connection to a gateway 340 having network stack 310b. Additionally, the lossless protocol connection of step 365 may be established in a secured manner, such as SSL, or as a virtual private connection. Although the network stacks 310a-310b are illustrated as having the same network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks may have corresponding layers, which may be of different versions or associated with different operating systems and/or drivers, and that each network stack 310a-310b may have additional layers, less layers or different layers.

At illustrative step 360, in one embodiment, the remote access client 120 intercepts a network packet, such as via the packet capture mechanism 365, and inspects the network packet by any suitable means and/or mechanisms to determine the type of the protocol used in the payload of the network packet, or the type of contents in the payload of the network packet. In some embodiments, the shim 322a-322b of the remote access client 120 may be used for intercepting and inspecting the network packet. In one embodiment, the remote access client 120 may intercept a network packet and determine if the network packet comprises any lossless protocol or a specific lossless protocol, such as TCP. If the network packet is a lossless protocol, the remote access client 120 checks the payload to determine the type of protocol and/or the type of data. In one embodiment, the remote access client 120 may determine by any suitable fields of the payload of the network packet, such as any portion of header of the lossy protocol representing the payload, that the payload has a lossy protocol content. In another embodiment, the remote access client 120 may determine by any data of the payload, if the payload comprises a lossy protocol or comprises real-time data.

In one embodiment, the remote access client 120 determines that a TCP packet comprises a payload of RTP or UDP, and applies an encryption of the payload. The remote access client 120 may encrypt the payload of the network packet using any type and/or form of encryption with a key provided in any suitable manner. In some embodiments, the key or cipher is negotiated via an out of band TLS session between the clients 105a-105b or the client 105a and gateway as shown in Figure 3A as opposed to, in other embodiments, a traditional TLS session where the session is first negotiated and the same socket is used for data communication. In some embodiments, the encryption at step 375 is performed on a packet by packet basis. In another embodiment, encryption is performed on multiple packets at a time.

At step 380 of illustrative method 360 of the present invention, a false acknowledgment of receipt of the network packet, e.g., the lossless protocol packet, is issued, communicated, or otherwise provided to the network stacks 310a-310b comprising the respective sending and receiving computing devices 102a-120b, or gateway 340. The shim 322a-322b, any portion of the remote access client 120, or any portion of the network stack 310a-310b may issue the false acknowledgment of receipt of the network packet. In one aspect, the false acknowledgement of receipt of the network packet is false in the sense that it is communicated not to acknowledge the actual receipt of a network packet but in order to prevent the lossless and reliable mechanisms of the lossless protocol associated with the network stacks 310a-310b. As such, the false acknowledgement of receipt of the network packet may comprise the same form and/or type as an actual acknowledgement of receipt of the network packet.

In some embodiments, the false acknowledgement of receipt is issued to the network stacks 310a-310b prior to communicating the network packet or packets. In other embodiments, the false acknowledgement of receipt is issued after communicating the network packet(s) but at a time or in a manner such as to prevent the lossless protocol mechanisms of the receiving network stack 310a-310b from being applied to the transmitted network packet. In one embodiment, the false acknowledgment of receipt of the network packet is issued for each network packet, and in another embodiment, may be issued once per communication session or lossless protocol connection. Furthermore, one ordinarily skilled in the art will recognize and appreciate the false acknowledgement of receipt may be performed in different places in the network stack 310a-310b for different operating systems. For example, in one

embodiment, the acknowledgement of receipt may be issued at the Network Driver Interface Specification (NDIS) driver level in the Microsoft Family of Windows Operating Systems.

At step 385 of illustrative method 360, the network stack 310a-310b receiving the false acknowledgment of receipt of the network packet from step 380 may in response to such receipt, may not execute, stop executing, or prevent from executing any one or more algorithms and operations providing one or more lossless characteristics of the lossless protocol. For example, in the embodiment of TCP as the lossless protocol, the network stack 310a-310b may not execute any one or more of the following with respect to the network packet, or the TCP connection: packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. In some embodiments, the false acknowledgment of receipt must be received on a packet by packet basis to prevent the lossless layer of the network stack 310a-310b from employing reliability algorithms. As such, the sending network stack 310a-310b can determine on a packet by packet basis which packets to apply the false acknowledgment techniques of the present invention to. There may be some lossless protocol network packets comprising the lossy protocol for which the reliability algorithms of the lossless protocol should be applied. In other embodiments, the false acknowledgment of receipt of the network packet may be received once for the lossless protocol connection to prevent employing reliability algorithms for any subsequent packets received during the lossless protocol session or connection.

At step 390, the illustrative method 360 communicates the lossless protocol packet having the lossless protocol payload via the network stacks 310a-310b. In one embodiment, the lossless protocol packet is communicated after step 385, or in other embodiments, before step 385. So, although the lossless protocol packet becomes lost in the network, no attempt is made to reclaim the packet as one would expect for a lossy protocol packet.

Although the illustrative embodiment of method 360 is discussed using a false acknowledgment of receipt of the network packet such as in TCP, any type and/or form of indication, request, or instruction may be communicated to the network stacks 310a-310b to prevent employing any reliability or lossless algorithms of the lossless protocol. In some embodiments, the lossless protocol layer of the network stack 310a-310b may be adapted or configured to have a configuration, flag, or instruction to not use the

reliability algorithms either on a packet by packet basis, or a session or connection basis. For example, the lossless protocol may have fields, such in a header of a lossless protocol packet, that indicates whether reliability should be discarded or avoided for the packet.

Referring now to Figure 3C, another embodiment of steps taken to transmit packets constructed according to a lossy protocol via a lossless protocol is shown by illustrative method 345, which may also be referred to as a payload shifting technique. In brief overview of illustrative method 345, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device, such as client 105. At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. The first device 105 transmits the first TCP packet to the second device at step 352. At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, and at step 356, creates a second TCP packet including a second payload of the received second packet and the first TCP header information. At step 358, the first device transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

Still referring to Figure 3C, and now in more detail, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device 105. In some embodiments, the packet is intended to be transmitted using a lossy protocol of UDP. In further embodiments, the packet comprises RDP over UDP. In other embodiments, the first packet is generated by an application program 338 executing in user mode 332. In some embodiments, the packet is generated by an application 338 executing in kernel mode 334. In other embodiments, the first packet is received by the first device 105 for retransmission. In still other embodiments, the first packet is intercepted by a filter process 322 before it reaches the network stack 310a-310b. The filter process 322 may execute in user mode 332 or in kernel mode 334. In some embodiments, the filter 322 is a mini-driver. In other embodiments, the filter 322 is an NDIS driver. In other embodiments, the filter 322 process uses application hooking to intercept the first packet. In further embodiments, the application hooking is implemented via an application programming interface (API). In one embodiment, the hooking of network packets occurs at the network layer of the network stack 310a-310n.

At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. For example, the TCP connection may be established between the client 105 and a peer computing device 102b in one embodiment, and between the client 105 and the gateway 340 in another embodiment. In some embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by opening a specific TCP port. In other embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by setting a flag in the TCP header. The TCP header may include information regarding the source node, information regarding the destination node, or a sequence number particularly identifying the TCP packet.

At step 352, the first device 105 transmits the first TCP packet to the second device. In some embodiments, the second device may be a gateway 340. In other embodiments, the second device is a "peer" computing device 102b. The first TCP packet may be encrypted before transmission to the second device using, for example, SSL or TLS.

At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, such as UDP. The second packet may be received from the same application 338 that generated the first packet. At step 356, the first device 105 creates a second TCP packet including a second payload of the received second packet and the first TCP header information, as described above. At step 358, the first device 105 then transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device. In some embodiments, when an acknowledgment is received from the second device, the first device 105 updates the TCP header information before transmitting the packet. In other embodiments, the first device 105 creates a third TCP packet with updated TCP header information and having the second payload. The first device then transmits the third TCP packet.

Upon receipt of the TCP packet, the second device decrypts it, if necessary, and determines that the payload is one or more packets constructed to be transmitted using a lossy protocol. The second device may determine this based on the port on which the

packet was received or by a flag in the TCP header information. Once determined, the second device strips the TCP header from the payload and delivers the payload.

In another aspect, the present invention is related to adjusting the reported maximum transmission unit (MTU) parameter to optimize network communications by reducing packet fragmentation for encrypted network packets. This technique may be applied on one or both network stacks 310a-310b of illustrative environment 300 of Figure 3A. Encrypting a payload of a network packet, such as any network packet processed according to the illustrative method 360 described above, may increase the size of the payload. That is, the size of the network packet may increase to account for the change in size of the unencrypted original payload to the encrypted payload.

Still referring to Figure 3A, the network stacks 310a-310b may comprise a maximum transmission unit 402a-402b (MTU) parameter to indicate the size of the largest unit of data that can be sent over a type of physical medium in a network, such as an Ethernet based network. In the embodiment of TCP/IP, the MTU 402a-402b indicates the largest datagram or packet than can be transmitted by an Internet Protocol (IP) layer interface, without the interface needing to br4eak down or fragment the datagram into smaller units. An MTU parameter 402a-402b may be associated with a communications interface such as a network interface card. The default MTU size for Ethernet is 1,500 bytes, and IEEE 802.3 is 1,492 bytes. As one ordinarily skilled in the art will recognize and appreciate, the default MTU size will be based on the networking technologies such as Token Ring, FDDI, X.25, etc.

Referring now to Figure 4, a flow diagram depicts an illustrative embodiment of the MTU adjustment method 400 of the present invention. In brief overview, at step 405, a session between computing devices is established, such as between a first computing device 102a and a second computing device 102b. At step 410, one of the computing devices 102, such as the first computing device 102a, detects a network packet having an encrypted payload. At step 415, the computing device 102a-120b determines a setting for the MTU 402a-402b parameter of the network stack 310a-310b to account for the size of the encrypted portion of the payload. At step 420, the MTU 402a-402b parameter is decreased to account for the encrypted portion. If the MTU 402a-402b is requested or reported, the MTU 402a-402b will indicate a size smaller than the MTU size associated with the physical layer, such as 1,500 for Ethernet.

Using this technique, any device on the network 104 may communicate network packets to the network stack 310a-310b according to the decreased MTU size that can be encrypted along the route to the network stack 310a-310b and not be fragmented. If the network packet is encrypted it should still fit in the actual MTU size of the physical network layer medium, such as Ethernet. For example, the MTU parameter 402a-402b may be set to the default MTU size of 1,500 for Ethernet and in accordance with the illustrative method 400 decreased by a determined number of bytes, for example 100, to account for encryption overhead. A network packet may be transmitted from a server resource to the client comprising a size equal to the reported MTU 402a-402b size of 1,400. The network packet may traverse the gateway 340 and get encrypted via the SSL tunnel, which in turns increases the network packet size to 1,475. Since this size fits into the MTU size of the Ethernet physical medium, the network packet will not be fragmented.

At step 405 of illustrative method 400, any type and/or form of communication session between a first computing device 102a and a second computing device 102b, such as client 105b or gateway 340 of Figure 2A, may be established. In some embodiments, the session is established using the remote access client 120 on a first computing device. In one embodiment, the remote access client 120 establishes a session with the gateway 340, such as an SSL VPN session, or to another remote access client 120 on a peer computing device 102b.

In some embodiments of step 410, the remote access client 120 detects a network packet having an encrypted payload. In one embodiment, the packet capture mechanism 365 intercepts network packets and the agent 326 determines if the packet is encrypted. However, any other portion of the remote access client 120, such as the filter 322 or frame monitor 360 may determine if the packet is encrypted. In one embodiment, the entire payload of the network packet is encrypted, while in other embodiments, a portion of the payload is encrypted. The present invention may use any type and/or form of means or mechanism for determining if a packet has encryption. For example, in some cases, the remote access client 120 may check for a flag or field of the network packet indicating the payload is encrypted. In other embodiments, the remote access client 120 may check whether any portion of the payload is unintelligible, because it contains random data or noise from encryption. Additionally, the encrypted payload may be

encrypted in association with any layer of the network stack 310a-310b, such as layer 2, 3, 6 or 7 encryption.

In some embodiments of step 415, the illustrative method 400 of the present invention determines the adjustment to the reported MTU 402a-402b size on a packet by packet basis, or in other embodiments, on a connection or session basis, and at step 420 adjusts the MTU 402a-402b accordingly. In one embodiment, the MTU 402a-402b is decreased exactly by the amount of encryption overhead for the network packet. In some cases, the illustrative method 400 determines the MTU 402a-402b size adjustment once for the entire session or connection and decreases the size of the MTU 402a-402b to a value to account for encryption overhead for the entire session. For example, although network packets may have varying encryption overhead, the adjustment accounts for the largest encryption overhead. In further embodiments, the MTU 402a-402b may be adjusted to take into consideration encryption that may occur when the network packet leaves the network stack 310a-310b, such as encryption by a gateway 340 that may occur in the end-to-end network traversal of the network packet .

Additionally, the MTU 402a-402b size may be adjusted for other network performance factors in addition to the encryption overhead. In some embodiments, although the MTU 402a-402b is decreased due to encryption overhead, it may be further decreased to account for other overhead and factors related to network communication, as well as increased in other cases. For example, the MTU 402a-402b may have been previously adjusted for a factor not related to encryption and after using the techniques of the present invention the MTU 402a-402b is decreased to take into account encryption overhead. One ordinarily skilled in the art will recognize and appreciate that there may be other factors and considerations for adjusting the MTU besides or in addition to adjusting for encryption overhead in accordance with the techniques of the present invention.

Referring now to Figures 5A and 5B, the present invention, in an additional aspect, is related to client-side application-aware network communication prioritization techniques. The remote access client 120 of the present invention provides for the intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application. As depicted in the system 500 of Figure 5A, the remote access client 105 of computing device 102 is connected to network 104. The client 105 may execute one or more applications 338a-338n, which

access the network 104 via the agent 326 and filter 322 of the remote access client 120. In some embodiments, the applications 338a-338n provide one or more real-time data communications, such as VoIP. In other embodiments, one or more of the applications 338a-338 may provide email, collaboration, online meeting, and/or desktop sharing related services or functionality.

As illustrated in Figure 5A, the packet capture mechanism 365, 365' may be included in the filter 322 or the agent 326 of the remote access client 120, for intercepting network traffic of any of the applications 338a-338n of the client 105. The remote access client 120 may comprise any queues 540a-540n for queuing and prioritizing network communications of the client 105. In one embodiment, the queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322, and in other embodiments, may be included with or accessible by the agent 326. The queues 540a-540n may comprise any type and/or form of suitable means and/or mechanisms for storing and/or arranging network packets, such as network packets intercepted by the packet capture mechanism 365. In some embodiments, the queues 540a-540n may be associated with or assigned to network packets related to applications 338a-338n of the client 105. In other embodiments, the queues 540a-540n may be organized by levels of priority, such as high, medium, low, or numerically such as priority 1...10. One ordinarily skilled in the art will recognize and appreciate that number of queues 540a-540n may be based on any desired granularity of prioritization, such as 3, 5 or 10 levels of priority. Additionally, some of the queues 540a-540n may be used for receiving and/or transmitting network packets prior to being placed into and/or taken out of a priority based queue 540a-540n.

The remote access client 120 may also have, access, or use a routing table 538 for determining how to route network packets of the client via the agent 326, such as onto the network 104 via a gateway 340. In one embodiment, the agent 326 establishes and maintains an SSL VPN connection to the gateway 340, such as illustrated in Figure 1A for example. In one embodiment, the routing table 538 comprise information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points. The routing table 538 may include a source IP address and source port, and an destination IP address and destination port to identify a communication path on the network 104. For example, the source IP address and source port may represent the IP

address of the client 105 and the port by which an application 338a-338n on the client 105 communicates on the network 105. The destination IP address may represent the IP address of a peer computing device to which the application 338a-338n communicates with via the destination port used by the peer device.

Additionally, the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application. These policies 520 may be specified by any suitable means and/or mechanisms. In some embodiments, the policies 520 may be specified by the name of the application 338a-338n and/or the type of application 338a-338n. In other embodiments, the policies 520 may be specified in accordance to the type of one or more protocols used by the applications 338a-338n and/or the size of the payload of the network packet. In another embodiment, the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105. In yet another embodiment, policies 520 may indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port number. Additionally, the policies 520 may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105 at any point. Furthermore, the policies 520 may be specified conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority. One ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.

The policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326. For example, the policies 520 may be provided by or downloaded via the gateway 340. The policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file. The policies 520 may be configurable by a user by any suitable means and/or mechanism. For example, the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.

In view of the system 500 of Figure 5A and Figures 1A-1C, the prioritization technique of the present invention illustrated by method 550 in Figure 5B will be described. In brief overview, at step 555 of the illustrative method 550, the client 105

intercepts one or more networks packets associated with an application 338a-338n on the client 105, and, at step 560, the network packets are stored to a queue 540a-540n. At step 565, a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application 338a-338n. At step 570, the determined priority is indicated for the network packets, and, at step 575, the network packets are communicated according to the determined priority. As such, the outbound network packets generated by an application 338a-338n on the client 105 are prioritized by the client 105 prior to transmission based on the type and/or priority of the application 338a-338n. For example, the application 338a may generate real-time data of VoIP communications, such as RTP over UDP via a TCP/IP session of an SSL connection to the gateway 340. The client 105, using the techniques of the present invention, may prioritize the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications. This technique may compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.

At step 555 of illustrative method 500, the client 105 may intercept network packets of one or more applications 338a-338n transparently to the application 338a-338n, the gateway 340, a peer computing device, and any of the network layers of a network stack. In this manner, the techniques of the present invention support any type of application 338a-338n on the client 105. In some embodiments, the network packets are intercepted by the packet capture mechanism 360 via agent 326 or filter 322. Any inbound and/or outbound network packets of an application 338a-338n may be intercepted by the remote access client 120 of the present invention.

At step 560, the network packets intercepted at step 555 may be stored in a queue 540a-540n. In one embodiment, the network packet is stored to a temporary queue 540a-540n prior to prioritizing the network packet at steps 565 and 570. In other embodiments, the network packet is stored to a determined priority queue 540a-540n or a queue 540a-540n associated with an application 338a-338n after the network packet is prioritized at steps 565 and/or step 570.

At step 565, the remote access client 120 of the present determines the association of network packets with applications 338a-338n in order to determine priorities and apply any priority based policies 520. The client 105, such as via agent 326, can associate network traffic with applications 338a-338n by any suitable means

and/or mechanisms. In some embodiments, the agent 326 identifies the network packet as generated from an application 338a-338n by any of the content of the network packet, such as any headers, fields, or the type and content of data in the payload of the network packet. In other embodiments, a network packet is associated with an application 338a-338n by matching information from the routing table 538, such as source and destination IP addresses and ports numbers with the IP addresses and ports numbers of the network packet. In some embodiments, the agent 326, such as via the frame monitor 360, may perform a checksum on the packet to verify that the identified application actually generated the packet.

Additionally, the remote access client 120 may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105. Furthermore, the remote access client 120 may determine any priorities, such as process task priority, assigned to the application 338a-338n by the operating system of the client 105. In other embodiments, the remote access client 120 may determine any other characteristics or statistics of the application 338a-338n such as size, memory usage, total execution time, and/or frequency of use. One ordinarily skilled in the art will recognize and appreciate the various characteristics of an application the present technique may use for providing client-side application-aware network communication prioritization.

At step 570, the remote access client 120 of the present invention indicates a priority for intercepted and queued network packets based on the application 338a-338n associated with the packet at step 565. In one embodiment, the agent 326 uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520. In some embodiments, the agent 326 may use characteristics of the application 338a-338n, such as running in the foreground or background, to indicate priority for a network packet of the application 338a-338n. In other embodiments, the agent 326 may use any combination of the policies 520 and characteristics of the application 338a-338n to indicate a priority for the network packets of the application 338a-338n.

In some embodiments, the agent 326 indicates the priority to the filter 322 for management of network packet queues 540a-540n to apply the indicated priorities. The agent 326 may communicate the priority of network packets to the filter 322 by any suitable means and/or mechanism such as via an application programming interface

(API), such an IOCTL interface, or any other type and/or form of interface known to those ordinarily skilled in the art. In one embodiment, the filter 322 is not aware of the application 338a-338n by name but can associate priorities to network packets of applications 338a-338n via the routing table 538. An application 338a-338n corresponding to a network packet can be identified by any combination of source and destination identifiers, such as IP addresses and port numbers. As such, in some embodiments, the agent 326 indicates priorities to the filter 322 by routing information instead of application name. In other embodiments, the agent 326 provides to the filter 322 a mapping between applications 338a-338n, such as by application name or process id, to the routing information in a routing table 538.

Based on the indicated priorities for applications 338a-338n, in some embodiments, the filter 322 may place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities. In one embodiment, the filter 322 may move network packets from temporary queues 540a-540n or from memory or other storage to a queue 540a-540n associated with the application 338a-338n, a queue 540a-540n associated with a priority, or a queue 540a-540n associated with both an application and a priority. For example, in one embodiment, all high priority network traffic may be placed in a high priority queue 540a and arranged in order based on an order of priority of the application 338a-338n, such as real-time data applications 338a-338n prior to other applications 338a-338n. In some embodiments, the network packets may be arranged in order in a priority queue 540a-540n based on the time the network packet was intercepted by the packet capture mechanism 365, such as in a FIFO manner. In yet a further embodiment, one queue 540a-540n may be used for prioritization by the filter 322. Each network packet may be placed and arranged in a priority order respective to all other intercepted network packets to provide a packet by packet prioritization across all applications 338a-338n and intercepted network packets. One ordinarily skilled in the art will recognize and appreciate that the network packets may be arranged in various priority queues 540a-540n, such as high, medium, low, or by any other granularity, and be placed or arranged in the queue in any suitable manner in practicing the operations of the present invention described herein.

In one embodiment, all network packets for an application 338a-338n are placed in a queue 540a-540n associated with the application 540a-540n. For example, intercepted network packets for an application communicating to a first destination IP

address, and a first destination port may be placed in a first queue 540a. In another embodiment, all networks packets for a type of application 338a-338n, such as an email or voice application, or all network packets for a type of protocol used by the application 338a-338n, such as RTP or UDP, may be placed in a queue 540a-540n for prioritizing networks packets for one or more applications. For example, online collaboration related applications 338a-338n may be placed and prioritized in a first queue 540a for collaboration related applications. A second queue 540b may be used for email related applications 338a-338n. In another example, a queue 540a may be used for applications 338a-338n communicating real-time data or communicating using the RTP and/or UDP protocol. In a further example, a queue 540a may be used for applications 38a-338n communicating using a remote display protocol, such as ICA or RDP.

Within each application associated queue 540a-540n organized by specific application 338a-338n, type or category of application 338a-338n, or by protocol, the network packets may be further prioritized by the characteristic of the application 338a-338n generating them, e.g., a foreground application, the size of the network packet, or the time the network packet was intercepted. In some embodiments, one or more queues 540a-540n may be used for network packets intercepted but not prioritized because a policy 520 does not exist or apply to the network packet, or the policies 520 indicate to ignore or not process the network packet for prioritization. One ordinarily skilled in the art will recognize and appreciate the various ways network packets may be placed and arranged in a priority based manner in queues 540a-540n associated with the application 338a-338n, the type of application 338a-338n or the protocol used by the application 338a-338n, and that the priority may be based on the policies 520 specified for the client 105.

At step 575 of illustrative method 550, the network packets are communicated from the queues 540a-540n according to the determined priorities for the network packets. In some embodiments, the network packets are organized into priority queues 540a-540b so that the network packets of the highest priority queue 540a-540n are communicated first, and then the next highest priority queue 540a-540n second, and so on. In other embodiments, the queues 540a-540n are organized by application 338a-338n, and therefore, at step 575, the present invention communicates network packets from the queue 540a-540n based on the respective priorities of the applications 338a-338n. Regardless of the queue 540a-540n organization and management, one ordinarily

skilled in the art will recognize and appreciate that the remote access client of the present invention will communicate the network packets from the queues in a manner according to or consistent with the determined priorities, which in turn, may be based or derived from the policies 520 of the client.

In some embodiments, the remote access client 120 of the present invention considers other network factors in determining what network packets to communicate from what queue. For example, the remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application 338a-338n. In another example, the remote access client 120 may recognize a high number of retransmits to a particular destination. As such, in some embodiments, the remote access client 120 may throttle back or not communicate network packets related to other networks factors, such as congestion, even though the network packets may have a higher priority than other network packets in a queue 540a-540n. Thus, the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338a-338n basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network.

In yet a further aspect and referring now to Figures 6A and 6B, the present invention is related to providing a network disruption shielding technique for persistent and reliable connectivity. Figure 6A illustrates environment 300 as discussed above in conjunction with Figure 3A. The environment 300 illustrates network stacks 310a and 310b, which may represent network stacks of computing devices 102a-120b or gateway 340, such as any of the computing devices 102 and the gateway 340 illustrated in Figures 1A-1C, 2A, or 5A. Each network stack 310a-310b may comprise one or more networks layers, such as a TCP/IP network layer on top of the frame network layer as one ordinarily skilled in the art will recognize and appreciate. Although the network stacks 310a-310b are illustrated in environment 300 of Figure 6A with a certain set of network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks 310a-310b may have any type and/or form of network layers, in any suitable combination, and each of the network stacks 310a-310b may have different forms of each layer in relation to the other network stack.

The network stacks 310a-310b may be considered to have a first portion 605a-605b of the network stack, and a second portion 610a-610b of the network stack. As

illustrated in the example network stacks 310a-310b of Figure 6A, the first portion 605a-605b of the network stack comprises the network layers at and below the TCP network layer. The second portion 610a-610b may comprise those network layers above the TCP network layer, such as a UDP over SSL protocol layer. Although the first portion 605a-605b and the second portion 610a-610b are shown as portioned, segmented, or otherwise divided at the TCP layer, the first portion and second portion may be formed at a higher or lower dividing layer in practicing the network disruption shielding technique of the present invention as one ordinarily skilled in the art will recognize and appreciate.

The network stacks 310a-310b illustrated in Figure 6A may represent an application 338a-338n on client 105, such as the client depicted in Figure 5A, establishing a peer-to-peer SSL VPN connection to a second computing device 102b or, alternatively, a gateway 340. The client 105 may be a mobile client, such as a notebook, personal digital assistant (PDA), a smart phone, or any type of mobile computing or telecommunication device. The client 105 may communicate real-time data such as VoIP communication via the UDP protocol or RTP over UDP via the SSL session established to the peer device 102b or gateway 340. In one embodiment, the agent 326 of the remote access client 120 establishes and maintains the SSL or SSL VPN session to the gateway 340 or to peer computing device 102b. The agent 326 may operate in user-mode 332, and may handle any network layer and protocol processing related to the second portion 610a-610b of the network stack 310a-310b, along with any application layer protocols. As a TCP/IP based network 104, the UDP over SSL session of the second portion 610a-610b of the network stack 310a-310b may be communicated over a TCP/IP stack forming the first portion 605a-605b of the network stack 310a-310b. In view of the remote access client 120 of the present invention, such as illustrated in Figure 1A or 5A, the filter 322 may be a network driver operating in kernel-mode 332 within the first portion 605a-605b of the network stack 310a-310b.

The present invention uses a network disruption shielding technique as depicted by illustrative method 650 in Figure 6B to maintain the second portion 610a-610b of the network stack 310a-310b through a network level connection interruption, such as any type and/or form of network disruption to the first portion 605a-605b of the network stack 310a-310b. The network disruption shielding technique of the present invention may be performed transparently to an application 338a-338n of the client 105, a user of the client 105, any one or more network layers above the first portion

605a-605b, and the gateway 340 or peer computing device 102b, and any portion of their respective network stacks 310a-310b. In one embodiment, the network disruption is shielded without notification to the user of the client that the network was disrupted or a session was interrupted.

In brief overview of illustrative method 650, at step 665, a client 105 establishes a session via at least a first protocol over a network connection between the client and another device, such as a peer computing device or gateway. As such, a network stack 310a-310b is established or used on the client 105. The network stack 310a-310b has a first portion 605a-605b and a second portion 610a-610b. At step 660, a disruption in the network connection is detected causing the first portion 605a-605b of the network stack 310a-310b to be disestablished, or otherwise disrupted from being used or continued to be used. At step 665, the present invention maintains the second portion 610a-610b of the network stack 310a-310b during the disruption and maintaining a session, or sessions, associated with the network layers of the second portion 610a-610b.

During the disruption, at step 670, any network packets related to the second portion 610a-610b of the network stack 310a-310b may be queued. At step 675, the first portion 605a-605b of the network stack 310a-301b is reestablished or otherwise received from the network disruption. While the first portion 605a-605b of the network stack 310a-301b is reestablished, the present invention maintains the second portion 610a-610b, and sessions thereof, allowing at step 680, to continue with the session by linking or re-associating the second portion 610a-610b with the first portion 605a-605b of the network stack 310a-310b. The network connection and/or the session may automatically be re-authenticated at step 680. At step 685, the illustrative method may communicate any queued network packets and continue with the session transparently as if the network disruption did not occur.

In an embodiment of illustrative step 655, a first computing device 102a may establish a network connection with a second device, such as a peer computing device 102b or a gateway 340, by any suitable means and/or mechanism and using any type and/or form of connection based protocol. For example, the network connection may be established via a TCP connection on a TCP/IP network or by an SPX connection on an IPX/SPX network. In some embodiments, the network connection may be initiated by any of the applications 338a-338n on the client, such as any application illustrated in

Figure 5A. For example, a remote display client, such as an ICA client of Citrix Systems, Inc. or a Remote Display Client of Microsoft Corporation may initiate or establish the network connection. In other embodiments, the network connection of illustrative step 665 may be initiated and/or established via the agent 326, filter 322, or any other portion of the remote access client 120. In one embodiment, the establishing of the network connection forms the first portion 605a-605b of the network stack 310a-310b. In other embodiments, the first portion 605a-605b of the network stack 310a-310b, or portion thereof, is established via connection to a network 104 upon startup of the client 105.

In some embodiments, the second portion 610a-610b of the network stack 310a-310b is formed by establishing one more sessions, such as an SSL session, via any type and/or form of protocol over the network connection, such as a remote display protocol of ICA or RDP. The session may be established via any application 338a-338n or the remote access client 120 of the client. In one embodiment, the session may correspond to a tunneling or gateway session with a peer computing device 102b or a gateway 340. In another embodiment, the session may be any type of interactive session such as a media session established via a signaling protocol, SIP for example. For example, the session of the second portion 610a-610b of the network stack 310a-310b may comprise a VoIP communication session, such as one established by illustrative method 260 of Figure 2B. Additionally, there may be multiple sessions associated with the second portion 610a-610b of the network stack 310a-310b. For example, an SSL or SSL VPN session may form one session, while a second session, such as media session via RTP over UDP may form a second session. Additionally, at any application layer of the network stack 310a-310b one or more applications 338a-338n on the client 105 may establish an application level session with a peer computing device 102b. In one embodiment, the agent 326 of the remote access client 120 is responsible for establishing and maintaining the second portion 610a-610b of the network stack 310a-310b and one or more of the associated sessions.

At step 660 of the illustrative method 650 of the present invention, a disruption is network connection is detected. In one embodiment, the network disruption may be caused by a mobile client 105 roaming between networks and networks segments, which, in some embodiments, causes the client 105 to obtain a new network IP address and/or host name. In some embodiments, the disruption disrupts the first portion 605a-

605b of the network stack 310a-310b, such as, for example, causing a TCP or SPX connection to be disconnected. In one aspect, the disruption causes the first portion 605a-605b, or any portion thereof, of the network stack 310a-310b to be disestablished, or otherwise needing to be re-established, reconnected, reconfigured or rebuilt. For example, in some embodiments, the IP layer of the network stack may maintain intact while the TCP layer is reestablished. In one embodiment, any TCP related drivers may need to be re-started. In other embodiments, the TCP/IP layer be intact even though the network connection is disrupted, and only a new TCP connection needs to be established. In other embodiments, the TCP/IP layer is intact but needs to reconfigure itself for a new network or network segment, such as changing the IP address of the client 105. One ordinarily skilled in the art will recognize and appreciate the various ways a network connection may be disrupted and impact or affect a first portion of the network stack.

In some embodiments, the agent 326, or any other portion of the remote access client 120 may detect the network disruption by any suitable means and/or mechanisms. In one embodiment, the agent 326 may determine a network disruption by receiving an error message or failure upon calling or executing an API call to the first portion 605a-605b of the network stack 310a-310b. For example, the SSL session maintained by the agent 326 for the second portion 610a-610b relies or depends on the TCP connection of the first portion 605a-605b of the network stack 310a-310b. As the agent 326 transacts via the SSL session, the agent 326 may receive an error or failure message indicating a problem with the TCP connection. In other embodiments, the agent 326 may receive an event or message from any network layer of the first portion 605a-605b of the network stack 310a-310b indicating a network disruption. One ordinarily skilled in the art will recognize and appreciate the various ways the network disruption may be detected.

At illustrative step 665, in some embodiments, upon detection of the network disruption, the agent 326 or any other portion of the remote access client 120 of the present invention maintains the second portion 610a-601b of the network stack 310a-310b during the disruption. For example, although the SSL based session maintained by the agent 326 depends on an underlying TCP connection, the agent 326 keeps the SSL session open or active through the disruption to the TCP connection. As there may multiple sessions associated with one or more layers of the second portion 610a-610b of the network stack, the agent 326, in some embodiments, keeps one or more, or all, of the

multiple sessions open or active although the first portion 605a-605b of the network stack 310a-310b is disrupted.

At step 670 of illustrative method 650, the remote access client 120 of the present invention, in some embodiments, queues one or more network packets of any of the protocols related to the second portion 610a-610b of the network stack 310a-310b during the network disruption. The remote access client 120 may use any type and/or form of queuing mechanisms, such as any of the queues 540a-540n illustrated in Figure 5A. In other embodiments, the remote access client 120 may discard network packets during the disruption, such any packets related to a lossy protocol, such as RTP over UDP for voice communications. In some cases, it may be desirable to discard packets, such as UDP packets, to reduce latency and quality issues, such as in voice communications. In further embodiments, the remote access client 120 may queue some network packets and discard other network packets. In an additional embodiment, the remote access client 120 may queue the network packets, and discard some or all of the network packets after a predetermined period of time. The remote access client 120 may use the policies 520 to determine which network packets to queue and/or discard. For example, a network packet of a first application 338a may be queued while a network packet of a second application 338n is discarded. In other embodiments, the remote access client 120 may use any network statistics or any network traffic inspection techniques, for example stateful inspection, as known to those skilled in the art to determine whether to queue and/or discard network packets during the disruption.

At step 675 of illustrative method 650, the first portion 605a-605b of the network stack 310a-310b is reestablished while the second portion 610a-610b of the network stack 310a-310b is maintained along with maintaining any desired session or sessions of the second portion 610a-610b of the network stack 310a-310b. The first portion 605a-605b of the network stack 310a-310b may be reestablished by any suitable means and/or mechanisms. For example, the client 105 may reestablish the TCP/IP connection to the network 104, such as by logging into a new network for a roaming mobile client 105. In other embodiments, the remote access client 120, such as via the agent 326 or the filter 322, reestablishes the first portion 605a-605b of the network stack 310a-310b. For example, the agent 326 may initiate and establish a new TCP connection. Upon reestablishing the first portion 605a-605b, the second portion 610a-610b of the network stack 310a-310b is linked with, re-associated with or starts to use or continue to use the

first portion 605a-605b to reestablish the network stack 310a-310b. In some embodiments, the agent 326 may be notified by an event of any network layer that the first portion 605a-605b has been reestablished or in other embodiments, may poll by any predetermined frequency to determine the first portion 605a-605b is reestablished. For example, the agent 326 may check if the TCP connection is active or can be reconnected.

In some embodiments, at step 680, the remote access client 120, such as the agent 326, may automatically re-authenticate the client 105 or a user of the client 105 for the network connection, such as a TCP connection for the first portion 605a-605b of the network stack 610a-610b. For example, the remote access client 120 may automatically re-authenticate the client 105 to a network 104 using any network related credentials of a user of the client 105. Additionally, the remote access client 120 may automatically re-authenticate the client 105 or a user of the client 105 for any session associated with the second portion 610a-610b of the network stack 310a-310b. For example, the SSL session between the agent 326 and the gateway 340 or peer computing device 102c may be re-authenticated.

In another example, an application 338a may be accessing a host service, web server, or application server that uses authentication credentials for access. The agent 326 may automatically re-authenticate the application 338a to the corresponding service or server using application related authentication credentials. In some embodiments, the remote access client 120 may re-authenticate the client and/or user of the client 105 at multiple levels, such as for network access and/or TCP connection, SSL or SSL VPN session, and/or any application level sessions, such as a media interactive user session, for example, a VoIP telephone session. Furthermore, the remote access client 120 may re-authenticate at any time prior to step 685, during step 685, for example, after communicating queued network packets but before continuing other communications, or after step 865, in response to a request to authenticate from a peer computing device, such as a server or the gateway 340.

At step 685 of illustrative method 650, the remote access client 120 of the present invention continues to use the session or sessions of the second portion 610a-610b of the network stack. If any network packets have been queued or remain queued at step 670, the remote access client 120 communicates the queued network packets and continues communicating any network packets of the client 105, such as network

packets generated by or sent to the one more applications 338a-338n of the client 105. As such, the network disruption shielding technique of the present invention provides a seamless and transparent solution to nomadic mobile computing solutions and for generally providing reliable and persistent network connectivity and access.

In the example of a VoIP communications, the illustrative method 650 of the present invention will reduce the number of telephone call drops due to network disruptions and improve the usage of and experience with VoIP. A VoIP user will not need to reconnect the telephone call due to temporary network disruptions in network availability as the remote access client 120 of the present invention will automatically maintain the session and reconnect to the network. Additionally, the remote access client 120 of the present invention will automatically re-authenticate the connection and sessions for providing security after the network disruption. Furthermore, the network shielding technique of the present invention is useful for 1) continuing transactions, commands, or operations automatically through the network disruption, 2) maintaining session related context and cache through the network disruption, and 3) automatically handling change in network address of the client due to changes in the network.

By providing a reliable and persistent connection, the present invention also avoids interruptions to transactions, commands or operations as part of the functionality exercised between the a first computing device 102a and a second computing device 102b, such as client 105a and 105b in Figures 1C. For example, a file copy operation using Windows Explorer has not been designed to continue working after there is a disruption in a network connection. A user on the client 105 may use the file copy feature of Windows Explorer to copy a file from the client 105 to a server 102c. Because of the size of the file or files, this operation may take a relatively extended period of time to complete. If during the middle of the operation of the copy of the file to the server, there is an interruption in the network connection between the client 105 and the server, the file copy will fail. Once the network connection is re-established, the user will need to start another file copy operation from Windows Explorer to copy the file from the client 105 to the server. Under the present invention, the user would not need to start another file copy operation. The network connection would be re-established in accordance with the network disruption shielding technique of the present invention as illustrated in Figure 6B. As such, the file copy of Windows Explorer would not get notified of the interruption in the network connection and therefore, would not

fail. The remote access client 120 would re-establish any connections and transmits any queued data so that operation can continue without failure. The remote access client 120 would maintain a queue of the data related to the file copy operations that has not been transferred to the server because of the interruption in the network connection. Once the network connection is re-established, the remote access client 120 can transmit the queued data and then continue on with transferring the data related to the file copy operation in due course.

Although this aspect of the invention is described in terms of a file copy operation example, one ordinarily skilled in the art will recognize that any operation, transaction, command, function call, etc. transacted between a first computing device 102a and a second computing device 102b, can be maintained and continued without failure from the network connection disruption, and, furthermore, without the client 105 or user of the client 105 recognizing there was a disruption or having notice of the disruption. Additionally, the transaction or operation can be maintained and continued transparently to the application 338, the gateway 340, second computing device 102c, and any part of the second portion 610a-610b of the network stack 310a-310b.

By providing the client 105 with a reliable and persistent connection to a peer computing device 102b or gateway 340, the present invention avoids the process of opening a new user session with an application 338 on the peer, such as a host service on server, by maintaining the user session through network connection interruptions. For each user session between peer computing device, each computing device may maintain session specific context and caches, and other application specific mechanisms related to that instance of the user session. For each new user session established, these session specific context and caches need to be re-populated or re-established to reflect the new user session. For example, a user on the client 105 may have an http session with a server 102c having a web server or web application. The server 102c may keep context specific to providing this instance of the http session with the client 105. The context may be stored in the memory of the server, in files of the server, a database or other component related to providing the functionality of the server 102c. Also, the client 105 may have local context specific to the instance of the http session, such as a mechanism for keeping track of an outstanding request to the web server. This context may be stored in memory of the client 105, in files on the client 105, or other software component interfaced with the client 105. If the connection between the client 105 and

the server 102c is not persistent, then a new user session needs to be established with new session specific context on the server 102c and the client 105. The present invention maintains the session so that a new session, and therefore new specific session context, does not need to be re-established.

The present invention maintains the user session through network level connection interruptions and without notification to the user of the client that the session was interrupted. In operation of this aspect of the invention, the client 105 establishes the connection to the peer computing devices. Via the connection, a session between the client 105 and the server is established. The remote access client 120 can store and maintain any session related information such as authentication credentials, and client 105 and host server 102c context for the established session. Upon detection of a disruption in network connection, the remote access client 120 can re-establish the first portion 605a-605b of the network stack 310a-301b while maintaining the second portion 610a-610b of the network stack. The network connection disruption may cause an interruption to the underlying TCP/IP connection used by the session between the client 105 and the server 102c. However, since the second portion 610a-610b of the network stack 310a-310b is maintained, the session can be re-established and/or continued after the network connection is re-established without the user on the client 105 having notification that the session was interrupted. Thus, the interruption of the session caused by the network connection disruption is effectively hidden from the user using the network disruption shielding techniques of the present invention.

Furthermore, by providing a reliable and persistent connection, the present invention also enables a client 105 to traverse through different network topologies without re-starting a session or an application 338 on the client 105. For example, the client 105 may be a computer notebook with a wireless network connection. As the client 105 moves from a first wireless network to a second wireless network, the client's network connection may be temporarily disrupted from the first wireless network as a network connection is established with the second wireless network. The second wireless network may assign a new network identifier, such as a host name or internet protocol address, to the client 105. This new network identifier may be different than the network identifier assigned to the client 105 by the first wireless network. In another example, the client 105 may be physically connected through an Ethernet cable to a port on the network. The physical connection may be unplugged and the client 105 moved to

another location to plug into a different port on the network. This would cause a disruption into the network connection and possibly a change in the assigned network identifier. Without the present invention, any sessions between peer computing devices may need to be restarted due to the change in the network topology, the disruption to the network connection, and/or the change in the assigned network identifier. By the method and systems described herein, the remote access client 120 of the present invention maintains the network connection for the client and automatically re-established the client's 105 network connection including handling changes in the network topology and network identifier. The client 105, and any applications or sessions on the client 105, can continue to operate as if there was not a network connection disruption or a change in the network identifier. Furthermore, the user on the client 105 may not recognize there were any interruptions or changes, and the client 105 may not receive any notice of such interruptions.

In an additional aspect, any of the techniques of the present invention, such as the illustrative methods of Figures 2B, 3B, 3C, 4, 5B and 6B, can be practiced in one or more combinations with each other. In one embodiment, the peer-to-peer routing technique may be practiced with the false acknowledgement and/or MTU adjustment techniques. This would provide a client communicating real-time data, such as VoIP, to connect to the peer via a more optimal and direct route and to communicate the real-time data via UDP over a secure SSL/TCP/IP connection, while avoiding any latency due to any reliability mechanism of TCP and reduce fragmentation due to the encryption overhead. Additionally, this embodiment may be further combined with the client-side application-aware prioritization technique and/or the network disruption shielding technique. As such, the secure real-time data communications can be communicated from the client at higher priorities than other applications of the client to improve the quality of the real-time experience, such as VoIP. The network disruption technique would allow a mobile VoIP phone, such as a soft phone of a notebook, roam between network access points and automatically continue with the session.

The techniques of the present invention are complimentary to each other for network communication optimizations, such as for example in VoIP communications over a SSL VPN gateway. As such, each of the 1) peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and 5) the network

disruption shielding technique of the present invention may be practiced with one or more of the following techniques and optimization of the present invention: 1) the peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and/or 5) the network disruption shielding technique.

In one further illustrative example of the present invention, an online meeting, collaboration and/or desktop sharing service, such as the hosted service of GoToMeeting.com, WebEx.com,or LiveMeeting.com may use the techniques of the present invention in one or more combinations. The host service may use a gateway 340, and the techniques of illustrative method 260 to facilitate a peer-to-peer connection between a first computing device of a meeting presenter and a second computing device of a meeting attendee. The computing devices of the meeting presenter and attendees may download via the host service the remote access client 120, or any portions thereof. Once the meeting presenter and the meeting attendee establish a peer-to-peer connection, the peer computing devices may use any of the optimization techniques of the present invention to optimize their communications, such as the MTU adjustment technique, client-side application aware technique, or the network disruption shielding technique. Along with the peer-to-peer routing, the optimization techniques of the present invention, will improve the performance, efficiency and user experience of the online meeting, collaboration, or desktop sharing.

In yet a further aspect and in view of Figure 2A, for example, the remote access client 120 of the present invention can distribute Dynamic Host Configuration Protocol (DHCP) IP addresses of the client 105 or the publicly visible IP addresses to the telecommunication device 210a-210b, such as either a hardware or software based VoIP telephone. The gateway 340 of the present invention facilitates the discovery of the public IP addresses of the client, such as client 105b illustrated in Figure 2A. As such, the techniques of the present invention enables protocols that communicate their IP address over the protocol to continue to function.

Many alterations and modifications may be made by those having ordinary skill in the art without departing from the spirit and scope of the invention. Therefore, it must be expressly understood that the illustrated embodiments have been shown only for the purposes of example and should not be taken as limiting the invention, which is defined by the following claims. These claims are to be read as including what they set forth

literally and also those equivalent elements which are insubstantially different, even though not identical in other respects to what is shown and described in the above illustrations.

We claim:

1. A method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device;

(b) initiating, by the first computing device, a communication session to the second computing device via the third computing device;

(c) receiving, by a server, a signal to establish the communication session;

(d) communicating, by the server, to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) communicating, by the first computing device, a request to initiate a connection with the second computing device using the first network address;

(f) intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating, by the third computing device, a request to the second computing device to allow a connection from the first computing device using the second network address.

2. The method of claim 1, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network

3. The method of claim 1, wherein the third computing device comprises a remote access gateway.

4. The method of claim 1, wherein the second computing device is located behind a firewall associated with the second network address.

5. The method of claim 1, comprising providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

6. The method of claim 1, comprising providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

7. The method of claim 1, comprising communicating, by the third computing device, a key to the first computing device and the second computing device.

8. The method of claim 7, comprising communicating, by the first computing device, the key to the second computing device.

9. The method of claim 8, comprising checking, by the first computing device, that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

10. The method of claim 7, comprising communicating, by the second computing device, the key to the first computing device.

11. The method of claim 10, comprising checking, by the second computing device, that the key received from the first computing device matches the key of the second computing device before transmitting data to the second computing device.

12. The method of claim 1, associating a first telecommunication device with the first computing device, and associating a second telecommunication device with the second computing device.

13. The method of claim 12, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

14. The method of claim 12, comprising establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection.

15. The method of claim 15, comprising communicating between the first telecommunication device and the second telecommunication device over the telecommunication session without traversing the to the first computing device

16. The method of claim 1, comprising communicating a remote display protocol via the connection between the first computing device and the second computing device.

17. The method of claim 16, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

18. The method of claim 1, comprising sharing a screen view of the first computing device with the second computing device via the connection.

19. In a gateway, a method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing a first tunneling session with the first computing device on a first network;

(b) establishing a second tunneling session with the second computing device on the second network;

(c) receiving a request by the first computing device to initiate a communication session with the second computing device;

(d) providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

(f) intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

20. The method of claim 19, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

21. The method of claim 19, wherein the second computing device is located behind a firewall associated with the second network address.

22. The method of claim 19, comprising providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

23. The method of claim 19, comprising communicating a key to the first computing device.

24. The method of claim 19, comprising communicating a key to the second computing device.

25. A system for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device, the first network disconnected from and not routable to the second network, the system comprising:

a first computing device on the first network;

a second computing device on the second network;

a third computing device establishing a first tunneling session with the first computing device and a second tunneling session with the second computing device;

a server accessible via the third computing device;

wherein:

the server communicates via the third computing device to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

the first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address;

the third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

the third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

26. The system of claim 25, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

27. The system of claim 25, wherein the third computing device comprises a remote access gateway.

28. The system of claim 25, wherein the second computing device is located behind a firewall associated with the second network address.

29. The system of claim 25, wherein the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session.

30. The system of claim 25, wherein the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

31. The system of claim 25, wherein the third computing device communicates a key to the first computing device and the second computing device.

32. The system of claim 31, wherein the first computing device communicates the key to the second computing device.

33. The system of claim 32, wherein the first computing device checks that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

34. The system of claim 31, wherein the second computing device communicates the key to the first computing device.

35. The system of claim 34, wherein the second computing device checks that the key received from the first computing devices matches the key of the second computing device before transmitting data to the second computing device.

36. The system of claim 25, comprising a first telecommunication device associated with the first computing device, and a second telecommunication associated with the second computing device.

37. The system of claim 36, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

38. The system of claim 37, wherein the first telecommunication device establishes a telecommunication session with the second telecommunication device via the connection.

39. The system of claim 38, wherein the first telecommunication device communicates with the second telecommunication device over the telecommunication session without traversing the third computing device.

40. The system of claim 25, wherein the first computing device and the second computing device communicate a remote display protocol via the connection.

41. The system of claim 25, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

42. The system of claim 25, wherein the first computing device shares a screen view with the second computing device via the connection.

43. A gateway for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the gateway comprising:

a means for establishing a first tunneling session with the first computing device on a first network;

a means for establishing a second tunneling session with the second computing device on the second network;

a means for receiving a request by the first computing device to initiate a communication session with the second computing device;

a means for providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

a means for receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

a means for intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

a means for communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

44. The system of claim 43, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

45. The system of claim 43, wherein the second computing device is located behind a firewall associated with the second network address.

46. The system of claim 43, comprising a means for providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

47. The system of claim 43, comprising a means for communicating a key to the first computing device.

48. The system of claim 43, comprising a means for communicating a key to the second computing device.

49. A method for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the method comprising the steps of:

(a) establishing a connection between a first computing device and a second computing device via a lossless protocol;

(b) detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

(c) communicating, by the first computing device, a false acknowledgement of receipt of
the lossless protocol packet to one of the first computing device or the second computing device; and

(d) communicating, by the first computing device, the lossless protocol packet to the second computing device.

50. The method of claim 49, comprising encrypting, by the first computing device, the one or more packets using a key.

51. The method of claim 50, comprising providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

52. The method of claim 49, comprising encrypting the one or more packets on a packet by packet basis.

53. The method of claim 49, further comprising performing step (c) before step (d).

54. The method of claim 49, wherein the second computing device is a gateway.

55. The method of claim 49, comprising, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

56. The method of claim 49, wherein the lossless protocol comprises a transport control protocol.

57. The method of claim 56, comprising preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, a flow control algorithm, a naple's algorithm, and a sliding window algorithm.

58. The method of claim 49, wherein the lossy protocol comprises a user datagram protocol.

59. The method of claim 49, comprising communicating, by the first computing device, the
lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to
the second computing device.

60. The method of claim 49, wherein the one or more packets comprises a real-time protocol.

61. The method of claim 49, comprising communicating by the first computing device one of
real-time voice, audio, or data to the second computing device via the one or more packets.

62. A system for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the system comprising:

a means for establishing a connection between a first computing device and a second computing device via a lossless protocol;

a means for detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

a means for communicating, by the first computing device, a false acknowledgement of receipt of the lossless protocol packet to one of the first computing device or the second computing device; and

a means for communicating, by the first computing device, the lossless protocol packet to the second computing device.

63. The system of claim 62, comprising a means for encrypting, by the first computing device, the one or more packets using a key.

64. The system of claim 63, comprising a means for providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

65. The system of claim 63, comprising a means for encrypting the one or more protocol packets on a packet by packet basis.

66. The system of claim 62, further comprising a means for communicating the false acknowledgement of receipt of the lossless protocol packet before communicating the

lossless protocol packet.

67. The system of claim 62, wherein the second computing device is a gateway.

68. The system of claim 62, comprising a means, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, for preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

69. The system of claim 62, wherein the lossless protocol comprises a transport control protocol.

70. The system of claim 69, comprising a means for preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, and a flow control algorithm.

71. The system of claim 62, wherein the lossy protocol comprises a user datagram protocol.

72. The system of claim 62, comprising a means for communicating, by the first computing device, the lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to the second computing device.

73. The system of claim 62, wherein the one or more packets comprises a real-time protocol.

74. The system of claim 62, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

75. A method for transmitting packets from an application using an unreliable

transport protocol over a TCP connection, comprising:

receiving, at a first device, a first packet to be transmitted using an unreliable transport protocol;

creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device;

transmitting, by the first device, the first TCP packet to the second device;

receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol;

creating a second TCP packet including a second payload of the received second packet and the first TCP header information; and

transmitting, by the first device, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

76. The method of claim 75, comprising establishing the TCP connection with a port number associated with the unreliable transport protocol.

77. The method of claim 75, comprising dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol.

78. The method of claim 75, wherein the unreliable transport protocol is UDP.

79. The method of claim 75, comprising further:

receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism.

80. The method of claim 75, comprising establishing, by the first device, the TCP connection with a VPN gateway device.

81. The method of claim 75, comprising establishing peer-to-peer communications between the first device and the second device via the TCP connection.

82. The method of claim 75, comprising encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

83. A method for transmitting packets from an application using an unreliable transport protocol over a TCP connection, comprising:

intercepting, at a second device, a first TCP packet created on a first device and received on the second device, the first TCP packet including a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device, the intercepting occurring before the first TCP packet is provides to a TCP stack on the second device;

identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable transport protocol;

stripping the TCP header of information from the first TCP packet; and

forwarding the first payload to an application using the unreliable data protocol.

84. The method of claim 83, wherein the unreliable protocol is UDP.

85. The method of claim 83, wherein the step of identifying comprises identifying the TCP header information includes a port number associated with the unreliable transport protocol.

86. The method of claim 83, comprising further:

intercepting, by the second device, the first TCP packet using a packet capture driver.

87. The method of claim 83, wherein the first device is a client device and the

second device is a VPN gateway.

88. The method of claim 87, comprising further:
performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

89. A system for transmitting packets from an application using an unreliable transport protocol over a TCP connection, the system comprising:
a first device, the first device comprising:
an application generating a first and second packet, the first and second packet intended to be transmitted using an unreliable transport protocol;
a filter process, the filter process intercepting the first and second packets from the application and forwarding the intercepted packets to a tunnel process; and
a tunnel process, the tunnel process requesting the opening of a TCP connection between the first device and a second device, the request to open the TCP connection indicating to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol, the tunnel process forwarding the first and second packets as payloads in a first and second TCP packet to the second device, the tunnel process sending the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet ; and
a second device in communication with the first device, the second device comprising:
a second tunnel process opening the TCP connection requested by the first device, the second tunnel process identifying and forwarding the source address of the TCP connection to a second filter process; and
the second filter process, the second filter process intercepting packets from the application received at the second device with the TCP connection source address in a header, the second filter process stripping the TCP header from the received packets and forwarding the stripped packets,

circumventing the TCP/IP stack on the second device, to an intended destination.

90. The system of claim 89, wherein the filter process on the first device comprises a packet capture driver.

91. The system of claim 89, wherein the second filter process on the second device comprises a packet capture driver.

92. The system of claim 89, wherein the first device is a client device and the second device is a VPN gateway device.

93. The system of claim 89, further comprising:
a third device to which the stripped packets are transmitted.

94. The system of claim 93, wherein the second device comprises further:
a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to a third device.

95. The system of claim 89, wherein the unreliable data protocol is UDP.

96. A method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the method comprising the steps of:

(a) establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

(b) detecting, by the first computing device, a network packet having an encrypted payload;

(c) determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

(d) altering the maximum transmission unit parameter of the first network stack to the determined setting.

97. The method of claim 96, comprising communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

98. The method of claim 96, wherein the payload comprises a real-time protocol.

99. The method of claim 96, further comprising altering the maximum transmission unit parameter via a network driver interface specification level mechanism of the first network stack

100. The method of claim 96, further comprising determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

101. The method of claim 96, comprising establishing the session between the first computing device and the second computing device via a gateway.

102. The method of claim 96, communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

103. The method of claim 96, comprising communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

104. The method of claim 96, further comprising establishing the session between the first computing device and the second computing device via an agent of the first computing device.

105. The method of claim 104, comprising communicating, by the agent, via an IOCTL application programming interface to the first network stack to alter the

maximum transmission unit parameter to the determined setting.

106. A system for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the system comprising:

a means for establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

a means for detecting, by the first computing device, a network packet having an encrypted payload;

a means for determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

a means for altering the maximum transmission unit parameter of the first network stack to the determined setting.

107. The system of claim 106, comprising a means for communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

108. The system of claim 106, wherein the payload comprises a real-time protocol.

109. The system of claim 106, wherein the payload comprises a representation of one of real-time voice, audio, or data.

110. The system of claim 106, further comprising a means for altering the maximum transmission unit parameter of the first computing device via a network driver interface specification level mechanism of the first network stack

111. The system of claim 106, further comprising a means for determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

112. The system of claim 106, comprising a means for establishing the session

between the first computing device and the second computing device via a gateway.

113. The system of claim 106, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

114. The system of claim 106, comprising a means for communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

115. The system of claim 106, wherein the network packet comprises a lossless protocol packet.

116. The system of claim 115, wherein the lossless protocol packet comprises a transport control protocol.

117. The system of claim 106, wherein the payload comprises a lossy protocol packet.

118. The system of claim 117, wherein the lossy protocol packet comprises a user datagram protocol.

119. The system of claim 106, comprising an agent of the first computing device for establishing the session between the first computing device and the second computing device.

120. The system of claim 119, wherein the agent communicates via an IOCTL application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

121. A method for a client to prioritize network communications of the client associated with an application of the client, the method comprising the steps of:

(a) intercepting, by the client, one or more network packets associated with one or more applications of the client;

(b) storing, by the client, the one or more network packets to a queue;

(c) determining, by the client, the queued one or more network packets is associated with a first application of the client;

(d) indicating, by the client, a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client; and

(e) providing the prioritized one or more network packets for communications via a network stack of the client.

122. The method of claim 121, wherein the step of determining, by the client, further comprises determining the queued one or more networks packets of the first application comprises real-time data.

123. The method of claim 122, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

124. The method of claim 121, comprising preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

125. The method of claim 121, comprising holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

126. The method of claim 121, comprising intercepting, by the client, the one or more network packets transparently to the one or more applications on the client.

127. The method of claim 121, comprising running the first application in the foreground, and the second application in the background.

128. The method of claim 121, comprising associating a priority with the first

application higher than a priority associated with the second application.

129. The method of claim 128, comprising specifying, by a user, the priority of one of the first application or the second application.

130. The method of claim 121, comprising receiving, by the client, the one or more network packets from a computing device.

131. The method of claim 121, comprising providing, by the one or more applications, the one or more network packets for communicating from the client to a computing device.

132. A client for prioritizing network communications of the client associated with an application of the client, the client comprising:

a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client, and

a network driver for storing the one or more networks packets to a queue and communicating the one or more network packets via a network stack of the client; and

an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

133. The client of claim 132, wherein the agent determines the one or more networks packets of the first application comprises real-time data.

134. The client of claim 132, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

135. The client of claim 132, wherein one of the agent or the network driver prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

136. The client of claim 132, wherein the network driver holds in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

137. The client of claim 132, wherein the mechanism intercepts the one or more network packets transparently to the one or more applications on the client.

138. The client of claim 132, wherein the first application is running in the foreground, and the second application is running in the background.

139. The client of claim 132, wherein the first application has a priority higher than the second application of the client.

140. The client of claim 132, comprising a configuration mechanism for a user to specify the priority.

141. The client of claim 132, wherein the client receives the one or more network packets from a computing device.

142. The client of claim 132, wherein the one or more applications provides the one or more network packets for communicating from the client to a computing device.

143. The client of claim 132, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

144. The client of claim 132, wherein the network driver operates in kernel-mode of an operating system of the client.

145. The client of claim 132, wherein the agent operates in user-mode of an operating system of the client.

146. The client of claim 132, wherein one of the agent or the network driver comprises the mechanism for intercepting one or more network packets of the client.

147. A method for shielding from a network disruption a session established via a first protocol, the method comprising the steps of:

(a) establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device, the network connection associated with a network stack, a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol;

(b) detecting a disruption in the network connection causing the first portion of the network stack to be disestablished;

(c) maintaining, by the agent, the session and the second portion of the network stack during the disruption; and

(d) re-establishing the second portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

148. The method of claim 147, comprising the step of:

(e) continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

149. The method of claim 147, comprising the step of

(e) dropping, by the second portion of the network stack, any network packets received

during the disruption.

150. The method of claim 147, wherein the device comprises one of a remote access gateway or a computing device.

151. The method of claim 147, further comprising establishing the session via the first protocol of one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

152. The method of claim 147, comprising communicating, by the agent, real-time data via the session between the client and the device.

153. The method of claim 152, wherein the real-time data comprises a real-time protocol.

154. The method of claim 152, wherein the real-time data comprises a representation of one of voice or audio.

155. The method of claim 147, comprising operating the agent in user-mode of an operating system of the client.

156. The method of claim 147, wherein the first portion of the network comprises one of a transport control protocol or an internet protocol.

157. The method of claim 147, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

158. The method of claim 147, comprising the client communicating with the device via a remote display protocol.

159. The method of claim 158, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

160. The method of claim 147, comprising performing one of steps (b), (c) and (d) transparently to an application of the client communicating via the network connection.

161. The method of claim 147, comprising intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application.

162. The method of claim 147, comprising intercepting, by a network driver

associated with the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

163. A system for shielding from a network disruption a session established via a first protocol, the system comprising

an agent of a client establishing a session between the client and a device over a network connection via a first protocol;

a network stack having a first portion and a second portion, the first portion of the network stack comprising one or more layers of the network stack below the layer of the first protocol, and the second portion of the network stack comprising a layer for the first protocol and one or more layers of the network stack above the first protocol; and

a detector for detecting a disruption in the network connection causing the second portion of the network stack to be disestablished;

wherein:

upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption; and

the client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

164. The system of claim 163, wherein the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

165. The system of claim 163, wherein one of the first portion or the second portion of the network stack drops any network packets received during the disruption.

166. The system of claim 163, wherein the device comprises one of a remote access gateway or a computing device.

167. The system of claim 163, wherein the first protocol comprises one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

168. The system of claim 163, wherein the agent communicates real-time data via the session between the client and the device.

169. The system of claim 168, wherein the real-time data comprises one of a real-time protocol.

170. The system of claim 168, wherein the real-time data comprises a representation of one of voice or audio.

171. The system of claim 163, wherein the agent operates in user-mode of an operating system of the client.

172. The system of claim 163, wherein the first portion of the network stack comprises one of a transport control protocol or an internet protocol.

173. The system of claim 163, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

174. The system of claim 163, wherein the first protocol comprises a remote display protocol.

175. The system of claim 174, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

176. The system of claim 163, wherein the agent intercepts one or more network packets of an application of the client transparently to the application.

177. The system of claim 163, comprising a network driver associated with the second portion of the network stack, the network driver intercepts one or more network packets of an application of the client transparently to the application, and provides the one or more packets to the agent to communicate via the session.

178. The system of claim 177, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

179. The system of claim 177, wherein the network driver operates in kernel-mode of an operating system of the client.

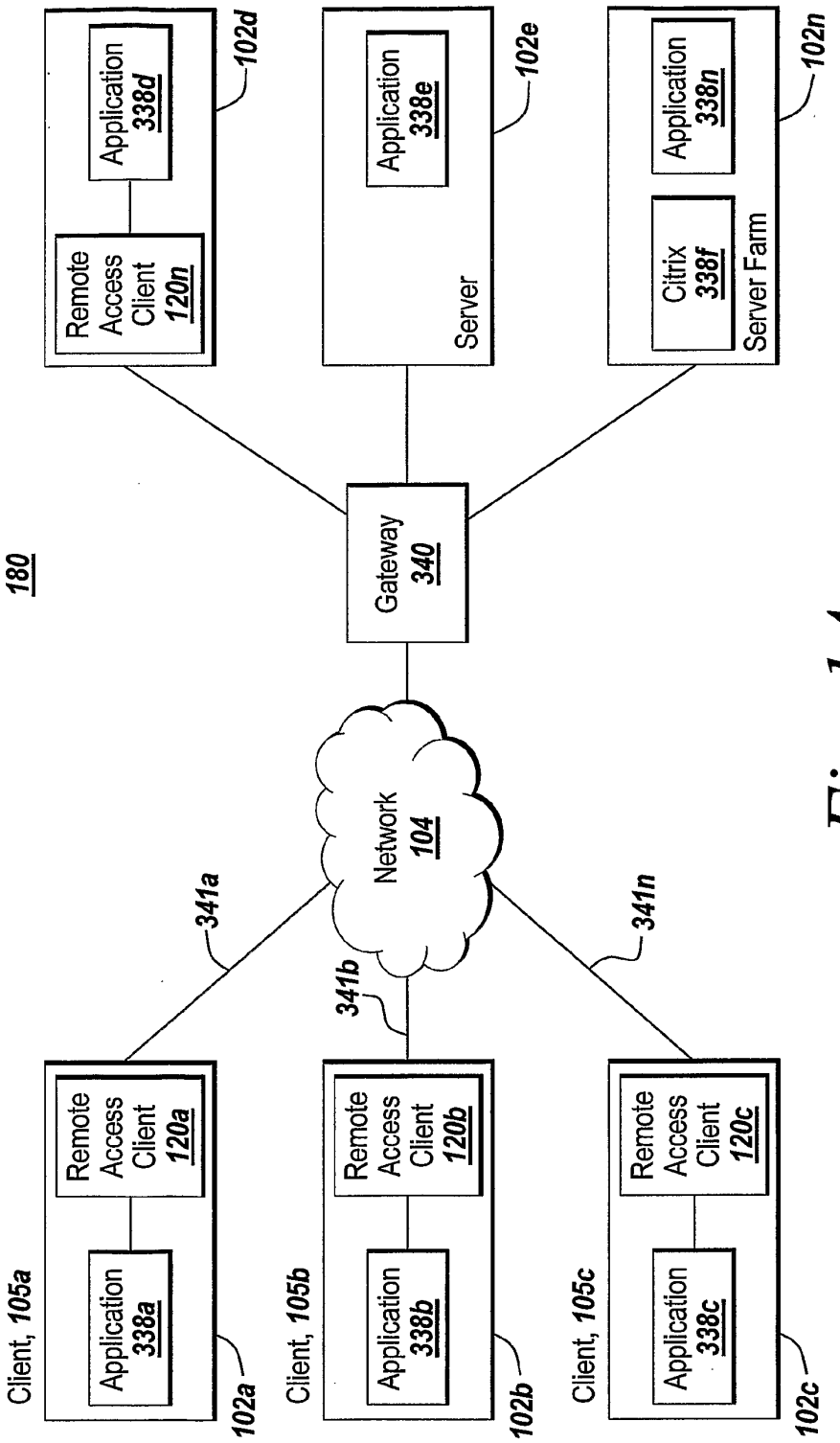

180
Client, 105a
Application 338a
Remote Access Client 120a
102a
341a
Client, 105b
Application 338b
Remote Access Client 120b
102b
341b
Client, 105c
Application 338c
Remote Access Client 120c
102c
341n
Network 104
Gateway 340
Remote Access Client 120n
Application 338d
102d
Server
Application 338e
102e
Server Farm
Citrix 338f
Application 338n
102n

Fig. 1A

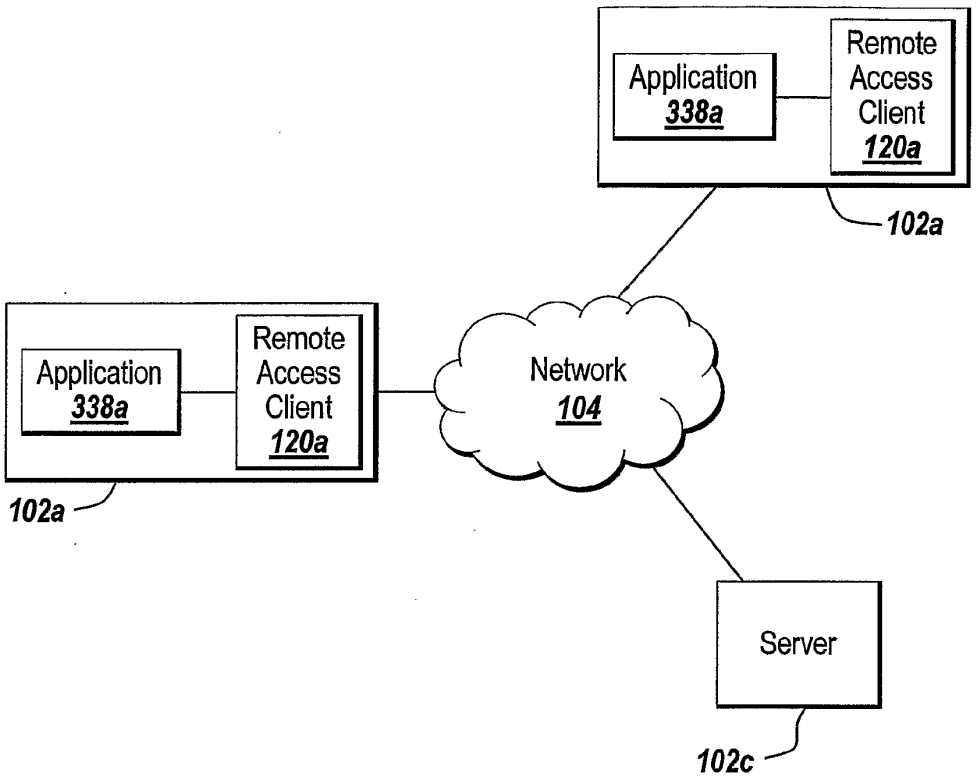

Application
338a
Remote
Access
Client
120a
102a
Application
338a
Remote
Access
Client
120a
102a
Network
104
Server
102c

Fig. 1B

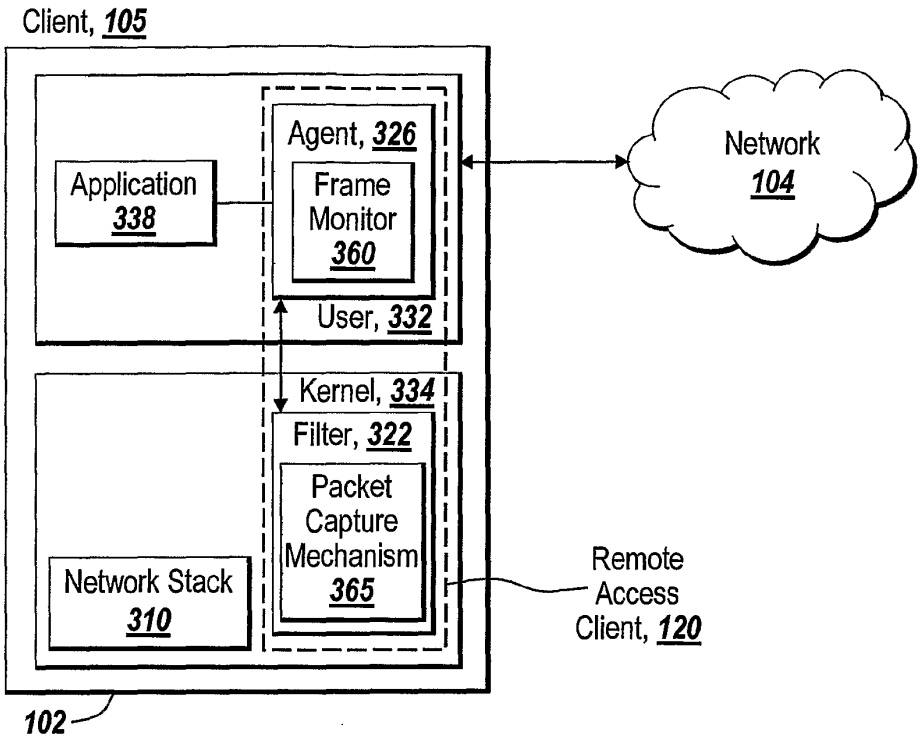

Client, 105
Agent, 326
Application 338
Frame Monitor 360
User, 332
Kernel, 334
Filter, 322
Packet Capture Mechanism 365
Network Stack 310
Network 104
Remote Access Client, 120
102

Fig. 1C

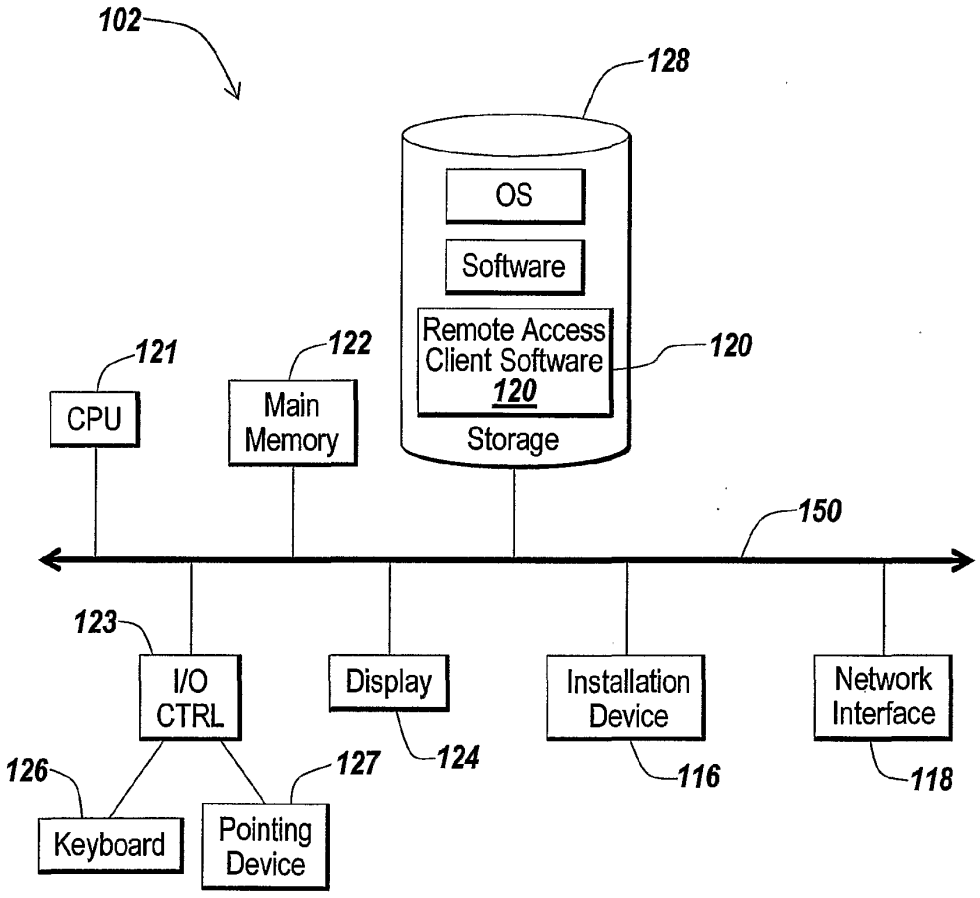

102
128
OS
Software
Remote Access Client Software
120
120
Storage
121
CPU
122
Main Memory
150
123
I/O CTRL
Display
124
Installation Device
116
Network Interface
118
126
Keyboard
127
Pointing Device

Fig. 1D

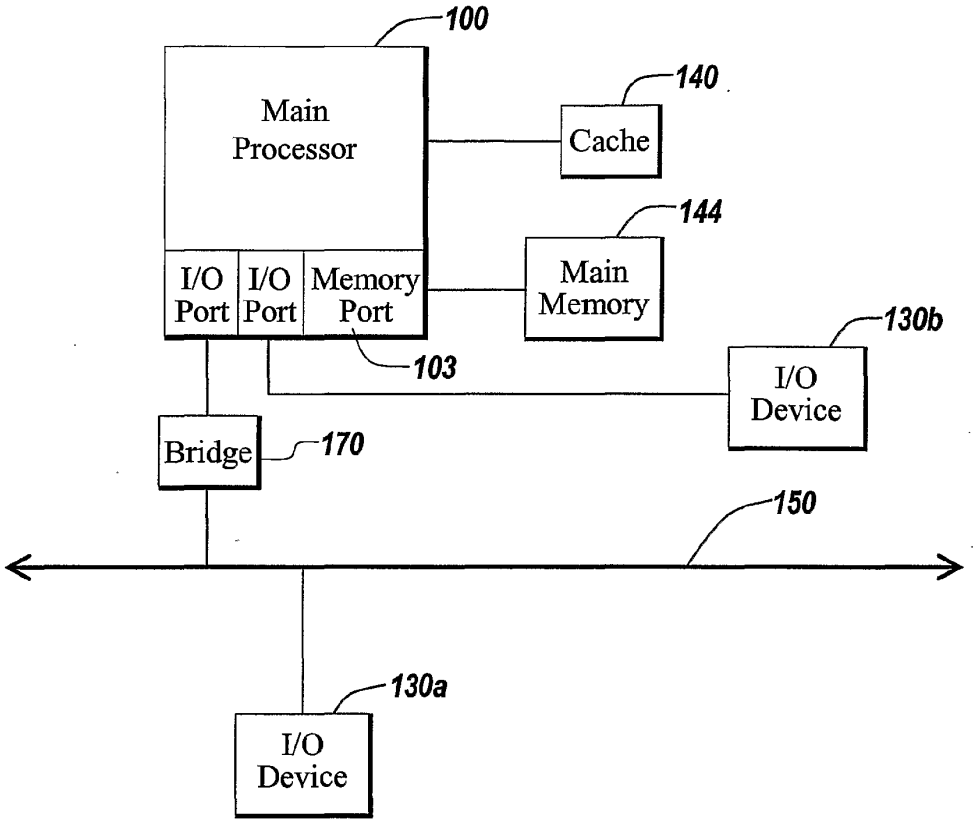

100
Main Processor
140
Cache
144
Main Memory
I/O Port
I/O Port
Memory Port
103
130b
I/O Device
Bridge
170
150
130a
I/O Device

Fig. 1E

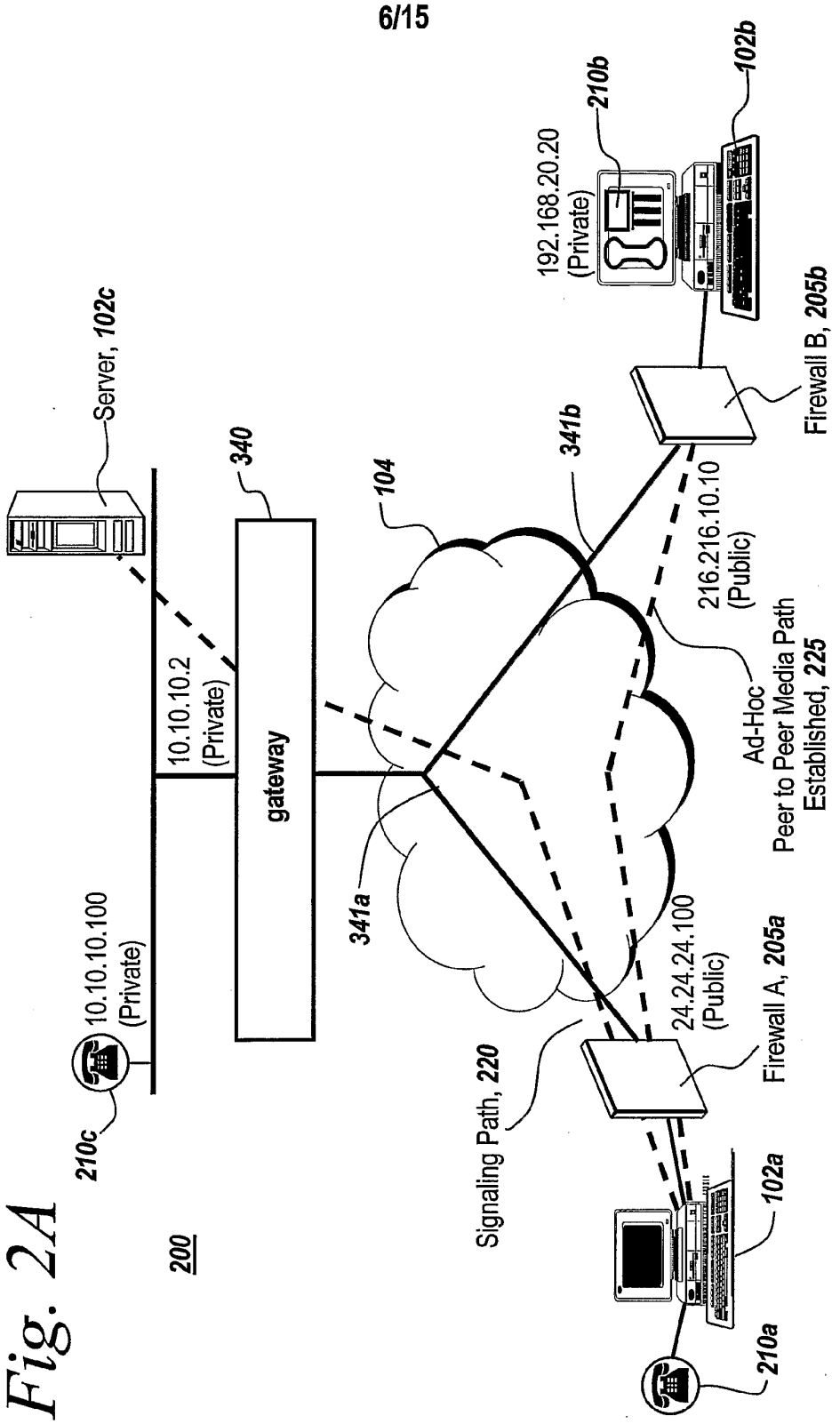

Server, 102c
340
104
341b
192.168.20.20
(Private)
210b
102b
10.10.10.2
(Private)
gateway
216.216.10.10
(Public)
Ad-Hoc
Peer to Peer Media Path
Established, 225
Firewall B, 205b
10.10.10.100
(Private)
341a
24.24.24.100
(Public)
Signaling Path, 220
Firewall A, 205a
210c
200
102a
210a

Fig. 2A

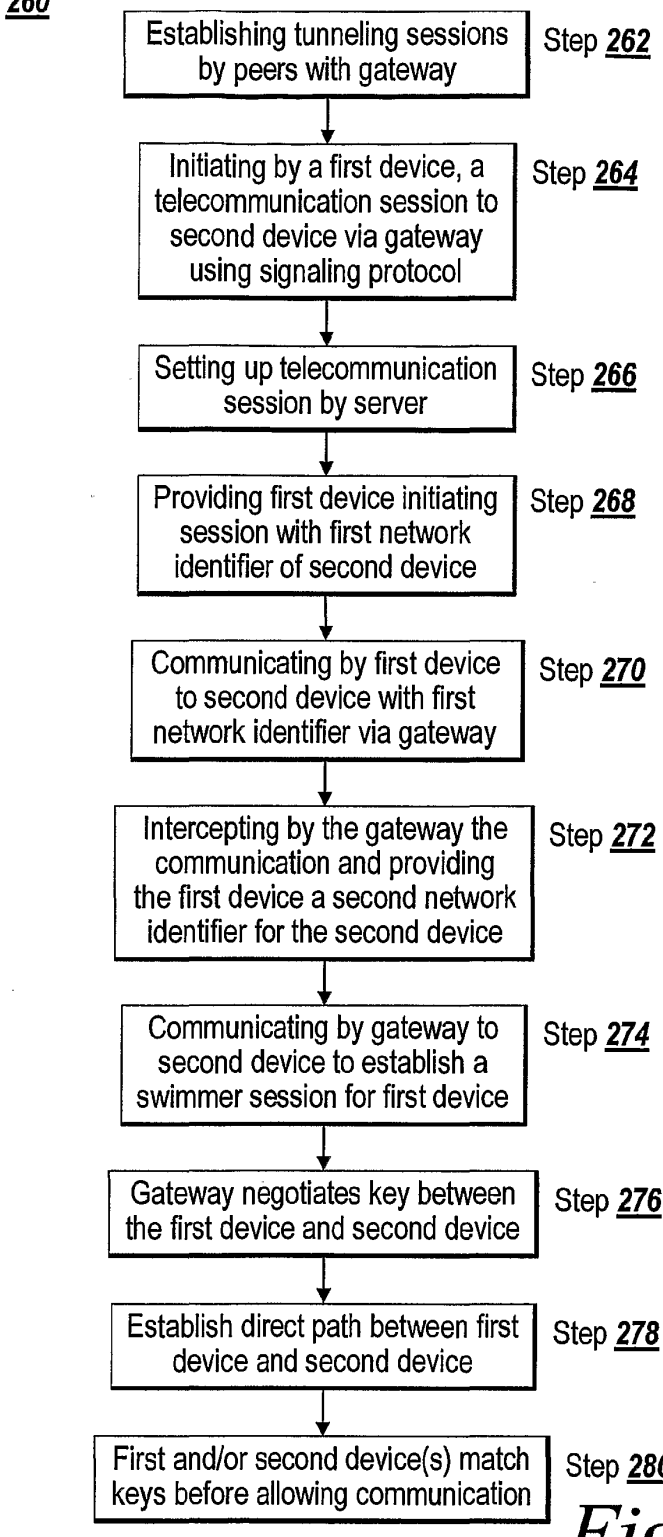

260
Establishing tunneling sessions by peers with gateway
Step 262
Initiating by a first device, a telecommunication session to second device via gateway using signaling protocol
Step 264
Setting up telecommunication session by server
Step 266
Providing first device initiating session with first network identifier of second device
Step 268
Communicating by first device to second device with first network identifier via gateway
Step 270
Intercepting by the gateway the communication and providing the first device a second network identifier for the second device
Step 272
Communicating by gateway to second device to establish a swimmer session for first device
Step 274
Gateway negotiates key between the first device and second device
Step 276
Establish direct path between first device and second device
Step 278
First and/or second device(s) match keys before allowing communication
Step 280

Fig. 2B

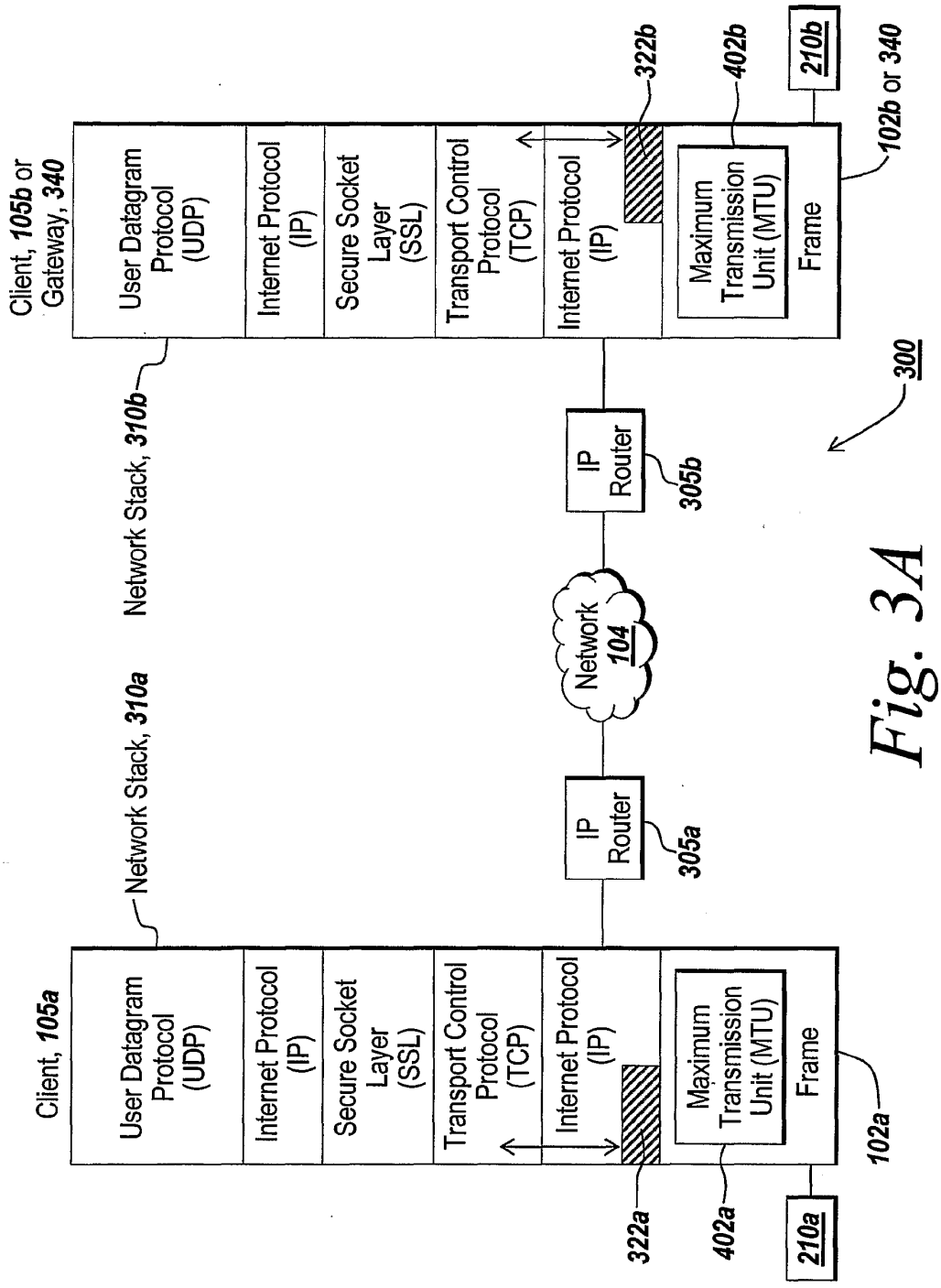

Client, 105a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
Network Stack, 310a
Network Stack, 310b
Client, 105b or Gateway, 340
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
IP Router
305a
IP Router
305b
Network 104
300
322a
402a
210a
102a
322b
402b
210b
102b or 340

Fig. 3A

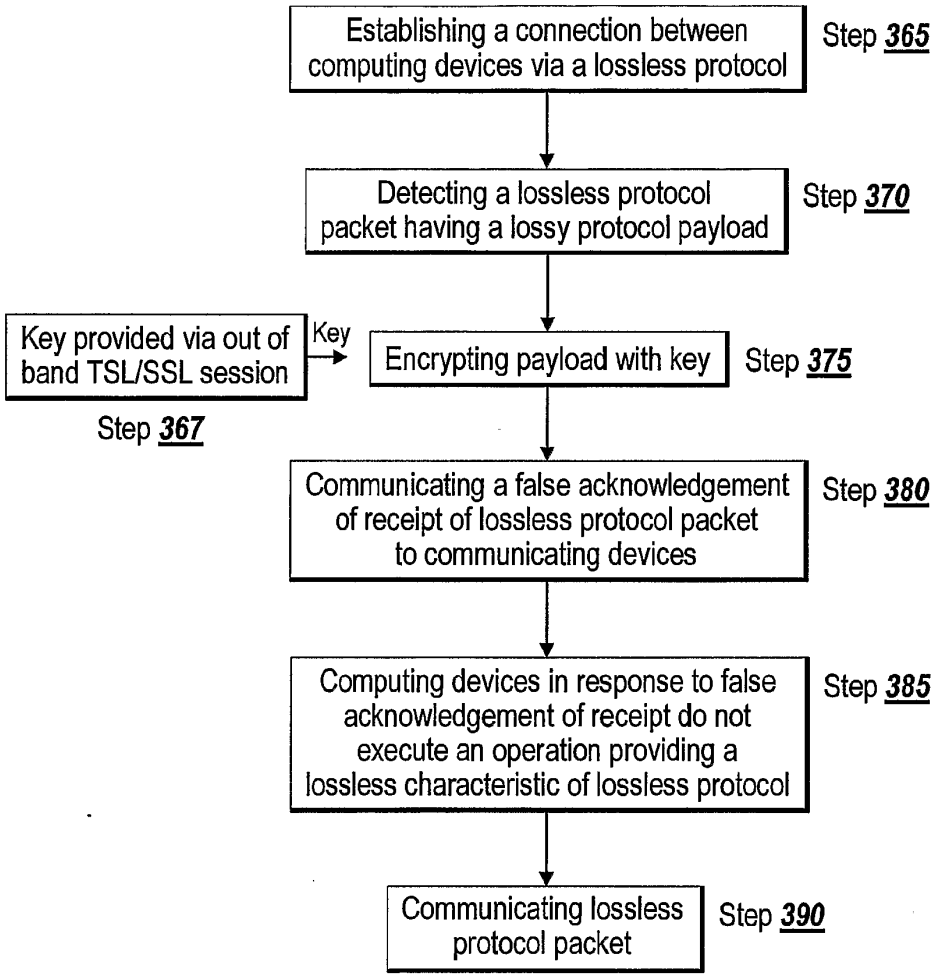

Establishing a connection between computing devices via a lossless protocol
Step 365
Detecting a lossless protocol packet having a lossy protocol payload
Step 370
Key provided via out of band TSL/SSL session
Key
Encrypting payload with key
Step 375
Step 367
Communicating a false acknowledgement of receipt of lossless protocol packet to communicating devices
Step 380
Computing devices in response to false acknowledgement of receipt do not execute an operation providing a lossless characteristic of lossless protocol
Step 385
Communicating lossless protocol packet
Step 390

Fig. 3B

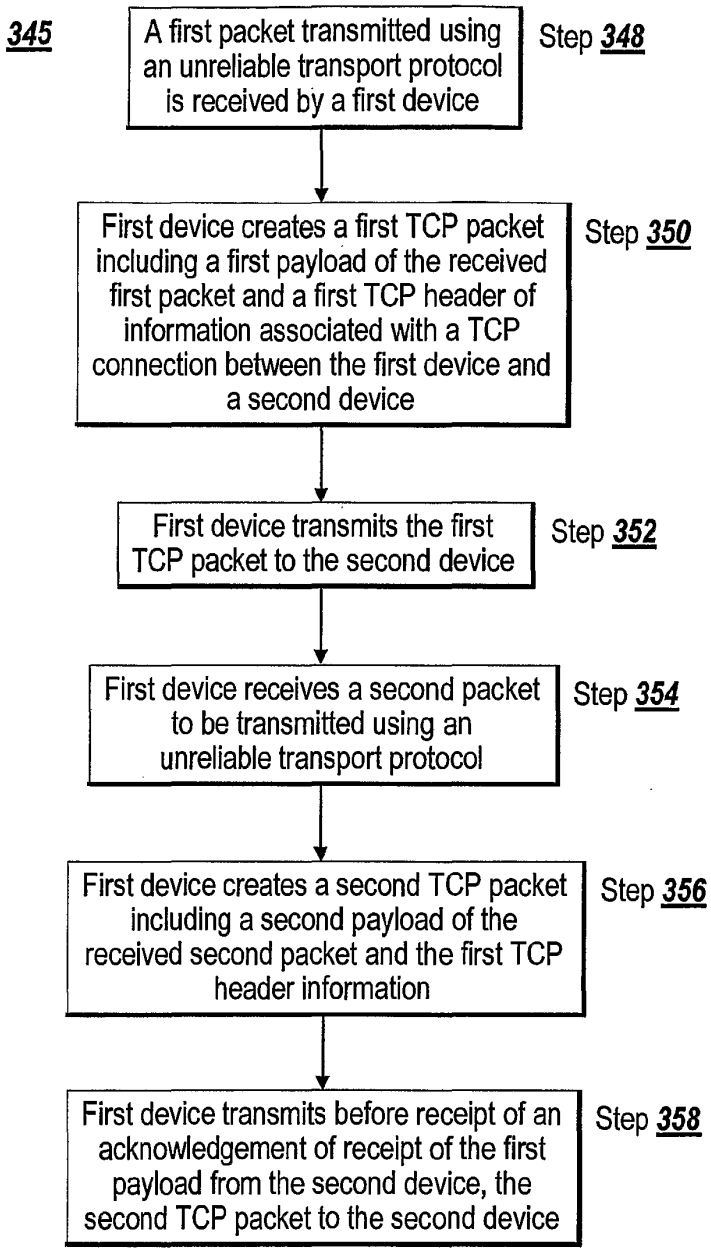

345
A first packet transmitted using an unreliable transport protocol is received by a first device
Step 348
First device creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection between the first device and a second device
Step 350
First device transmits the first TCP packet to the second device
Step 352
First device receives a second packet to be transmitted using an unreliable transport protocol
Step 354
First device creates a second TCP packet including a second payload of the received second packet and the first TCP header information
Step 356
First device transmits before receipt of an acknowledgement of receipt of the first payload from the second device, the second TCP packet to the second device
Step 358

Fig. 3C

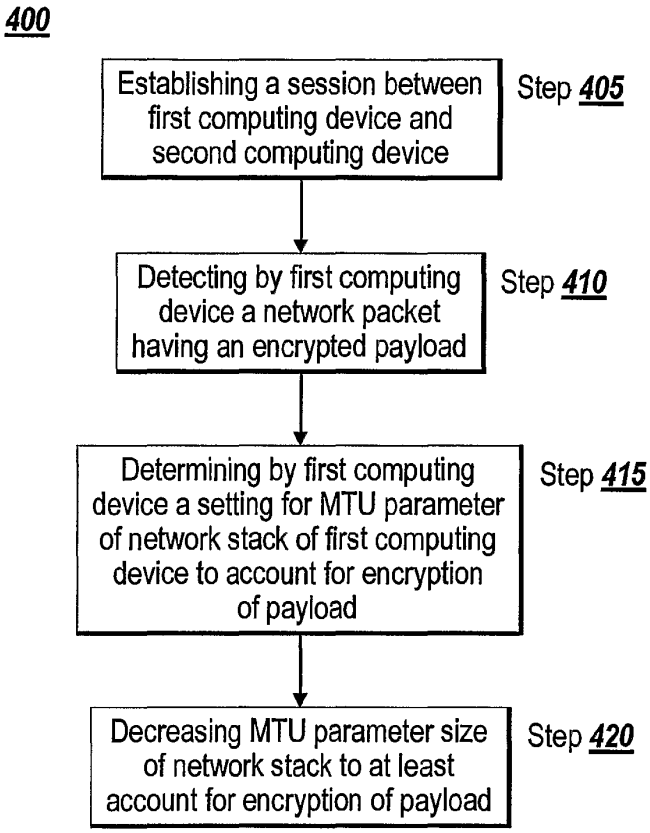

400
Establishing a session between first computing device and second computing device
Step 405
Detecting by first computing device a network packet having an encrypted payload
Step 410
Determining by first computing device a setting for MTU parameter of network stack of first computing device to account for encryption of payload
Step 415
Decreasing MTU parameter size of network stack to at least account for encryption of payload
Step 420

Fig. 4

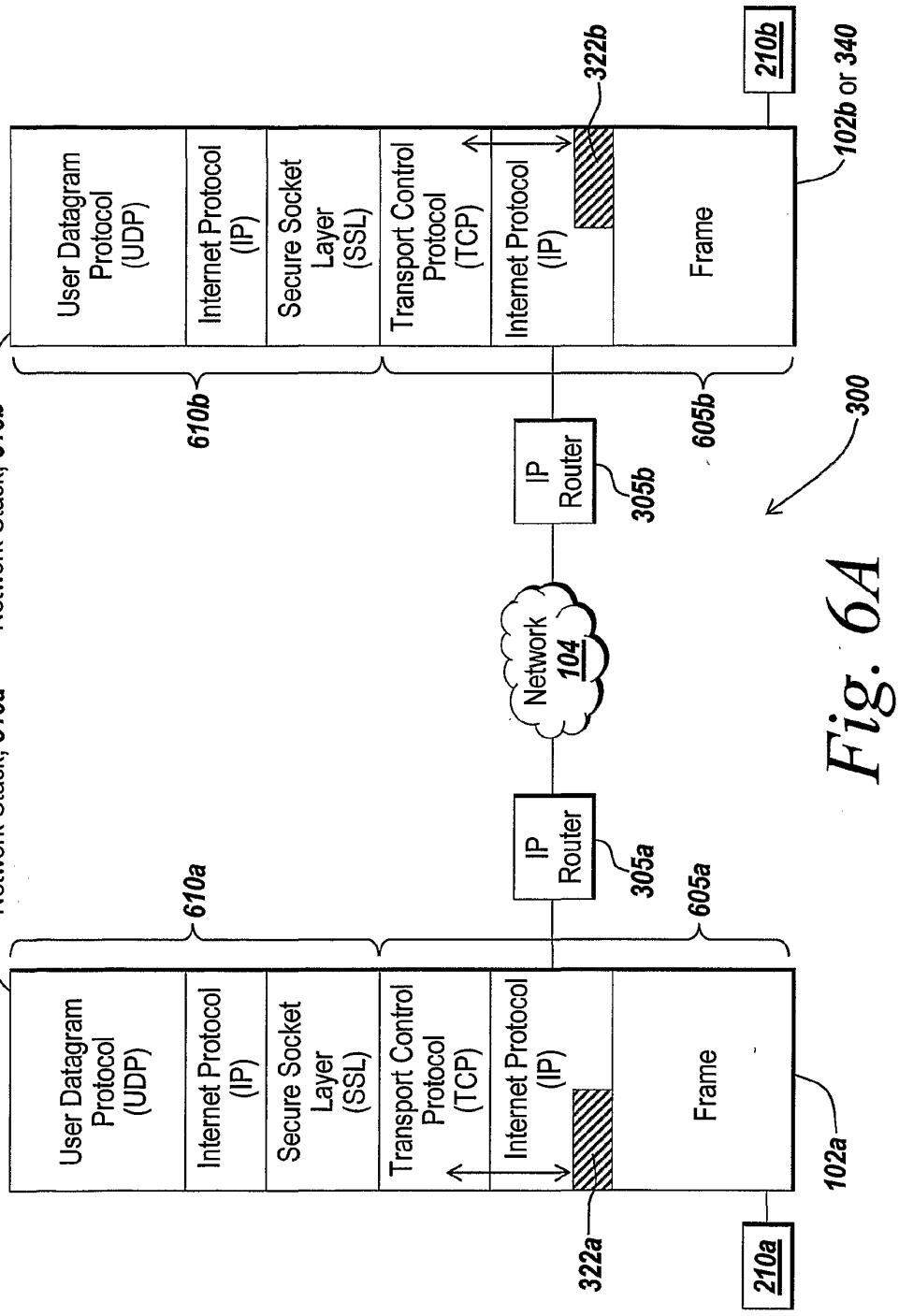

Network Stack, 310b
Network Stack, 310a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Frame
610b
610a
605b
605a
322b
322a
210b
210a
102b or 340
102a
IP Router
305b
IP Router
305a
Network 104
300

Fig. 6A

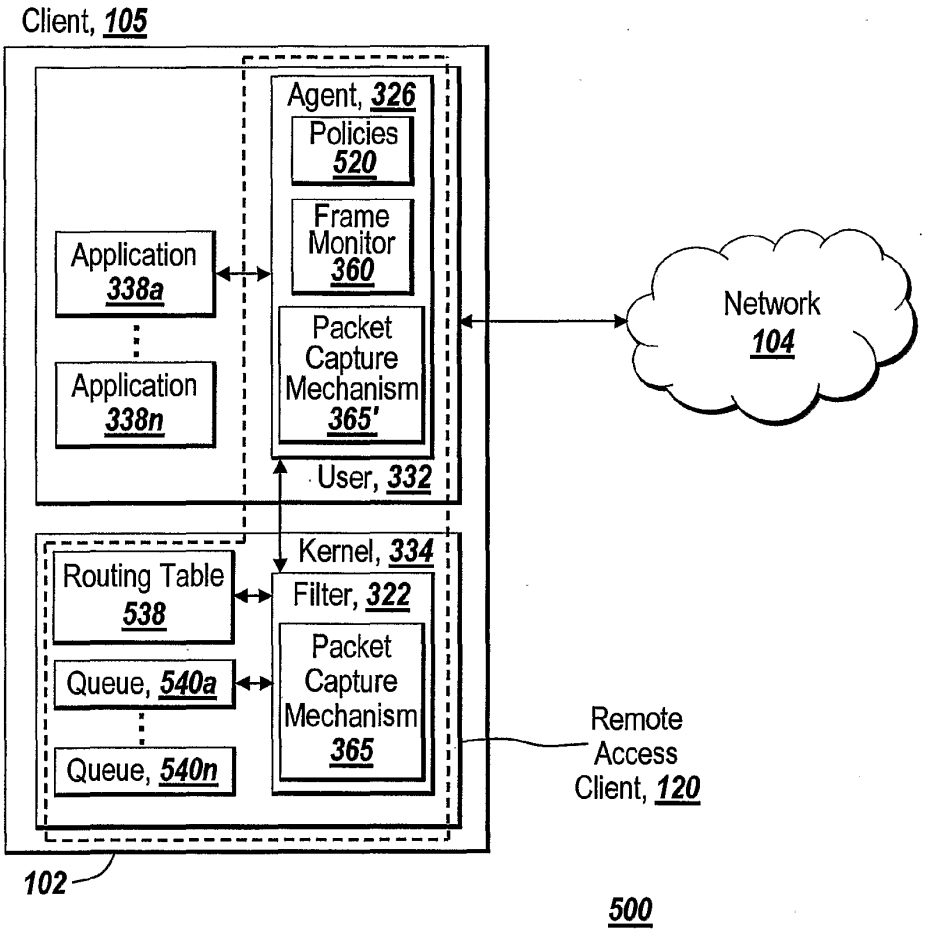

Client, 105
Agent, 326
Policies 520
Frame Monitor 360
Application 338a
Application 338n
Packet Capture Mechanism 365'
Network 104
User, 332
Kernel, 334
Routing Table 538
Filter, 322
Queue, 540a
Queue, 540n
Packet Capture Mechanism 365
Remote Access Client, 120
102
500

Fig. 5A

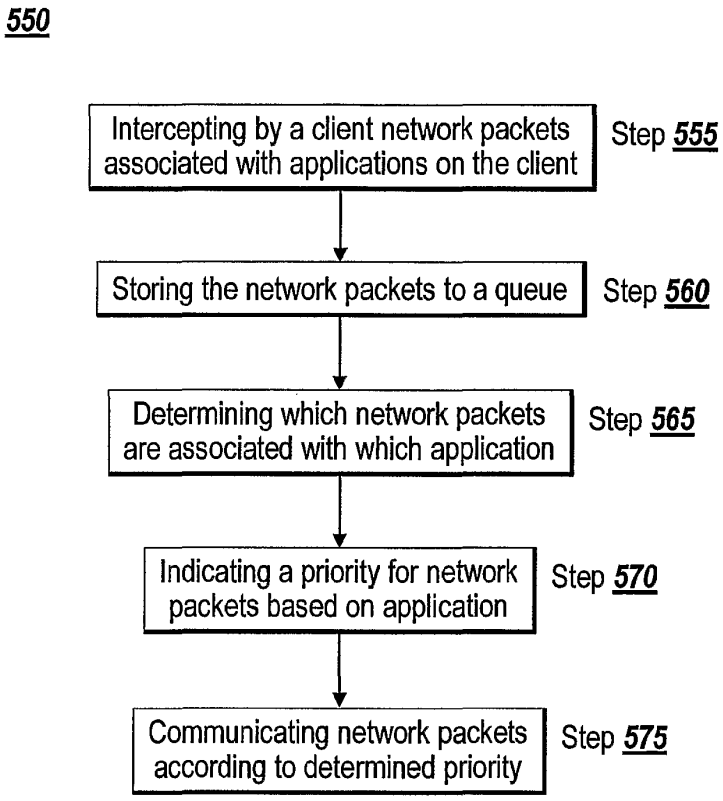

550
Intercepting by a client network packets associated with applications on the client
Step 555
Storing the network packets to a queue
Step 560
Determining which network packets are associated with which application
Step 565
Indicating a priority for network packets based on application
Step 570
Communicating network packets according to determined priority
Step 575

Fig. 5B

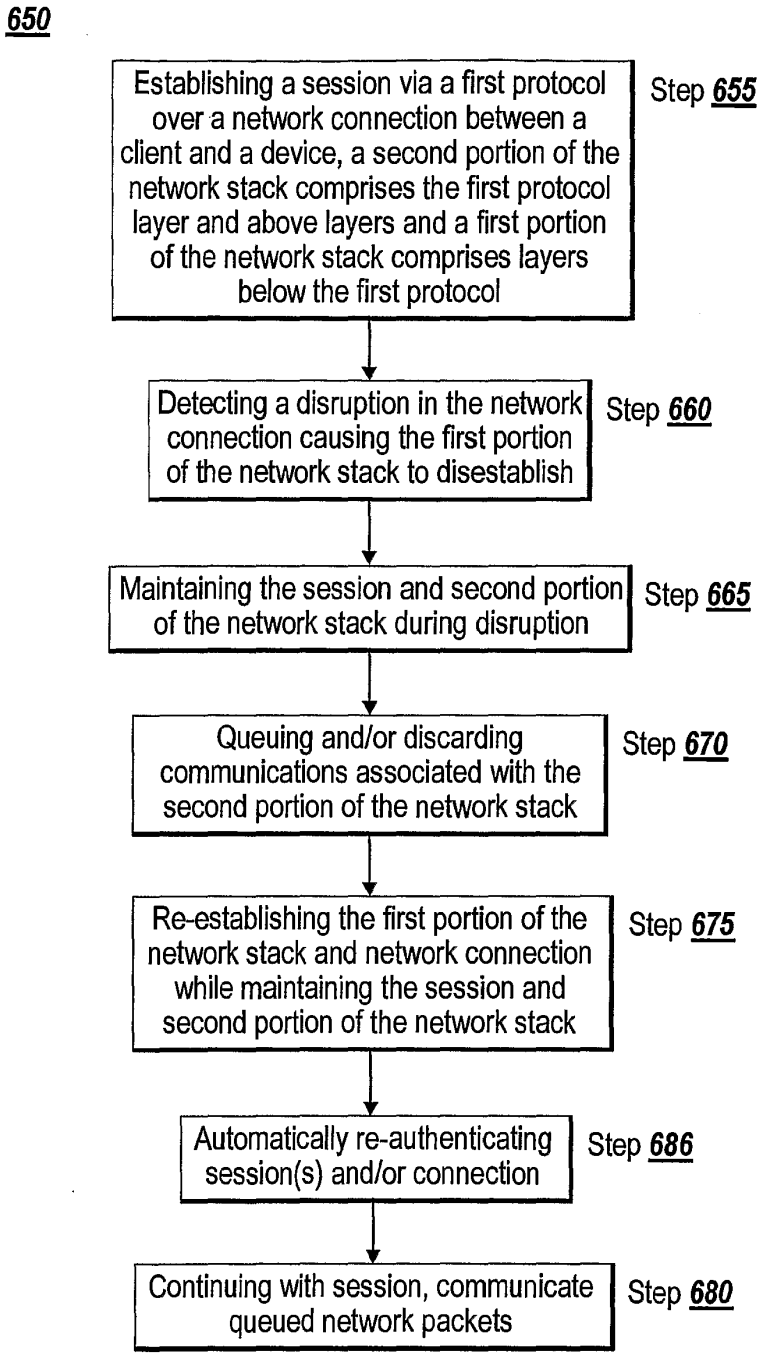

650
Establishing a session via a first protocol over a network connection between a client and a device, a second portion of the network stack comprises the first protocol layer and above layers and a first portion of the network stack comprises layers below the first protocol
Step 655
Detecting a disruption in the network connection causing the first portion of the network stack to disestablish
Step 660
Maintaining the session and second portion of the network stack during disruption
Step 665
Queuing and/or discarding communications associated with the second portion of the network stack
Step 670
Re-establishing the first portion of the network stack and network connection while maintaining the session and second portion of the network stack
Step 675
Automatically re-authenticating session(s) and/or connection
Step 686
Continuing with session, communicate queued network packets
Step 680

Fig. 6B

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/60

[12] 发明专利申请公开说明书

[21] 申请号 02156671.2

[43] 公开日 2004 年 6 月 30 日

[11] 公开号 CN 1508734A

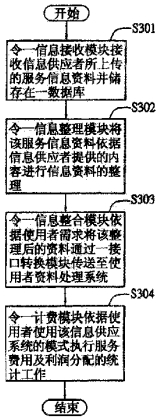
[22] 申请日 2002.12.13 [21] 申请号 02156671.2
[71] 申请人 华人创意股份有限公司
地址 台湾省台北市
[72] 发明人 温世仁 吴鸿祺

[74] 专利代理机构 北京三幸商标专利事务所
代理人 刘激扬
权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称 用以支持中小企业营运发展的信息供应方法以及系统

[57] 摘要

一种用以支持中小企业营运发展的信息供应方法以及系统，令一信息接收模块接收信息供应者上传的服务信息资料并储存在数据库中；令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行相关资料的整理；令一信息整合模块依据使用者输入的需求将该整理后且符合该需求的资料，通过一接口转换模块传送至使用者数据处理系统；最后，令一计费模块依据使用者使用系统的模式，执行服务费用的统计工作。 通过该使用本发明，能够提供个人工作室、住家办公室及中小企业的经营者及其从业人员使用者通过单一网站即可获得所需的信息服务。



ISSN1008-4274

1. 一种用以支持中小企业营运发展的信息供应方法，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应方法包括：

令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；

令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；

令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及

令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

2. 如权利要求 1 所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式所提供的网络协议地址及统一资源寻址器地址资料其中的一种。

3. 如权利要求 1 所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的一种。

4. 如权利要求 1 所述的方法，其特征在于，该信息资料的整理步骤还包括将同一信息供应者及不同信息供应者其中任一者提供的相同、相似及不同信息的其中任一种信息，加以分类、归纳及结合的数据处理过程。

5. 如权利要求 1 所述的方法，其特征在于，该信息整合形式可以是数据库信息的搜寻、信息服务提供者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

6. 如权利要求 1 所述的方法，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

7. 如权利要求 1 所述的方法，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

8. 如权利要求 1 所述的方法，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、

个人数字助理以及移动电话中的任一种。

9. 如权利要求 1 所述的方法，其特征在于，该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

10. 如权利要求 1 所述的方法，其特征在于，该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

11. 如权利要求 1 所述的方法，其特征在于，该数据库是一关系型数据库。

12. 如权利要求 1 所述的方法，其特征在于，该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

13. 如权利要求 1 所述的方法，其特征在于，该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

14. 一种用以支持中小企业营运发展的信息供应系统，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应系统包括：

一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；

一信息接收模块，用以接收信息提供者通过网络通讯系统提供的信息；

一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；

一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；

一接口转换模块，用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格；以及

一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

15. 如权利要求 14 所述的系统，其特征在于，该信息供应者提供的信息可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式提供的网络协议地址及统一资源寻址器地址资料中的任一种。

16. 如权利要求 14 所述的系统，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的任一种。

17. 如权利要求 14 所述的系统，其特征在于，该信息整理模块是将同一信息供应者及不同信息供应者中任一者提供的相同、相似及不同的信息中的任一种信息，加以分类、归纳及结合的数据处理过程。

18. 如权利要求 14 所述的系统，其特征在于，该信息整合模块的整合形式可以是数据库信息的搜寻、信息服务者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

19. 如权利要求 14 所述的系统，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

20. 如权利要求 14 所述的系统，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

21. 如权利要求 14 所述的系统，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、个人数字助理以及移动电话中的任一种。

22. 如权利要求 14 所述的系统，其特征在于，该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

23. 如权利要求 14 所述的系统，其特征在于，该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

24. 如权利要求 14 所述的系统，其特征在于，该数据库是一关系型数据库。

25. 如权利要求 14 所述的系统，其特征在于，该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

26. 如权利要求 14 所述的系统，其特征在于，该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

用以支持中小企业营运发展的信息供应方法以及系统

技术领域

本发明是关于一种用以支持中小企业营运发展的信息供应方法以及系统，特别是关于一种整合信息以提供使用者通过单一网站获取该整合信息的信息供应方法与系统。

背景技术

随着电子信息科技的蓬勃发展，诸如个人计算机、笔记本型计算机、平板计算机、掌上型计算机、个人数字助理乃至移动电话等具有数据处理功能的电子装置或系统，其在功能上愈来愈强大，除单纯进行数据处理外，这些设备已经能够提供使用者上网浏览、信息的上传或下载、听音乐、编辑、播放影像信息等多元化的多媒体服务，来获取所需要的信息。另一方面由于有线及无线网络通讯技术的日益成熟，再加上这些电子装置或系统的体积愈来愈轻薄短小，便于使用者在行动中进行信息的取得。基于上述种种客观环境，使用者主观上也更乐意通过该具有网络连接与数据传输功能的电子装置或系统进行信息的搜寻及取得。

但是当愈来愈多的使用者不再通过报纸、杂志，甚至广播电视等传统的媒体来取得信息，而是选择通过具有实时性的网络通讯系统来取得所需的信息时，网络信息供应商势必要考虑如何能够充分利用网络通讯系统的特性，提供有别于传统媒体所能够提供的信息。

现有通过网络通讯系统提供使用者信息的方法不一般是以下方法：由使用者通过浏览器联接门户网站，输入要搜寻信息的关键词等搜寻条件，通过该门户网站提供的搜寻引擎进行与该关键词相符及/或近似的网页资料，由使用者通过输入网址或借由超级链接的方式与该网址进行联接，通过浏览器进行资料的浏览或传输。

这种现有的信息搜寻方法，对于缺乏网络搜寻经验或是搜寻条件等相关信息不是十分充分的使用者而言，信息的寻找、取得有时就如同大海捞针。此外，若使用者要同时搜寻许多具有实质关联性、却不具有形式关联性的网站时，上述的搜寻方式恐怕无法有效解决使用者的需要。此时，使用者仍须通过一次次的搜寻才有可能找到所需要的

信息。即令使用者已经搜寻到所有的相关信息，但若缺乏有效率的资料筛选，则所搜集到的信息对于使用者而言不但无法有效的解决自身的需要，有时反而会成为庞大的负担。

另一方面，使用者在通过付费网站获取信息方面，通常所采用的方法有固定费率制，也就是缴纳一定的费用取得在一定期间内无限次的使用权；储值制，也就是购买一定的点数，再从所使用的信息对应的点数中加以扣除。除上述两种以外，再一种方法就是依据服务提供商所开列的价格，通过信用卡或转帐的方式支付费用。上述服务费用的支付方法均是依据固定的服务价目表收费，并不能够将使用者登录或连接的等级、范围甚或是服务内容作为服务费率调整的依据。

综上所述，如何能够为使用者提供一套具有整合多元信息、并能够更合理地保证信息服务提供商与信息需求方利益的方法，是亟需解决的问题。

发明内容

为克服现有技术的缺点，本发明的主要目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一信息供应网站，让信息供应者通过该信息供应网站提供信息服务。

本发明的另一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率。

本发明的又一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易。

本发明的再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算。

本发明的又再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一接口转换机制，用以提供客户端的使用者可以借由不同类型的数据处理系统通过本发明获得信息服务。

为达成上述目的，本发明之用以支持中小企业营运发展的信息供应系统包括：一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；一信息接收模块，用

以接收信息提供者通过网络通讯系统提供的信息；一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；一接口转换模块，用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格；以及一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

通过该用以支持中小企业营运发展的信息供应系统，进行信息供应的方法是：令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

与传统的信息供应方法以及系统比较，本发明通过整合信息供应者提供的信息机制、信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息供应者通过该信息供应网站提供信息服务，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率；同时能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易，它所提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算及收取。本发明提供的接口转换机制，能够让客户端的使用者可以借由不同类型的数据处理系统通过本发明获得其所需的信息服务。

附图说明

图 1 为一应用架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的应用架构；

图 2 为一系统架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的系统架构；以及

图 3 为流程图，用以显示本发明之用以支持中小企业营运发展的信息供应方法的流程步骤。

具体实施方式

实施例

在以下实施例中，本发明用以支持中小企业营运发展的信息供应方法以及系统中所提供的信息包括文字资料、图像数据、影音资料以及其它无法由人类通过感官直接辨识的电磁记录资料，实际上能够通过本发明的用以支持中小企业营运发展的信息供应方法以及系统提供信息供应服务的，均适用于本发明的用以支持中小企业营运发展的信息供应方法以及系统。

请参阅图 1，如图所示，在本实施例中，本发明的用以支持中小企业营运发展的信息供应系统 100，是应用在现有的主从架构网络通讯系统 200 中，又该用以支持中小企业营运发展的信息供应系统 100 是建构在该网络通讯系统 200 的伺服端，用以提供具有网络连接功能的网络终端装置 300 及网络终端装置 400 的客户端使用者，借由一浏览器应用程序通过该网络通讯系统 200，与建构在该伺服端的用以支持中小企业营运发展的信息供应系统 100 相互连接，进行包括程序或资料的上传或下载、资料储存及数据管理等工作。其中，该网络通讯系统 200 可以是一国际互联网(Internet)、企业内部互联网(Intranet)或企业间互联网(Extranet)；该网络终端装置 300 及网络终端装置 400 可以是个人计算机(PC)、笔记本型计算机(NB)、工作站(Workstation)或其它具有数据处理功能的装置或系统；该浏览器应用程序可以是微软的网络探险家(Internet Explorer)或是网景的领航员(Netscape Navigator)等。上述的主从架构网络通讯系统 200、该网络终端装置及该浏览器应用程序均为现有的软、硬件架构，故在此不重复说明。

请参阅图 2，它显示了本发明的用以支持中小企业营运发展的信息供应系统 100 的系统架构，如图所示，该用以支持中小企业营运发展的信息供应系统 100 搭配至一网络服务器 210，该网络服务器 210 是提供该用以支持中小企业营运发展的信息供应系统 100，通过该网络通讯系统 200 与网络终端装置 300 及网络终端装置 400 相互连接，并提供该网络终端装置 300 及网络终端装置 400 响应使用者的指令或其它需求以进行资料存取之用。在本实施例中，该网络终端装置 300 及网络终端装置 400，是利用各该网络终端装置上的网络浏览器应用程序，如上述的微软的 IE 或是网景的 Navigator，通过网络通讯系统 200 经由该网络服务器 210，与该用以支持中小企业营运发展的信息供应系统 100 相互连接，以进行档案管理相关的工作。需特别说明的是，该用以支持中小企业营运发展的信息供应系统 100 还可以与一防火墙(Firewall)系统联接(未图标)，用以保护该用以支持中小企业营运发展的信息供应

系统 100。该用以支持中小企业营运发展的信息供应系统 100 包括：一数据库 220、一信息接收模块 230、一信息整理模块 240、一信息整合模块 250、一接口转换模块 260 以及一计费模块 270。

该数据库 220 是用来储存至少包括信息提供者所提供的信息、信息整合的相关资料、信息需求者的信息资料、信息需求者及信息供应者之间信息服务整合的资料以及服务费用等资料表。在本实施例中，为增加资料查询及检索的效率，该数据库 220 可以是一关系型数据库。其中，该信息提供者所提供的信息资料表，用来储存至少包括信息提供者所提供的文字资料、图像数据、影音资料以及其它能够以储存在该数据库的任何形式的资料等数据区位；该信息整合的相关资料表，用以储存至少包括信息类别资料、信息内容相互关系资料以及信息整合资料等数据区位；该信息需求者的信息资料表，用以储存至少包括使用者基本身分、使用者使用信息的权限以及使用者使用资源的记录等数据区位；该信息需求者及信息供应者之间信息服务整合的资料表，用以储存至少包括有信息服务整合类别资料以及信息服务整合历史记录资料等数据区位；该服务费用资料表，则用以储存至少包括信息供应者的收费模式、信息供应者所提供的信息被使用的计量以及信息供应者与该用以支持中小企业营运发展的信息供应系统管理者之间利润分配基础等数据区位。

通过这种关系型数据库的建立，当使用者输入上述任一种资料时，该用以支持中小企业营运发展的信息供应系统 100 即可快速的寻找到其对应的资料。需特别说明的是，上述的各该数据区位及其所属的资料表仅为举例而已，在实际情况下，其内容应更为明确详细。此外，各该数据区位的内容也有可能包括有其它的数据区位或是资料表，只是由于篇幅所限，以及为陈述上的简洁，仅显示与本发明的用以支持中小企业营运发展的信息供应方法以及系统有关的部分资料。另一方面，该关系型数据库的系统架构也有多种，应视使用者的需要加以建构，故也不再重复说明。

该信息接收模块 230 是用来接收信息提供者通过网络通讯系统 200 所提供的信息。在本实施例中，信息提供者可以是顾问咨询服务、专业规划服务、生活增值服务、知识增值服务、业务连接服务，甚至包括法人组织或政府机关的行政单位或对外服务窗口等任何自然人或法人构成的信息提供主体。该信息提供者可借由该网络终端装置通过该网络通讯系统 200，将提供的信息服务内容上传至该网络服务器 210，该信息接收模块 230 随即将接收到的信息服务相关资料加以储存至该

数据库 220 中。

需特别说明的是，信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间应建立一资料传送的协议，如以特定的识别号码或文字定义的特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息相关资料时，则应依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段。

该信息整理模块 240 是对该信息接收模块 230 接受该信息提供者提供的信息内容，按照一定的规则进行整理。在本实施例中，由于信息提供者所提供的信息内容包罗万象，内容可能包括各个领域中不同层次的内容，可能是民间企业或是政府机关。但是通常一种业务的处理流程可能包括许多不同的信息供应者才能完成。如专利的申请，其流程可能包括寻找专业的专利事务所讨论专利申请的相关信息，委托其办理如专利说明书的撰写或专利申请程序的代办，当完成专利说明书的撰写后，还必须送交专利局进行专利审查，最后再经由相关的作业程序才能确定是否获得专利权。

该信息整理模块 240 能够将与专利申请相关的信息服务内容作一整理，当使用者欲搜寻与专利申请相关的信息服务时，即可获取一连串有用且相关的信息服务。在整理手段上，可以通过上述由信息供应者与用以支持中小企业营运发展的信息供应系统管理者之间的协议，借由特定的识别号码或文字加以分类，以将前阶段由民间专利事务所提供的服务，与后阶段由政府机关的专利局提供的行政程序服务等加以连接。也就是当信息供应者提供的信息通过该信息接收模块 230 储存至该数据库 220 时，该信息整理模块 240 能够将该特定相关的信息加以整理，并以特定的关键内容如“专利申请”等储存至该数据库 220 中的特定数据区位中，以供该用以支持中小企业营运发展的信息供应系统 100 进行资料的存取。

该信息整合模块 250 用来将该信息整理模块 240 所整理出的信息与使用者所提出的信息需求作一个连接互通。在本实施例中，当使用者借由网络终端装置通过该网络通讯系统 200，与建构有该用以支持中小企业营运发展的信息供应系统 100 的网站相互连接时，该网站会提供一信息服务相关的搜寻机制，如请求使用者输入使用者基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需的信息服务与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的相关信息服务相互结合。其结合方式包括提

供使用者以超级链接的方式与该信息供应者相互连接、以提供如统一资源寻址器(URL)等网络资源的连接及/或提供如线上实时视频会议(Net-Meeting)等线上实时的信息请求及响应。

该接口转换模块 260 会依据不同客户端的网络终端装置提供符合该系统资料传送存取的资料规格。在本实施例中，该网络终端装置 300 及 400 并不限定为现有的个人计算机或笔记本型计算机，还可包括任何能够通过网络通讯系统 200 连接至架构有该用以支持中小企业营运发展的信息供应系统 100 网站的系统或装置，如移动电话所适用的无线应用软件协议(WAP)等其它网页浏览格式。该接口转换模块 260 是为使用不同资料浏览或存取协议的系统或装置提供转换接口，使其均可连接到架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，供使用不同浏览或存取协议的网络终端装置进行信息的搜寻或接受信息供应者所提供各种形式的信息服务。

该计费模块 270 是用以依据使用者使用资源服务的模式，计算其所应支付的服务费用。在本实施例中，该计费模块 270 除了依据信息供应者或该用以支持中小企业营运发展的信息供应系统 100 的管理者所确定的信息服务价目表，计算使用者所使用的信息服务内容所应支付的总服务费用外。还能够依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式及其历史记录，作为计算服务费用的标准。以上述的“专利申请”流程为例，使用者自搜寻相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式、并加以记录，若该使用者与其中一家具有专利代理经验的信息供应者相互联系，并且双方进行了如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间服务与被服务的信息，若使用者再通过该网站与专利局进行信息需求与供应的服务时，该计费模块 270 仍会记录他们之间的有关信息。通过上述追踪记录使用者的行为模式、并加以记录的方式，能够以依据使用者利用该网站的不同层次(Level)作为计算服务费用的标准。

请参阅图 3，它显示通过上述的用以支持中小企业营运发展的信息供应系统 100，在实施该用以支持中小企业营运发展的信息供应方法的步骤是。

在步骤 S301 中，令该信息接收模块 230 接收信息供应者上传的服务信息资料并储存在该数据库 220 中。通过该信息接收模块 230 能够接收资料供应者所传送的信息资料，以超级链接的方式所提供的网络

协议地址及／或统一资源寻址器地址等资料。

承前所述，该信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间得建立一资料传送的协议，如以特定的识别号码或文字定义特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息等相关资料时，则能够依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段中。

在本实施例中，若一专利事务所欲通过该用以支持中小企业营运发展的信息供应系统 100 作为一专利信息供应者，则其能够借由网络终端装置通过该网络通讯系统 200，将其所能提供的信息资料传送至该网络服务器 210，其中该传送的资料包括文字或影像信息资料，以超级链接方式所提供的网络协议地址及／或统一资源寻址器地址等资料。此外，还包括特定的识别号码或文字，如“0001”与“专利服务”等，该信息接收模块 230 在该网络服务器 210 接收到上述的资料时，随即将该资料储存至该数据库 220 中符合该识别号码“0001”与识别文字“专利服务”的数据区位中，接着进行步骤 S302。

在步骤 S302 中，令该信息整理模块 240 将该服务信息资料依据信息供应者所提供的内容进行相关资料的归纳、整理。其过程包括将同一信息供应者或不同信息供应者所提供的相同、相似或不同的信息加以分类、归纳或结合等。

承前所述，除该专利服务的信息供应者能够传送相关信息资料外，设架构有该用以支持中小企业营运发展的信息供应系统 100 的网站还能够与政府机关、如上述的专利局等相互合作，提供诸如线上专利申请或咨询等服务。由于一专利的申请流程可能需通过包括专利事务所与专利局等信息服务提供者的协助才能顺利完成。则该信息整理模块 240 则应将专利事务所及专利局所提供的信息服务作一信息归类，当使用者登录架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，且欲请求该网站提供“专利申请”的信息服务时，则能够轻易的搜寻到上述经归纳后的该专利事务所及专利局所提供的信息服务，接着进行步骤 S303。

在步骤 S303 中，令一信息整合模块 250 依据使用者输入的需求，将该整理后且符合该需求的资料通过一接口转换模块 260 传送至客户端网络终端装置。其整合的模式包括数据库 220 信息的搜寻、信息服务提供者网络资源的连接及/或提供线上实时的信息请求及响应等。

承前所述，当有“专利服务”信息需求的使用者登录该网站后，该网站能够提供使用者一输入该使用者相关信息的功能，如要输入使

用者的基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字，如识别号码“0001”与识别文字“专利服务”等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需要的“专利服务”的相关信息服务，与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的、经整合后的该专利事务所及专利局所提供的信息服务相互结合。

在本实施例中，使用者进行数据库 220 中相关资料的搜寻、与该专利事务所进行网络视频会议及上述假设的专利局线上的专利申请作业流程等信息服务，接着进行步骤 S304。

在步骤 S304 中，令一计费模块 270 依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式，执行服务费用的统计工作。它是依据使用者使用信息的模式，计算所需支付的费用以及信息供应者之间的利润分配。

承前所述，在使用者通过上述的信息整合模块 250 取得该用以支持中小企业营运发展的信息供应系统 100 所提供的服务信息的过程中，该计费模块 270 会记录使用者与该信息供应者整合的信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其信息。

在本实施例中，以上述的“专利申请”流程为例，使用者自搜寻相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式并加以记录，若该使用者与其中一具有专利代理经验的信息供应者相互联系，双方进行如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间的相关信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其有关信息。通过上述的信息记录，该计费模块 270 能够依据所记录该使用者连接该网站的层次、连接的时间及/或信息服务的内容等，计算出相对应的服务费用，其中，该服务费用的计算基准应视实际情况加以制定。此外，该计费模块 270 还能够依据信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者对于信息提供的利润分配基准，进行利润分配的计算。

综上所述，本发明之用以支持中小企业营运发展的信息供应方法以及系统，能够通过整合信息服务供应者所提供的信息服务供应机制、信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息服务供应者通过该信息供应网站提供信息服务。

本发明的用以支持中小企业营运发展的信息供应方法以及系统能够协助个人工作室、住家办公室及中小企业的经营者及其从业人员，在接取订单、增创营收、善用外部资源、进行委外服务、增加经营弹性、减少聘雇人员及办公室空间的需求、节省营运成本、降低创业门槛等方面提供帮助，进而达到解决失业问题及调整产业结构的目的。

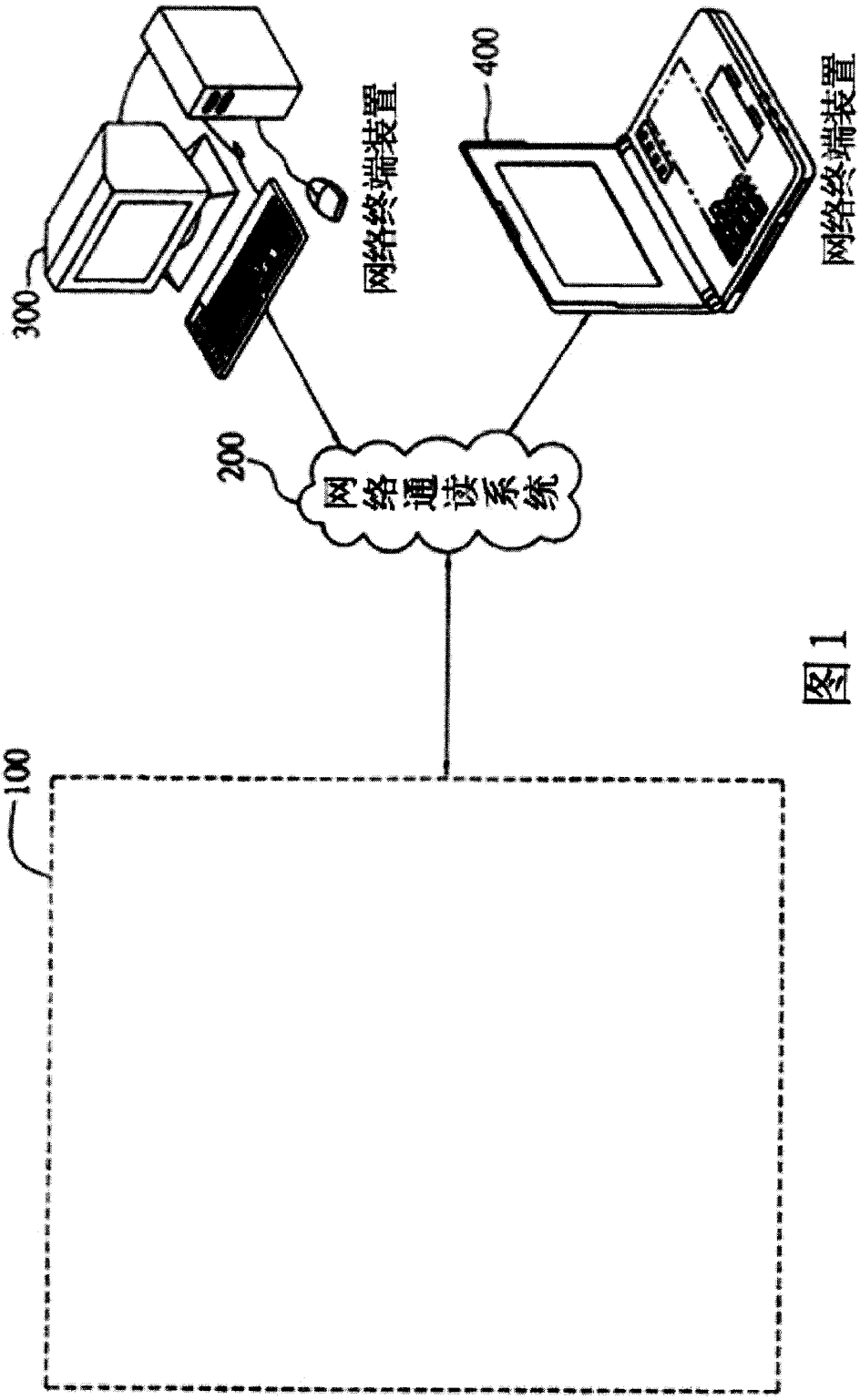


图 1

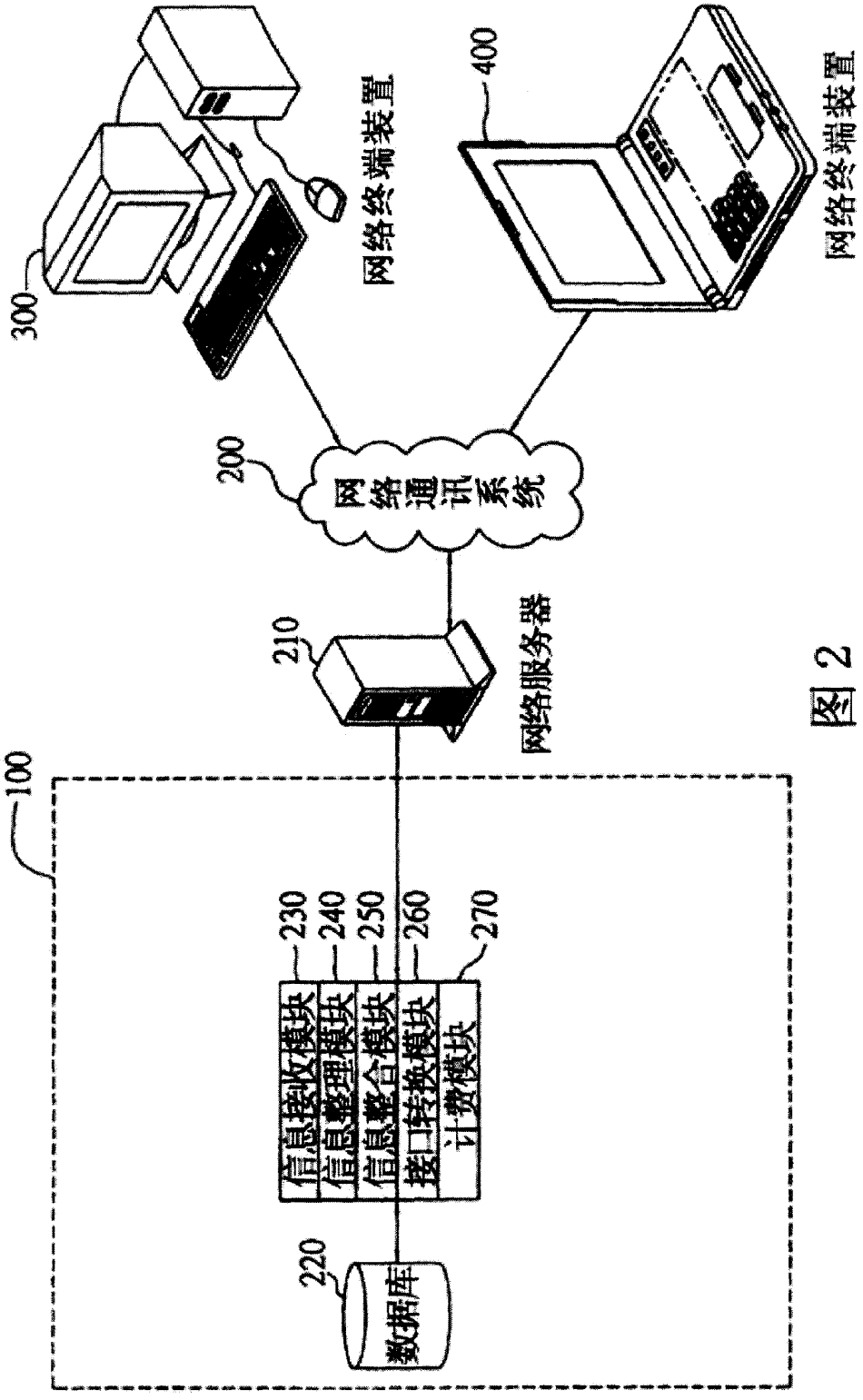

300
网络终端装置
400
网络终端装置
200
网络通讯系统
210
网络服务器
100
230
240
250
260
270
信息接收模块
信息整理模块
信息整合模块
接口转换模块
计费模块
220
数据库

图 2

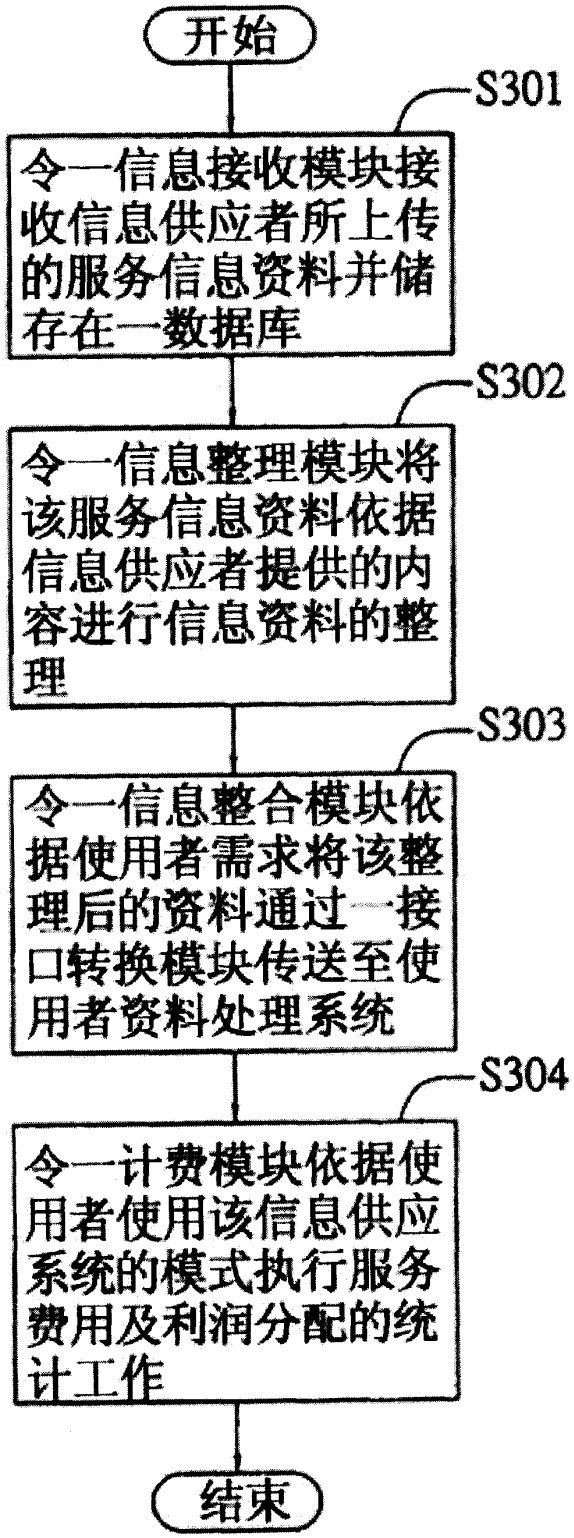

开始
S301
令一信息接收模块接收信息供应者所上传的服务信息资料并储存在一数据库
S302
令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行信息资料的整理
S303
令一信息整合模块依据使用者需求将该整理后的资料通过一接口转换模块传送至使用者资料处理系统
S304
令一计费模块依据使用者使用该信息供应系统的模式执行服务费用及利润分配的统计工作
结束

图 3

Annie

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Method and system for providing information for supporting operation development of small-medium enterprises

CN 1508734 A

Publication number	CN1508734 A
Publication type	Application
Application number	CN 02156671
Publication date	Jun 30, 2004
Filing date	Dec 13, 2002
Priority date	Dec 13, 2002
Inventors	温世仁, 吴鸿祺
Applicant	华人创意股份有限公司
Export Citation	BiBTeX, EndNote, RefMan

Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention is a kind of information supplying method and the system for supporting small and medium-sided enterprise development. A information receiving model receives the service information data uploaded by supplier and stores them in the databank; a information arranging model carries on the arrangement of relative data according to the content supplied by the supplier; a information integrating model transmits the proper data to the user data processing system through a interface converting model, finally, a charge calculating model calculates the charge according to the mode used by the user.

DESCRIPTION translated from Chinese

Supply methods to support the development of SMEs as well as operating system

Technical Field

The present invention relates to an operation to support the development of SMEs information provision method and system, especially with regard to an integrated information to provide users to access information through a single Web site that integrated information provision method and system.

Background

With the rapid development of electronic information technology, such as personal computers, notebook computers, tablet computers, palmtop computers, personal digital assistants and even mobile phones and other electronic devices or systems having a data processing function, its increasingly powerful in function, In addition to simple data processing, these devices have been able to provide users with Internet browsing, upload or download information, music, editing and playback of multimedia video information and other diversified services to get the information they need. On the other hand due to the wired and wireless network communications technologies become more sophisticated, the volume plus these electronic devices or systems increasingly compact size, ease of access to information in the user performs actions. Based on all these objective circumstances, users are more willing subjective electronic device or system that has a network connection and data transmission capabilities to search and access to information.

But when more and more users are no longer to obtain information through traditional media, newspapers, magazines and even radio and television, choosing instead to obtain the necessary information through the network communication system with real-time, online information provider bound to consider how to take full advantage of the characteristics of the network communications system, providing different from traditional media to provide information.

Existing methods provide user information through the network communication system is not generally the following methods: by the user through a browser connection portal, enter search keywords and other search criteria information

CLAIMS (26) translated from Chinese

An information provision method to support SME Business Development, to provide users with a data processing system by means of the information required to obtain services through a network communication system, wherein the means for support of the SME Business Supply method development include: make an information receiving module receives the information service provider information uploaded and stored in a database; make an information consolidation module based on the content of the service information provided by the information provider of information materials finishing; make an information integration module based on the needs of the user input, the finishing and meet the needs of data through a user interface conversion module is transferred to the data processing system; and to make a billing module according to the user to use the use to support the development of SMEs operating mode of information supply system, the implementation of service fees and profit distribution statistics work.

2. The method according to claim 1, characterized in that the information service provider information may be uploaded text data, image data, audio data, image data, network protocol address provided by hyperlinks and unified address information resource addressing one of them.

3. The method according to claim 1, characterized in that the service information This information can be uploaded provider of business intelligence, business opportunities, professional services, professional planning, business connections, administrative procedures and value-added services in one .

4. The method according to claim 1, characterized in that the finishing step also includes the same information will be different from the same information provider and wherein any one of the information provider provides, any of which is similar to and different information information, classify, summarize and combine the data processing.

5. The method according to claim 1, characterized in that the integration of information and forms can be connected to provide search and information services provider of database information online real-time network resource information request and response in

provided through the portal, and the search engine Keywords consistent and / or similar web information input by the user through the website or by way of hyperlinks connecting with the site, browse or transfer data through the browser.

This existing information search method, for lack of experience, or search Web search and related information is not very full of users, the information search, obtain sometimes like needle in a haystack. In addition, if the user to simultaneously search a number of substantive relevance, is not associated with a form of site, said search means could not be effectively addressed the needs of users. In this case, the user must still search through time and time again possible to find the information they need. And even if the user has to find all the relevant information, but if the lack of effective screening information, then the information gathered for the user not only can not effectively solve their own needs, sometimes it will become a huge burden.

On the other hand, users get to information through pay sites, typically used a fixed rate system, which is to pay a fee to obtain unlimited times within a certain period the right to use; stored value system, which is to buy a certain points, and then be deducted from the corresponding point information used in the. In addition to the two outside, then one approach is based on the service provider listed price, pay by credit card or debit way. The method of payment of the above services are based on a fixed fee service price list, the user is not able to log on or connect the level, the scope of services or even service rates as the basis for the adjustment.

In summary, how can we provide users with a set of integrated pluralistic information and the ability to more reasonable assurance that the information service provider and information needs of Fangli Yi approach is needed to solve problems.

DISCLOSURE

To overcome the disadvantages of the prior art, the main object of the present invention is to provide a support operation for the development of SMEs information provision method and system capable of providing an information provider website information provider to provide information so that the information supplied by website services.

Another object of the present invention is to provide a support operation for the development of SMEs information provision method and system that can provide information on the information provider for effective integration, improve the efficiency of users to find the information.

A further object of the present invention is to provide a support for the development of the SME Business information provision method and system, which can provide a user through an information service integration mechanisms and information provider of information services deals.

A further object of the present invention is to provide a support operation for the development of SMEs information provision method and system, which can provide an accounting mechanism to allow information providers to use information service based on user model to calculate the cost of services .

Again object of the present invention is to provide an operation to support the development of SMEs information provision method and system, which can provide an interface conversion mechanism for providing client user can borrow from the different types of data processing systems The present invention is to obtain information services.

To achieve the above objects, the present invention in order to support the development of SMEs operating information supply system comprising: a database for storing information providers including at least the information provided, the relevant data and information collated, the information needs of those information, information and data as well as those who need services cost any one.

The method according to claim 6, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

7. The method according to claim 1, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

8. The method according to claim 1, characterized in that the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

9. The method according to claim 1, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

10. The method according to claim 1, characterized in that the network communication system may be a wired communication systems and wireless communication system of any one.

11. The method according to claim 1, characterized in that the database is a relational database.

12. The method according to claim 1, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

13. The method according to claim 1, characterized in that the user may be operators and their employees personal studio, home office and SME any one.

14. A method for supporting the development of the SME Business information supply system to provide users with borrowed by a data processing system to obtain the required information and services through a network communication system, wherein the means for support of the SME Business development of information supply system comprising: a database for storing at least include the information provided by those who provide information, relevant data and information collated, the information needs of those information, information needs and information providers who integrate data and information services Service cost information; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module receives information about the content of the information provided by the provider; an information integration module to the information needs of information consolidation module collated information submitted by the user to make a connection interworking; an interface converter module for different clients according to the data processing system to provide data transmission in line with the system, access specifications; and a billing module for computing services they need to pay the costs, as well as information provider and distribution of profits to support the development of SMEs operating information providing system administrators use of resources based on user-service model.

15. The system according to claim 14, characterized in that the information provider provides information may be text data, image data, audio data, image data, addresses in hyperlinks network protocol and provide uniform resource addressing address data in either.

16. The system of claim 14, wherein the service information provider uploaded the information may be business intelligence, business

data integration between information provider of information services; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module an information integration module to the information needs of information consolidation module collated information and user make a connection the proposed exchange;; an interface converter module for different customers based on the content of the information provided by the information provider end data processing system provides data transmission in line with the system specifications access; and a billing module for computing services they need to pay the costs, as well as information service providers based on user patterns and the use of resources to support SME Business Development Supply system administrator profit distribution.

The method by which to support the development of SMEs operating information supply system for the supply of information is: make an information receiving module receives information on the service provider information uploaded and stored in a database; an information consolidation module makes the service information provided in accordance with the content of the information provider to collate information; and make an information integration module based on the needs of the user input, the finishing and meet the needs of data transmission via an interface conversion module to the user data processing systems; and to make a billing module according to the user to use the development of SMEs to support operations information supply system mode, performing a service fee of statistical work and the distribution of profits.

Compared with the traditional supply methods and information systems, information mechanism of the present invention to provide by integrating information provider, the information service integration mechanisms, billing mechanism and interface conversion mechanism, through information supplied by a website to provide information by the information provider Supply website provides information services, information providers can provide information for effective integration, improve the efficiency of users to find the information required; at the same time be able to provide users with information and services through an integrated mechanism and information provider of information services transaction, it provides a billing mechanism, so that information providers use information service based on user patterns, calculate and charge for the services. Interface conversion mechanism of the present invention provides, allows the client user can borrow from the different types of data processing systems and services to get the information they need by the present invention.

Brief Description

Figure 1 is a block diagram of the application architecture, application architecture to show support for the operation of the present invention the development of SMEs information supply system; Figure 2 is a block diagram of the system architecture, the present invention is used to show support for SMEs operation and development of information systems architecture supply system; and Figure 3 is a flow chart, the process steps for information provision method of the present invention to support the development of SMEs operating display.

opportunities, professional services, professional planning, business connections, administrative procedures and any value-added services species.

17. The system according to claim 14, characterized in that the module is the same as information of the same sort of information providers and different information provider provided by any one, any one of similar and different information in the information, classify, summarize and combine the data processing.

18. The system according to claim 14, characterized in that the form of the integration of information integration module may search a database of information, and providing on-line information services connected by network resources and real-time information request in response to any one of species.

19. The system of claim 14, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

20. The system of claim 14, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

21. The system of claim 14, wherein the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

22. The system of claim 14 claim, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

23. The system of claim 14 claim, wherein the network communication system may be wired communication systems and wireless communications systems in any one.

24. The system according to claim 14, characterized in that the database is a relational database.

25. The system according to claim 14, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

26. The system of claim 14 claim, characterized in that the user may be operators and their employees personal studio, home office and small and medium enterprises of any kind.

DETAILED DESCRIPTION

Example In the following examples, the present invention is to support the development of SMEs operating information supply method and an information system is provided including text data, image data, audio and video data as well as by other human senses can not be recorded by the direct identification of electromagnetic data actually able to provide information supply services through information provision method and system to support the operation and development of SMEs in the present invention are useful in the present invention, an information provision method and system to support the operation and development of SMEs.

See Figure 1, as shown in this embodiment, in order to support the operation and development of SMEs in the information supply system 100 of the invention, is used in the existing master-slave architecture network communication system 200, versus a to support the operation and development of SMEs in the information supply system 100 is constructed on the

servo end of the network communication system 200 for providing network terminal device has a network connection function client user network terminal device 300 and 400, made by a browser application 200, 100 interconnected with the construction of the servo end to support the operation and development of SMEs in the information supply system via the network communication system for including a program or data upload or download, data storage and data management. Wherein the network communication system 200 may be a Internet (Internet), intranet (Intranet) or enterprises Internet (Extranet); the network terminal device 300 and a network terminal device 400 may be a personal computer (PC), notebook computer (NB), workstation (Workstation) or other device or system with data processing capabilities; the browser application may be Microsoft's Internet Explorer (Internet Explorer) or Netscape Navigator (Netscape Navigator) and so on. Said main are existing software and hardware architecture from architecture network communication system 200, the network terminal device and the browser application, so this will not be repeated.

See Figure 2, which shows the operation to support the development of SMEs information systems architecture supply system 100 of the invention, as shown in the operation to support the development of SMEs with information supply system 100 to a network server 210, the network server 210 is provided to support the operation and development of SMEs in the information supply system 100 through the network communication system 200 and the network terminal device 300 and a network terminal device 400 connected to each other, and to provide the network terminal device 300 and network the terminal apparatus 400 in response to user commands or other requirements for use of data access. In this embodiment, the network terminal device 300 and a network terminal device 400 is using a web browser application on each of the network terminal device, such as Microsoft's IE or Netscape Navigator as described above, through the network communication system 200 210, 100 connected to each other via the network server to support the development of SMEs operating information supply system for records management-related work. In particular, and it noted that the operation to support the development of SMEs information supply system 100 also may be a firewall (Firewall) system connections (not shown) to protect the operation to support the development of SMEs information supply system 100 . The operation to support the development of SMEs information supply system 100 includes: a database 220, an information receiving module 230, an information consolidation module 240, an information integration module 250, an interface conversion module 260, and a billing module 270.

The database is used to store at least 220, including information provided by the information provided, the information related to the integration of data, information, information needs of those, who between information needs and information providers of information services and integrated information service expense sheet . In the present embodiment, in order to increase the efficiency of data query and retrieval, the database 220 may be a relational database. Among them, the information sheet provided by the information provider, used to store text data including at least provided information provider, image data, video and audio information and other data can be stored in any form of the databases and other data area bits; information integration related information table for storing information including at least category, information content and information integration relationship information data such as location information; the information needs of those information table for storing includes at least the basic user identity, user permission to use information and recording user data such as resource use location; the information needs of persons between information providers and information services to integrate the data sheet, including an information service for storing at least types of information integration and data information services into history data such as location; the service cost data tables, including at least information provider to store the charging mode, metering and information provider information provider the information provided is used to support the operation and development of SMEs Supply Profit distribution between basic data such as location system administrator.

Through this relationship database when a user enters any of the above information, which is used to support 100 to quickly find the information corresponding to its SME Business Development Supply System. In particular, and it noted that all the data and information on the location of the above table belongs only way of example only, in reality, its contents should be more clearly detailed. In addition, the contents of each bit of the data area may also include other data or information table location, but due to limited space, as well as a succinct statement on the show only to the present invention supports SME Business Development Supply methods and some of the information system related. On the other hand, the relational database system architecture also has many, depending on the needs of users should be construction, it is also not repeated.

The message receiving module 230 is used to receive network information provider through the communication system 200 to provide information. In this embodiment, the information provider may be consulting services, professional planning services, life value-added services, value-added knowledge services, business connectivity services, and even any natural or legal person or legal entity government administrative units or foreign service window, etc. Information provided constituted body. This information is provided by the network may, by the terminal device 200 via the network communication system, the information services to be provided to upload to the network server 210, the information receiving module 230 then the received information service related information to be saved to the database 220.

Need of special note is the establishment between information providers and managers to support the operation and development of the SME information supply system 100 a data transfer protocol, the particular type of information, such as specific identification number or text definition When 230 receives information related information having the identification

number or character of the information receiving module should be based on the identification number or text to the relevant information stored in the database 220 corresponding information storage field.

This information consolidation module 240 is receiving module 230 accepts the information content of the information providers, in accordance with certain rules finishing. In this embodiment, since the information content provided by the information provider all-inclusive, the content may include various fields at different levels of content, may be private companies or government agencies. But usually a business process flow may include a number of different information provider to complete. As a patent application, the process may include professional patent search firm to discuss patent applications related information for the execution of programs written or patent application as the patent specification of the charge d'affaires, after the completion of drafting patent specification must also be sent to the Patent patent examination Board, and finally by the relevant operating procedures in order to determine whether the franchise.

This information consolidation module 240 can be related applications and patent information services as a consolidation, when the user wants to search and patent applications related to information services, you can get a series of useful and related information services. On finishing means, said by agreement by the information provider and to support the development of SMEs operating information supply system between managers, to be borrowed by a particular identification number or text classification, to the front stage by private patent matters services provided, to be connected with the later stages of the administrative service provided by government agencies and other offices. That is when the information provider of information provided by the information receiving module 230 to 220 stored in the database, the information sorting module 240 can be related to the specific information received, and in particular the key elements as "patent application" and storage to the database 220 of location-specific data in order for the operation to support the development of SMEs information supply system 100 access data.

The information integration module 250 to the information needs of information consolidation module 240 to sort out information and users are asked to make a connection exchange. In this embodiment, when the user by the network terminal device 200 via the network communication systems, and construction has to support the operation and development of SMEs in the information supply system 100 is connected to each other at the site, the site will provide an information service relevant search mechanism, such as requesting the user to enter a personal identification data basic user identity, user permission to use the information, as well as specific information search key identification number, or text and so on, through the information integration module search function 250, that can The information requirements are needed for information services and related information services to support the operation and development of the SME information supply system 100 can offer combined with each other. Its combination of methods include providing users with hyperlinks connected to each other and the information provider to provide a unified resource addressing connector device (URL) and other network resources, and / or provide such as on-line real-time video conferencing (Net-Meeting) and other online real-time information requests and responses.

The interface conversion module 260 will be based on network unit to provide different clients in line with the specifications of the information system data transmission access. In this embodiment, the network terminal device 300 and 400 is not limited to existing personal computer or notebook computer, it may also include any communication system 200 connected via a network to have the infrastructure to support SME Business Development system or device information supply system 100 sites, such as mobile phones applies wireless applications protocol (WAP) and other browser formats. The interface conversion module 260 is to use a different browser or system or device data access protocol conversion interface is provided, it can be connected to architecture has to support the operation and development of SMEs in the information supply system 100 sites for different use Browse or access protocol network terminal devices to search for information or receive information providers are providing various forms of information services.

The billing module 270 is for the use of resources based on user mode services, computing services, they should pay the costs. In this embodiment, the billing module 270, in conformity with the information provider or manager to support the development of SMEs operating information providing system 100 of the determined price list information services, information services used to calculate the user Total service charges to be paid outside. It can also be based on the user to use the operation to support the development of SMEs information supply system model and its history of 100, as a standard computing service costs. In the aforementioned "patent application" process, for example, when a user from searching for relevant patent office or patent offices of information, the billing module 270 begins recording the user to use the site of use, click on the number or download files The amount of data and other behavior patterns, and recorded, if the user with one of the information provider has experienced patent agents interrelated, and both sides were as real-time online information and consulting service, the billing module 270 immediately recorded use between those and the information provider services and information to be served, if the user then the demand and supply of information services through the site with the Patent Office, the billing module 270 will still record information between them. It is recorded by the above-mentioned track record of user behavior patterns and the way the user can take advantage of different levels according to the website (Level) as a standard to calculate the cost of services.

See Figure 3, which shows through the above-mentioned operation to support the development of SMEs information supply system 100, the procedures described in the information supply method to support the operation and development

of SMEs in yes.

In step S301, so that the information service information receiving module 230 receives information provider uploaded and stored in the database 220. Information received by the information provider module 230 is capable of receiving data transmitted, the network protocol address provided by way of hyperlinks and / or uniform resource addressing address and other information.

Cheng said before, the information provider to support the operation and development of SMEs in the information supply system was set up a data transfer protocol between the 100 managers, such as a specific identification number or text to define specific types of information, when The information receiving module 230 receives the information and other related information with that identification number or text, it is possible according to the identification numbers or letters to the relevant information stored in the database 220 corresponding information storage field.

In this embodiment, if a patent office by the desire to support the operation and development of SMEs in the information supply system 100 as a provider of patent information, it can borrow from the network terminal device 200 via the network communication system, which It can provide information sent to the network server 210, wherein the transmission of data, including text or image information, network protocol addresses to hyperlinks provided and / or uniform resource addressing address and other information. Moreover, further comprising a specific identification number or text, such as "0001" and "Patent services", the information receiving module 230 at the network server 210 receives the information, then the information stored in the database 220 to meet the The identification number "0001" and recognized character "Patent Services" data location, followed by step S302.

In step S302, so that the information received from the service module 240 on the basis of information provided by the content information provider summarize the relevant information and organize. The process includes the same information the same provider or different information provided by suppliers, similar or different information to be classified, or a combination of induction and the like.

Cheng said before, in addition to the patent information service providers can communicate the relevant information, provided the architecture has to support the development of SMEs operating site information providing system 100 also with government agencies, such as the above-mentioned patent offices and other mutual cooperate in providing such as online and other patent applications or consulting services. Because of a patent application process may include assistance and other needs by the patent office and patent office information service providers in order to successfully complete. Then this information should be finishing module 240 information services Patent Office and the Patent Office provided information to make a classification, when the user logs architecture has to support the operation and development of the SME information supply system 100 sites, and wants When requesting the site to provide "patent application" of information services, it is possible to easily find the information and services that the patent office and summarized by the Patent Office after the above offer, followed by step S303.

In step S303, so that an information integration module 250 in accordance with the needs of the user input, the finishing and meet the needs of data through an interface conversion module 260 is transmitted to the client network terminal devices. Its integrated model includes a connection search, information services provider database 220 information network resources and / or provide real-time online information request and response and so on.

Before the bearing, when the "Patent Services" users log on to the information needs of the site, the site can provide users with an input of the user information related functions, such as the identity of the user to enter basic user usage information permissions and other personally identifiable information, as well as specific information search key identification number or character, such as the identification number "0001" and recognition of the word "patent services" through which information integration module search function 250, that person can demand the required information "patent" of related information services, and information services to support the operation and development of the SME information supply system 100 can be provided by the Patent Office and the Patent Office provided consolidated combined with each other.

In this embodiment, the user searches the database 220 relevant information, and the patent office video conferencing and network of offices above assumptions online patent application processes and other information services, followed by step S304.

In step S304, so that a billing module 270 according to the user to use this information to support the development of SMEs operating mode supply system 100, performing a service fee of statistics. It is based on the user using the information mode, calculate the required fees paid profits and the distribution of information between providers.

The front bearing, when the user 250 acquires service information to support the operation and development of the SME information supply system 100 is provided by the above process of information integration module, the billing module 270 will record the information supply Aggregated information, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will still record its information.

In this embodiment, the above-mentioned "patent application" process, for example, when users search for relevant patent office or patent offices of information from the billing module 270 begins recording the user to use the site of use, point When the selected frequency or amount of data downloaded file to record patterns of behavior and, if the user and the information provider which patent agency experience having contact with each other, the two sides as online real-time information and consulting services, the billing module 270 then record the relevant information and the user information between suppliers, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will continue to record their information. By the above information recording, the billing module 270 can connect the user based on the recorded level of the site, the connection time and / or information services and other content, calculate the corresponding service charges, which the service fees calculation basis should be developed as practicable. In addition, the billing module 270 can also provide the basis for information and managers to support the operation and development of SMEs in the information supply system 100 is provided baseline information for profit distribution, the calculated distribution of profits.

In summary, the present invention in order to support the development of the SME Business information provision method and system capable of information services through the integration of information mechanism provided by the service provider, information service integration mechanisms, billing mechanism and interface conversion mechanism , by the information supplied by a website to provide information and services provider to provide information services through the information provider sites.

Information provision method and system to support the operation and development of SMEs in the present invention can assist individuals studio, home office and SME managers and employees, in the next to take orders, to create revenue, use of external resources, conduct outsourcing services and increase business flexibility, reduce demand and office space, hiring staff, to save operating costs, reduce business barriers, such as providing help, and then to solve the unemployment problem and the purpose of the adjustment of industrial structure.

LEGAL EVENTS

Date	Code	Event	Description
Jun 30, 2004	C06	Publication	
Sep 8, 2004	C10	Request of examination as to substance	
Mar 21, 2007	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2688553 A1 2008/12/04

(21) 2 688 553

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2008/06/01
(87) Date publication PCT/PCT Publication Date: 2008/12/04
(85) Entrée phase nationale/National Entry: 2009/11/26
(86) N° demande PCT/PCT Application No.: IL 2008/000740
(87) N° publication PCT/PCT Publication No.: 2008/146296
(30) Priorité/Priority: 2007/05/30 (US60/940,882)

(51) Cl.Int./Int.Cl. *G06F 21/24* (2006.01)
(71) Demandeur/Applicant:
YOGGIE SECURITY SYSTEMS, LTD., IL
(72) Inventeur/Inventor:
TOUBOUL, SHLOMO, IL
(74) Agent: HICKS INTELLECTUAL PROPERTY LAW

(54) Titre : SYSTEME ET PROCEDE POUR FOURNIR A UN DISPOSITIF UNE PROTECTION PARE-FEU POUR RESEAU ET ORDINATEUR AVEC ISOLEMENT D'ADRESSE DYNAMIQUE

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

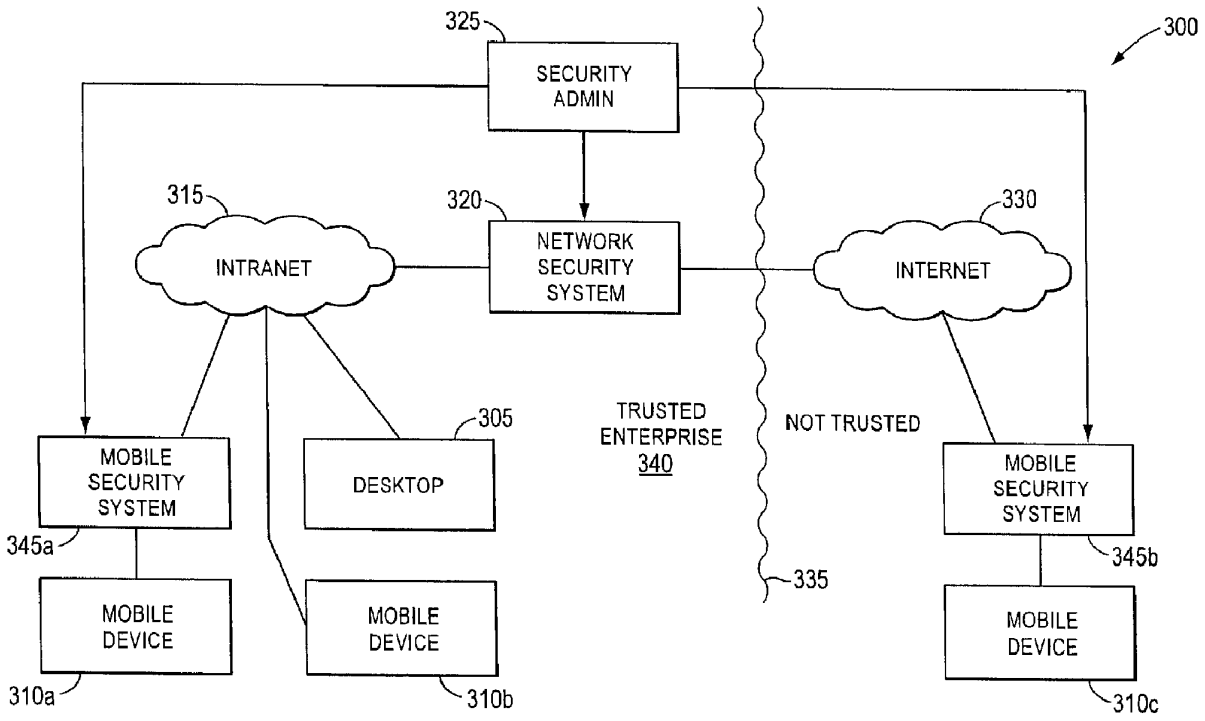


FIG. 3

(57) Abrégé/Abstract:
A computer performs dynamic address isolation. The computer comprises an application associated with an application address, a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network, a

(21) 2 688 553

(13) A1

(57) Abrégé(suite)/Abstract(continued):
network address translation engine configured to translate between the application address and a public address, and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The computer may communicate with a firewall configured to handle both network-level security and application-level security.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2008 (04.12.2008)

PCT

(10) International Publication Number
WO 2008/146296 A2

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/IL2008/000740

(22) International Filing Date: 1 June 2008 (01.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/940,882 30 May 2007 (30.05.2007) US

(71) Applicant *(for all designated States except US)*: **YOGGIE SECURITY SYSTEMS, LTD.** [IL/IL]; 42870 Beit Halevy (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TOUBOUL, Shlomo** [IL/IL]; 6 Main Street, 42945 Kefar Haim (IL).

(74) Agent: **SANFORD T. COLB & CO.**; P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

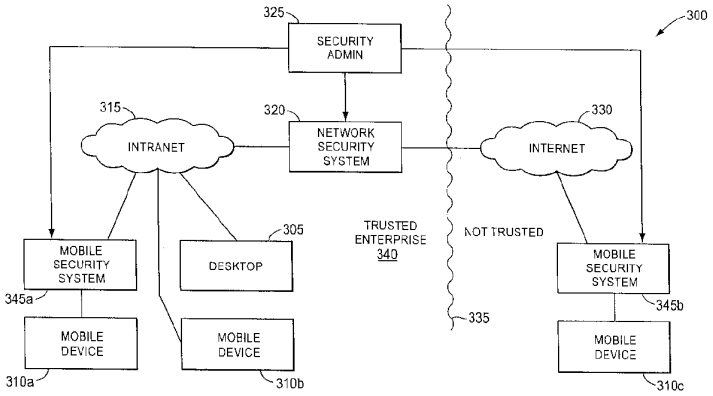


FIG. 3

(57) Abstract: A computer performs dynamic address isolation. The computer comprises an application associated with an application address, a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network, a network address translation engine configured to translate between the application address and a public address, and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The computer may communicate with a firewall configured to handle both network-level security and application-level security.

WO 2008/146296 A2

SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

PRIORITY CLAIM

This application claims benefit of U.S. provisional patent application serial no. 60/940,882, which is hereby incorporated by reference.

TECHNICAL FIELD

This invention relates generally to computer security, and more particularly provides a system and method for providing data and device security between external and host devices.

BACKGROUND

The internet is an interconnection of millions of individual computer networks owned by governments, universities, nonprofit groups, companies and individuals. While the internet is a great source of valuable information and entertainment, the internet has also become a major source of system damaging and system fatal application code, such as "viruses," "spyware," "adware," "worms," "Trojan horses," and other malicious code.

To protect users, programmers design computer and computer-network security systems for blocking malicious code from attacking both individual and network computers. On the most part, network security systems have been relatively successful. A computer that connects to the internet from within an enterprise's network typically has two lines of defense. The first line of defense includes a network security system, which may be part of the network gateway, that includes firewalls, antivirus, antispyware and content filtering. The second line of defense includes individual security software on individual machines, which is not typically as secure as the network security system and is thus more vulnerable to attacks. In combination, the first and second lines of defense together provide pretty good security protection. However, when a device connects to the internet without the intervening network security system, the device loses

its first line of defense. Thus, mobile devices (e.g., laptops, desktops, PDAs such as RIM's Blackberry, cell phones, any wireless device that connects to the internet, etc.) when traveling outside the enterprise network are more vulnerable to attacks.

Figure 1 illustrates an example network system 100 of the prior art. Network system 100 includes a desktop 105 and a mobile device 110, each coupled to an enterprise's intranet 115. The intranet 115 is coupled via a network security system 120 (which may be a part of the enterprise's gateway) to the untrusted internet 130. Accordingly, the desktop 105 and mobile device 110 access the internet 130 via the network security system 120. A security administrator 125 typically manages the network security system 120 to assure that it includes the most current security protection and thus that the desktop 105 and mobile device 110 are protected from malicious code. Demarcation 135 divides the trusted enterprise 140 and the untrusted public internet 130. Because the desktop 105 and the mobile device 110 are connected to the internet 130 via the network security system 120, both have two lines of defense (namely, the network security system 120 and the security software resident on the device itself) against malicious code from the internet 130. Of course, although trusted, the intranet 115 can also be a source of malicious code.

Figure 2 illustrates an example network system 200 of the prior art, when the mobile device 110 has traveled outside the trusted enterprise 140 and reconnected to the untrusted internet 130. This could occur perhaps when the user takes mobile device 110 on travel and connects to the internet 130 at a cybercafé, at a hotel, or via any untrusted wired or wireless connection. Accordingly, as shown, the mobile device 110 is no longer protected by the first line of defense (by the network security system 120) and thus has increased its risk of receiving malicious code. Further, by physically bringing the mobile device 110 back into the trusted enterprise 140 and reconnecting from within, the mobile device 110 risks transferring any malicious code received to the intranet 115.

As the number of mobile devices and the number of attacks grow, mobile security is becoming increasingly important. The problem was emphasized in the recent Info-Security

Conference in New York on December 7-8, 2005. However, no complete solutions were presented.

Similarly, when a host device is connected to an external device such as a USB flash drive, iPod, external hard drive, etc., both devices are vulnerable to receipt of malicious code or transfer of private data. Figure 11 illustrates an example prior art data exchange system 1100 that includes a host computer (host) 1105 and an external device 1110. The host 1105 includes a external device (ED) port 1115, such as a USB port, for receiving the external device 1110. The host 1105 also includes ED drivers 1120 for performing enumeration and enabling communications between the external device 1110 and the host 1105. The external device 1110 includes an ED plug, such as a USB plug, for communicating with the ED port 1115. Both of the host 1105 and external device 1110 are vulnerable to receipt of malicious code or transfer of private data.

Accordingly, there is a need for a system and method of providing security to host and external devices.

SUMMARY

In one embodiment, the present invention provides a computer comprising an application associated with an application address; a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network; a network address translation engine configured to translate between the application address and a public address; and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The network address translation engine may be part of the driver or part of a firewall. The firewall may be located on a mobile security system. The network address translation engine may be configured to use Dynamic Host Configuration Protocol. The computer may be configured to send data packets identifying the application to a firewall, and the firewall may be configured to handle both network-level security and application-level security.

In one embodiment, the present invention provides a system comprising a network interface; a firewall in communication with the network interface configured to handle both network-level security and application-level security; and a computer in communication with the firewall, having one or more applications, and being configured to send data packets identifying the one or more applications to the firewall. Each data may be is associated with one of the one or more applications. Each data packet may comprise data identifying the application associated with the data packet. The firewall may be configured to use the data identifying the application associated with the data packet to handle application-level security, to create a data packet subset by removing the data identifying the application from the data packet, and to send the data packet subset to an external network. The network interface may be configured to receive incoming data from an external network, and to route the incoming data to the firewall. Each application may be associated with at least one address. The firewall may be configured to dynamically isolate the address from an external network. The firewall may be configured to dynamically isolate the address from the external network through the use of Dynamic Host Configuration Protocol.

In one embodiment, the present invention provides a method within a personal computer of processing incoming data associated with a public address, the method comprising receiving the data from an external network; translating the public address into an internal address associated with an application; analyzing the data for malicious code; and routing the data to the application if the data does not comprise malicious code. The analyzing step may comprise analyzing the data for malicious code at both the network level and the application level. The translating step may use Dynamic Host Configuration Protocol.

In one embodiment, the present invention provides a method within a computer of processing outgoing data, the method comprising receiving outgoing data from an application, the application being associated with an internal address; translating the internal address into a public address; and routing at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network. The translating step may use Dynamic Host Configuration Protocol. The method may further comprise configuring the outgoing data into one or more data packets; associating each of the one or more data packets with the application; and embedding application-identifying data in each of the one or more data packets. The method may further comprise creating one or more data packet subsets by removing the application-identifying data from each of the one or more data packets, wherein the routing step comprises routing the one or more data packet subsets to the external network.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art network system in a first state.

Figure 2 is a block diagram of a prior art network system in a second state.

Figure 3 is a block diagram of a network system in accordance with an embodiment of the present invention.

Figure 4 is a block diagram illustrating details of a computer system in accordance with an embodiment of the present invention.

Figure 5 is a block diagram illustrating details of the mobile security system in accordance with an embodiment of the present invention.

Figure 6 is a block diagram illustrating details of the mobile security system in accordance with a Microsoft Window's embodiment.

Figures 7 is a block diagram illustrating details of a smart policy updating system in accordance with an embodiment of the present invention.

Figure 8 is a block diagram illustrating details of network security measures relative to the OSI layers.

Figure 9 is a block diagram illustrating details of the communication technique for spreading security code to the mobile security systems.

Figures 10A-10C are block diagrams illustrating various architectures for connecting a mobile device to a mobile security system, in accordance with various embodiments of the present invention.

Figure 11 is a block diagram illustrating a prior art data exchange system.

Figure 12 is a block diagram illustrating a secure data exchange system, in accordance with an embodiment of the present invention.

Figure 13 is a block diagram illustrating details of a security device, in accordance with an embodiment of the present invention.

Figure 14 is a block diagram illustrating details of a security system, in accordance with an embodiment of the present invention.

Figure 15 is a block diagram illustrating a secure data exchange system, in accordance with another embodiment of the present invention.

Figure 16 is a flowchart illustrating a method of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention.

Figure 17 is a block diagram illustrating a prior art network system having a hardware-based firewall.

Figure 18 is a block diagram illustrating a prior art network system having a software-based firewall.

Figure 19 is a block diagram illustrating a network system that performs dynamic address isolation, in accordance with an embodiment of the present invention.

Figure 20 is a block diagram illustrating a prior art network system having separate network and personal firewalls.

Figure 21 is a block diagram of a network system comprising a hybrid firewall in accordance with an embodiment of the present invention.

Figure 22 is a block diagram illustrating a network system comprising a hybrid firewall and configured according to the embodiment of the present invention shown in Figure 10A.

Figure 23 is a flowchart of a method of routing a data communication from an external network to an application, in accordance with an embodiment of the present invention.

Figure 24 is a flowchart of a method of routing a data communication from an application to an external network, in accordance with an embodiment of the present invention.

Figure 25 is a flowchart of a method of routing a data communication from an external network to an application, in accordance with an embodiment of the present invention.

Figure 26 is a flowchart of a method of routing a data communication from an application to an external network, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

The following description is provided to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the embodiments may be possible to those skilled in the art, and the generic principles defined herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

Figure 3 illustrates a network system 300 in accordance with an embodiment of the present invention. Network system 300 includes a desktop 305, a first mobile device 310a, and a second mobile device 310b. The first mobile device 310a is illustrated as within the enterprise network 340 at this time and is coupled via a mobile security system 345a to the enterprise's intranet 315. The desktop 305 and second mobile device 310b are also within the enterprise network 340 but in this embodiment are coupled to the intranet 315 without an intervening mobile security system 345 such as mobile security system 345b. The intranet 315 is coupled via a network security system 320 (which may be part of the enterprise's gateway) to the untrusted internet 330. Accordingly, the first mobile device 310a, the second mobile device 310b and the desktop 305 access the untrusted internet 330 via the network security system 320. Each may also be protected by a personal security system resident thereon (not shown). A third mobile device 310c is currently outside the enterprise network 340 and is coupled via a mobile security system 345b to the untrusted internet 330. The third mobile device 310 may be in use by an employee of the trusted enterprise 340 who is currently on travel. A security administrator 325 manages the mobile security system 345a, the mobile security system 345b, and the network

security system 320 to assure that they include the most current security protection. One skilled in the art will recognize that the same security administrator need not manage the various devices. Further, the security administrator could be the user and need not be within the trusted enterprise 340.

Demarcation 335 divides the trusted enterprise 340 and the untrusted publicly accessible internet 330. Each of mobile device 310a, 310b and 310c may be referred to generically as mobile device 310, although they need not be identical. Each mobile security system 345a and 345b may be referred to generically as mobile security system 345, although they need not be identical.

As shown, although the mobile device 310c has traveled outside the trusted enterprise 340, the mobile device 310c connects to the untrusted internet 330 via the mobile security system 345b and thus retains two lines of defense (namely, the mobile security system 345b and the security software resident on the device itself). In this embodiment, the mobile security system 345 effectively acts as a mobile internet gateway on behalf of the mobile device 310c. In an embodiment, the mobile security system 345 may be a device dedicated to network security. In an embodiment, each mobile security system 345 may support multiple mobile devices 310, and possibly only registered mobile devices 310, e.g., those belonging to enterprise 340.

Each mobile security system 345 (e.g., 345a, 345b) may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and open-source firewall, IDS/IPS and antivirus protection. The mobile security system 345 may be based on a hardened embedded Linux 2.6.

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b. The security administrator 325 can centrally manage all enterprise devices, remotely or directly. Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security

systems 345 accordingly. Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

The mobile security system 345 may be designed as an add-on to existing software security or to replace all security hardware and software on a traveling mobile device. These security applications will preferably operate on different OSI layers to provide maximum security and malicious code detection, as shown in the example system illustrated in Figure 8. Operating on the lower OSI layers and doing TCP/IP packets analysis only (by screening firewall or router packets) would miss virus and/or worm behavior. Also, many modern viruses use mobile code implemented on a "higher" level than the 7th OSI layer (Application – HTTP, FTP, etc.) and therefore cannot be interpreted at the packet layer nor at the application layer. For example, applying antivirus analysis only at the session or transport layer on a malicious Java Script (that is included in an HTML page), trying to match the signature with packets and without understanding the content type (Java Script), will not detect the malicious nature of the Java Script. To offer greater protection, the mobile security system 345 may act as corporate class security appliance and engage different security applications based on the content type and the appropriate OSI layers, (or even a "higher" level if content is encapsulated in the application layer). The mobile security system 345 may be configured to perform content analysis at different OSI layers, e.g., from the packet level to the application level. It will be appreciated that performing deep inspection at the application level is critical to detect malicious content behavior and improve detection of viruses, worms, spyware, Trojan horses, etc. The following software packages may be implemented on the mobile security system 345:

- Firewall and VPN – including stateful and stateless firewalls, NAT, packet filtering and manipulation, DOS/DDOS, netfilter, isolate user mobile devices from the internet and run VPN program on the device, etc.
- Optional web accelerator and bandwidth/cache management based on Squid.
- IDS/IPS – Intrusion detection and prevention system based on Snort. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol- and anomaly-based inspections.

- Antivirus and antispyware based on ClamAV; additional AV and AS engines, e.g., McAfee, Kaspersky, Pandamay, may be offered for additional subscription fees.
- Malicious Content Detection – on the fly heuristics that perform content analysis to detect malicious content before having signatures. This will be based on a rule base and updated rules and will be content dependent scanning.
- URL Categorization Filtering – based on a commercial engine, such as Surfcontrol, Smart Filters or Websense. May provide around 70 categories of URLs such as gambling, adult content, news, webmail, etc. The mobile device 345 may apply different security policies based on the URL category, e.g., higher restriction and heuristics for Gambling or Adult content web sites, etc.

FIG. 4 is a block diagram illustrating details of an example computer system 400, of which each desktop 305, mobile device 310, network security system 320, mobile security system 345, and security administrator 325 may be an instance. Computer system 400 includes a processor 405, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 410. The computer system 400 further includes an input device 415 such as a keyboard or mouse, an output device 420 such as a cathode ray tube display, a communications device 425, a data storage device 430 such as a magnetic disk, and memory 435 such as Random-Access Memory (RAM), each coupled to the communications channel 410. The communications interface 425 may be coupled directly or via a mobile security system 345 to a network such as the internet. One skilled in the art will recognize that, although the data storage device 430 and memory 435 are illustrated as different units, the data storage device 430 and memory 435 can be parts of the same unit, distributed units, virtual memory, etc.

The data storage device 430 and/or memory 435 may store an operating system 440 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, UNIX OS, LINUX OS and/or other programs 445. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology.

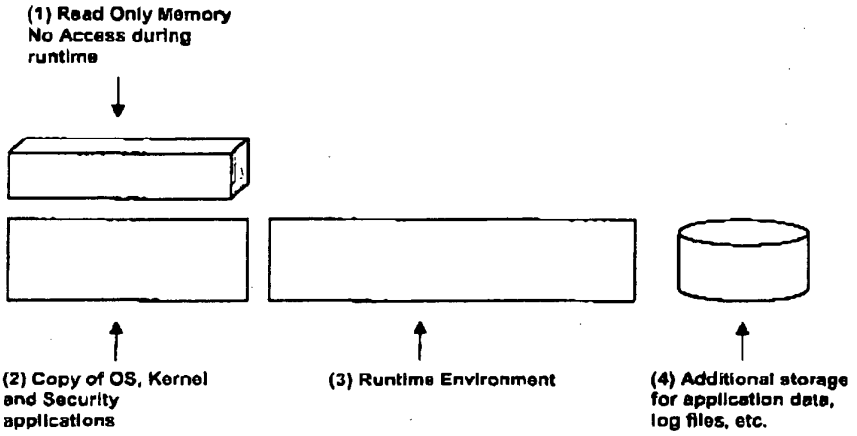
One skilled in the art will recognize that the computer system 400 may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled in the art will also recognize that the programs and data may be received by and stored in the system in alternative ways. For example, a computer-readable storage medium (CRSM) reader 450 such as a magnetic disk drive, hard disk drive, magneto-optical reader, CPU, etc. may be coupled to the communications bus 410 for reading a computer-readable storage medium (CRSM) 455 such as a magnetic disk, a hard disk, a magneto-optical disk, RAM, etc. Accordingly, the computer system 400 may receive programs and/or data via the CRSM reader 450. Further, it will be appreciated that the term "memory" herein is intended to cover all data storage media whether permanent or temporary.

Figure 5 is a block diagram illustrating details of the mobile security system 345 in accordance with an embodiment of the present invention. Mobile security system 345 includes adapters/ports/drivers 505, memory 510, a processor 515, a preboot flash/ROM memory module 520 storing a secure version of the mobile security system's operating system and other applications, network connection module 525, security engines 530, security policies 535, security data 540, remote management module 550, distribution module 555, and backup module 560. Although these modules are illustrated as within the mobile security system 345, one skilled in the art will recognize that many of them could be located elsewhere, e.g., on the security administrator 325 or on third-party systems in communication with the mobile security system 345. The mobile security system 345 may be in a pocket-size, handheld-size or key-chain size housing, or possibly smaller. Further, the mobile security system 345 may be incorporated within the mobile device 310.

The adapters/ports/drivers 505 include connection mechanisms (including software, e.g., drivers) for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection data ports on the mobile security system 345. In one embodiment, the adapters/ports/drivers 505 may be capable of connection to multiple devices 310 to provide network security to the multiple devices 310.

Memory 510 and processor 515 execute the operating system and applications on the mobile security system 345. In this example, the preboot flash 520 stores the operating system and applications. At boot time, the operating system and applications are loaded from the preboot flash 520 into memory 510 for execution. Since the operating system and applications are stored in the preboot flash 520, which cannot be accessed during runtime by the user, the operating system and applications in the preboot flash 520 are not corruptible. Should the copy of the operating system and applications in memory 510 be corrupted, e.g., by malicious code, the operating system and applications may be reloaded into the memory 510 from the preboot flash 520, e.g., upon restart. Although described as stored within the preboot flash 520, the OS and applications can be securely stored within other read-only memory devices, such as ROM, PROM, EEPROM, etc.

Memory (including memory 510 and preboot flash 520) on the mobile security system 345 may be divided into zones as follows:



Upon each "hard" restart, the boot loader (resident at area 1) of the mobile security system 345 copies the kernel and security applications (a fresh unchanged copy) from area 1 to 2. This causes a clean version of the OS and applications to be loaded into area 2 each time. That way, if a special mobile security system 345 attack is developed, the attack will be unable to infect the

system, since the OS and applications are precluded from accessing memory area 1 during runtime. Further, any attack that does reach memory 510 will be able to run only once and will disappear upon a hard restart. A triggering mechanism may be available to restart the mobile security system 345 automatically upon infection detection.

The network connection module 525 enables network connection, e.g., to the internet 330 or the intranet 315 via network communication hardware/software including WiFi, WiMAX, CDMA, GSM, GPRS, Ethernet, modem, etc. For example, if the mobile device 310 wishes to connect to the internet 330 via a WiFi connection, the adapters/ports/drivers 505 may be connected to the PCI port, USB port or PCMCIA port of the mobile device 310, and the network connection module 525 of the mobile security system 345 may include a WiFi network interface card for connecting to wireless access points. Using the network connection module 425, the mobile security system 345 may communicate with the network as a secure gateway for the mobile device 310. Other connection architectures are described in Figures 10A-10C.

The security engines 530 execute security programs based on the security policies 535 and on security data 540, both of which may be developed by IT managers. Security engines 530 may include firewalls, VPN, IPS/IDS, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine 530 may have dedicated security policies 535 and security data 540 to indicate which procedures, content, URLs, system calls, etc. the engines 530 may or may not allow. The security engines 530, security policies 535 and security data 540 may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system 320.

To provide a higher security level provided by antivirus and antispyware software, the security engines 530 on each mobile security system 345 may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. This is because many attacks are hidden within wrong mime types and/or may use

sophisticated tricks to present a text file type to a dangerous active script or ActiveX content type. The HRCF may integrate with a URL categorization security engine 530 for automatic rule adjustment based on the URL category. In one embodiment, when the risk level increases (using the described mechanism) the mobile security system 345 may automatically adjust and increase filtering to remove more active content from the traffic. For example, if greater risk is determined, every piece of mobile code, e.g., Java script, VB script, etc. may be stripped out.

Three aspects for integration with corporate policy server legacy systems include rules, LDAP and active directory, and logging and reporting as discussed below. In one embodiment, a policy import agent running on the security administrator 325 will access the rule base of Checkpoint Firewall-1 and Cisco PIX Firewalls and import them into a local copy. A rule analysis module will process the important rules and will offer out-of-the-box rules and policies for mobile security systems 345. This proposed policy will offer all mobile security systems 345 a best fit of rules that conform the firewall policy of the enterprise 340. The agent will run periodically to reflect any changes and generate updates for mobile security system 345 policies 535. The LDAP and Active Directory may be integrated with the directory service to maintain mobile security system 345 security policies 535 that respond to the enterprise's directory definitions. For example, a corporate policy for LDAP user Group "G" may automatically propagate to all mobile security systems 345 in "G" group. Mobile security system 345 local logs and audit trails may be sent in accordance to a logging and reporting policy to a central log stored at the security administrator 325. Using a web interface, IT may be able to generate reports and audit views related to all mobile device 310 users, their internet experiences, and attempts to bring infected devices back to the enterprise 340. IT will be able to forward events and log records into legacy management systems via SYSLOG and SNMP Traps.

The security engines 530 may perform weighted risk analysis. For example, the security engine 530 may analyze HTTP, FTP, SMTP, POP3, IM, P2P, etc. including any traffic arriving from the internet 330. The security engine 530 may assign a weight and rank for every object based on its type, complexity, richness in abilities, source of the object, etc. The security engine 530 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 530 may assign weight to objects based on the category of the

source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 530 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 530 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

In some embodiments, the security engines 530, security policies 535 and security data 540 may enable bypassing the mobile security system 345. The security policy 535, set by the security administrator 325, may include a special attribute to force network connection through the mobile security system 325 when outside the trusted enterprise 340. Thus, if this attribute is set "on," when a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 and not from within the trusted enterprise 340, all data transfer connections including LAN connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed. The mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330.

In one embodiment, to enable this, when first connecting the mobile security system 345 to the mobile device 310 using for example the USB cable (for both power and USB connection creation), the USB plug & play device driver will be sent into the mobile device 310. The installed driver may be "Linux.inf" which allows a USB-net connection for the mobile security system 345. This connection allows the mobile security system 345 to access the internet 330 via the USB port and using the mobile device 310 network connection plus additional code ("the connection client"). In a Windows example, the connection client may be installed at the NDIS level of the mobile device 310 above all the network interface cards of every network connection as shown in Figure 6. The implementation will be as an NDIS Intermediate (IM) Driver or NDIS-Hooking Filter Driver. Both implementations may be at the kernel level, so that an end user cannot stop or remove it. When starting the mobile device 310, the connection client may attempt to connect to the security administrator 325 or the network security system 320 locally

within the trusted enterprise 340. If the node is not found (finding via VPN is considered as not found in local LAN), the connection client will assume it is working from outside the trusted enterprise 340 and expects to find the mobile security system 345 connected, e.g., via USB-net or other connection mechanism. If the mobile security system 345 is not found, the connection client may avoid any communication to any network connection. By a policy definition, this behavior can be modified to allow communication to the enterprise 340 via VPN installed in the mobile device 310. Similarly, in case of a mobile device system 345 failure, all traffic may be disabled, except for the VPN connection into the enterprise 340.

It will be appreciated that NDIS is one possible implementation of intercepting traffic at the kernel level. For example, in another embodiment, the system may hook Winsock or apply other ways that may be in future Windows versions.

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (e.g., based on for example user preferences or IT decision). Alternatively, it can apply the same engines 530, policies 535 and data 540 for all connected devices 310.

The remote management module 550 enables communication with security administrator 325 (and/or other security administrators), and enables local updating of security engines 530, security policies 535, security data 540 including signatures and other applications. In one embodiment, modification to the security policies 535 and data 540 can be done by the security administrator 325 only. The remote management module 550 of the mobile security system 345 may receive updates from an update authorities device (UAD), e.g., on the security administrator 325 via a secured connection. A UAD may operate on an update server at a customer IT center located on the internet 330 to forward updates to mobile security systems 345 that possibly do not belong to an enterprise 540 in charge of managing updates. A UAD may operate on a mobile security system 345. Security engine 530 updates may modify the antivirus engine DLL, etc. OS and security application updates may be implemented only from within the enterprise 540

while connecting to the security administrator 325 and via an encrypted and authenticated connection.

The security administrator 325 can modify URL black and white lists for remote support to traveling users. In case of false positives, the security administrator 325 may allow access to certain URLs, by bypassing the proactive heuristics security but still monitoring by firewall, antivirus, IPS/IDS, etc. Additional remote device-management features may enable the security administrator 325 to perform remote diagnostics, access local logs, change configuration parameters, etc. on the mobile security system 345. The security administrator 325 may delegate tasks to a helpdesk for support.

The remote management module 550 may communicate with a wizard (e.g., wizard 745), which may be on the security administrator 325, as illustrated in Figure 7, or on another system. Details of the wizard 745 and details of the communication schemes between the remote management module 550 and the wizard 745 are described below with reference to Figure 7.

The distribution module 555 enables distribution of updates, e.g., security policy 535 updates including rule updates, security data 540 updates including signature updates, security engine 530 updates, application/OS updates, etc. by the mobile security system 345 to N other mobile security systems 345. A routing table identifying the N other mobile security systems 345 to whom to forward the updates may be provided to the distribution module 555 to enable system 345 to system 345 communication. Updates may be implemented according to policies set by the security administrator 325. When forwarding updates, the distribution module 555 acts as a UAD.

Each mobile security system 345 may obtain its routing table with security information updates, periodically, at predetermined times, upon login, etc. The routing tables may be maintained on a server, e.g., the security administrator 325 or another mobile security system 345. In one embodiment, the mobile security systems 345 may contact the server to retrieve the routing tables. Alternatively, the server may push the routing tables to the mobile security systems 345.

The distribution module 555 may enable rapid updates as shown in Figure 9. Currently, all commercial antivirus products available do not update devices faster than viruses spread. To assure that a new virus attack does not spread faster than for example signature updates, each mobile security system 345 may be an active UAD. In one embodiment, as shown in Figure 9, each mobile security system 345 is responsible for forwarding the signature updates to four other devices 345. As one skilled in the art will recognize, all devices 345 need to forward to the same number of other devices 345. Multiple devices 345 may be responsible for forwarding to the same device 345. When necessary, offline devices 345 being activated may poll the server, e.g., the security administrator 325, for routing table updates. Many other updating techniques are also possible.

The backup module 560 may constantly backup image and changes of the boot sector and system files of the mobile device 310 into the flash memory 520 or into another persistent memory device. That way, in case of major failure, including a loss of the system or boot sector of the mobile device 310, the mobile security system 345 may be identified as a CD-ROM during reboot and may launch the backup module (or separate program) to restore the boot sector and system files on the mobile device 310, thereby recovering the mobile device 310 without the need for IT support. In an embodiment where the network security system 345 supports multiple mobile devices 310, the backup module 560 may contain separate boot sector and system files for each of the mobile devices 310, if different.

Figure 7 is a block diagram illustrating details of a smart policy updating system 700 in accordance with an embodiment of the present invention. System 700 includes the security administrator 325 coupled to the network security system 320 and to the mobile security system 345. The network security system 320 includes security engines 705, including an antivirus engine 715, an IPS/IDS engine 720, a firewall engine 725, and other security engines. The network security system 320 also includes security policies and data 710, including antivirus policies and data 730, IPS/IDS policies and data 735, firewall policies and data 740, and other policies and data. Similarly, the mobile security system 345 includes an antivirus engine 755, an IPS/IDS engine 760, a firewall engine 765, and other engines. The mobile security system 345

also includes security policies and data 535/540, including antivirus security policies and data 770, IPS/IDS security policies and data 775, firewall security policies and data 780, and other security policies and data.

The security administrator 325 includes a wizard 745 for enabling substantially automatic initial and possibly dynamic setup of the security engines 530, security policies 535 and security data 540 on the mobile security system 345. In one embodiment, the wizard 745 may automatically load all security engines 705 and policies and data 710 of the network security system 320 as the security engines 530 and policies and data 535/540 on the mobile security system 345. In another embodiment, the wizard 745 may include all security engines 705 and policies and data 710 except those known to be irrelevant, e.g., those related to billing software used by accounting, those relating to web software running only on the web servers, etc. In another embodiment, the engines 530 would need to be loaded by an IT manager, and would not be loaded automatically by the wizard 745.

In one embodiment, the wizard 745 may determine whether the mobile security system 345 requires a particular security engine 530, e.g., an antivirus engine 755, IPS/IDS engine 760, firewall engine 765, etc. If so determined, then the wizard 745 would load the engine 530 onto the mobile security system 345. The wizard 745 would then determine which policies and data sets, e.g., some for antivirus engine 755, some for the IPS/IDS engine 760, some for the firewall engine 765, etc. are important to the mobile security system 345. The wizard 745 will then determine which of the antivirus policies and data 730 on the network security system 320 are relevant to the antivirus policies and data 770 on the mobile security system 345, which of the IPS/IDS policies and data 735 on the network security system 320 are relevant to the IPS/IDS policies and data 775 on the mobile security system 345, which of the firewall policies and data 740 on the network security system 320 are relevant to the firewall policies and data 780 on the mobile security system 345, and which of the other policies and data on the network security system 320 are relevant to the policies and data on the mobile security system 345. As stated above, the wizard 745 may determine that all security engines 705 or just a subset are needed on the mobile security system 345. The wizard 745 may determine that all policies and data 710 for a given engine type or just a subset should be forwarded. The wizard 745 may determine which

relevant policies and data 710 should be forwarded to the mobile security system 345 based on rules developed by an IT manager, based on item-by-item selection during the setup procedure, etc. Alternative to the wizard 745, an IT manager can setup the engines 530 and policies and data 535/540 on the mobile security system 345 without the wizard 745.

The security administrator 325 may also include an update authorities device 750. The update authorities device 750 may obtain security system updates (e.g., signature updates) and may send the updates to the network security system 320 and to the mobile security system 345. One skilled in the art will recognize that the updates to the network security system 320 and the updates to the mobile security system 345 need not be the same. Further, the update authorities device 750 may obtain the updates from security managers, security engine developers, antivirus specialists, etc. The update authorities device 750 may forward the updates to all network security systems 320 and all mobile security systems 345, or may forward routing tables to all mobile security systems 345 and the updates only to an initial set of mobile security systems 345. The initial set of mobile security systems 345 may forward the updates to the mobile security systems 345 identified in the routing tables in a P2P manner, similar to the process illustrated in Figure 9. As stated above, each mobile security system 345 operating to forward updates is itself acting as an update authorities device 750.

Other applications may be included on the mobile security system 345. For example, add-on applications for recurring revenue from existing customers may include general email, anti-spam, direct and secured email delivery, information vaults, safe skype and other instant messaging services, etc.

- Email Security and Anti-spam – implementation of mail relay on mobile security systems 345 (including the web security engine above) and a local spam quarantine (based on SendMail or similar process) may implement a complete mail security suite (SMTP and POP3) including anti-spam with real time indexing (via online web spam quarries). Users may have access to the quarantine to review spam messages, release messages, modify and custom spam rules, etc., via a web interface.
- Direct and Secured Email Delivery based on mail relay will allow the mobile security system 345 to send user email directly from one mobile security system 345 to another

mobile security system 345 without using in route mail servers. This allows corporate users to send emails that need not travel in the internet, thus leaving trace and duplicates on different unknown mail servers in route. This combined with the ability to use a secured pipe between two mobile security systems is valuable to corporations. Without such methodology, people could trace emails exchange without accessing to the enterprise's mail server, by tracking down copies in intermediate mail servers that were used to deliver the messages.

- Information Vault – Application to encrypt and store end user information on the mobile security system 345 may be available only to authorized users via a web interface and a web server implemented on every mobile security system 345 (e.g., BOA, Apache, etc.)
- Safe Skype and Other IM – implementing an instant messaging client on the mobile security system 345 can guarantee that the instant messaging system or P2P application has no access to data on the mobile device 310. Adding a chipset of AC/97 to provide a sound interface on the mobile security system 325 could allow users to talk and receive calls directly from/to the mobile security system 325.

Although not shown, a small battery may be included with the mobile security system 345. This battery may be charged by the USB connection during runtime or using the power adapter at any time. The battery may guarantee proper shutdown, e.g., when user disconnects the USB cable from the mobile security system 345. It will be signaled by the system which will launch applications and system shutdown. This will ensure a proper state of the file system and flashing open files buffers.

A multi-layered defense and detection abilities is required. This may be done by a special code that is constantly monitoring the scanning result by different systems (antivirus, IDS/IPS, firewall, antispyware, URL category, etc.) and at different levels to build a puzzle and identify an attack even if its not recognized by each of the individual subsystems. By doing this, the mobile security system 345 will maintain and in some cases even improve the security level provided within the enterprise 540.

One available benefit of the mobile security system 345 is its ability to enforce the policy of the enterprise 540 on the end user while they are traveling or working from home. Since the mobile security system 345 uses similar security engines and policy as when connected from within the enterprise 540 and since the end user cannot access the internet 330 without it (except via VPN connection into the enterprise 540), IT may be capable of enforcing its security policy beyond the boundaries of the enterprise 540. The OS may be under the entire supervision of IT, while the mobile security system 345 OS acts as an end user OS under his control. This resolves the problems of who controls what and how security and productivity face minimal compromise.

A standalone version of the mobile security system 345 may offer the same functionality, and may provide a local management interface via web browser. Attractive to home users and small offices that lack an IT department, the mobile security system 345 enables the end user to launch a browser, connect to the mobile security system 345, set the different policies (update policy, security rules, etc.) including modifying the white and black URL lists, etc. There is also an opportunity to provide end users with a service of remote management of the mobile security systems 345 by subscription.

Figures 10A, 10B and 10C illustrate three example architectures of connecting a mobile security system 345 to a mobile device 310, in accordance with various embodiments of the present invention. In Figure 10A, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1015 and 1020 and is coupled to the internet 330 via a NIC card 1005. The mobile device 310 receives internet traffic from the internet 330 via its NIC card 1005. A kernel-level redirector 1010 (e.g., via NDIS, Winsock, etc.) on the mobile device 310 automatically redirects the internet traffic via the USB connections 1015 and 1020 to the mobile security system 345, which scans, cleans and returns the cleaned internet traffic to the mobile device 310 via the USB connections 1015 and 1020. In Figure 10B, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1025 and 1030. The mobile security system 345 includes a NIC card 1035 for receiving internet traffic from the internet 330. The mobile security system 345 scans, cleans and forwards the internet traffic via the USB connections 1025 and 1030 to the mobile device 310. In Figure 10C, the mobile device 310 is coupled to the mobile security system 345 via NIC cards 1040 and 1045. The mobile security

system 345 receives internet traffic from the internet 330 via its NIC card 1045. The mobile security system 345 scans, cleans and forwards the internet traffic wirelessly via the NIC cards 1040 and 1045 to the mobile device 310. Other connection architectures are also possible.

Figure 12 is a block diagram illustrating a secure data exchange system 1200, in accordance with an embodiment of the present invention. The secure data exchange system 1200 includes a host computer (host) 1205 coupled via a security device 1210 to an external device 1110. The host 1205 may include a laptop, desktop, PDA, mobile phone, or other processor-based device. The external device 1110 may be any external device with memory such as a USB drive, external hard drive, PDA, music player, cell phone, etc. The security device 1210 is communicatively coupled to the host 1205 via an ED port 1225 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and an ED plug 1230 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The external device 1110 is communicatively coupled to the security device 1210 via an ED port 1235 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and ED plug 1120 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The connector type of the ED port 1225 and ED plug 1230 combination may be different that the connector type of the ED port 1235 and ED plug 1120 combination. In one embodiment, all ports 1225/1235 and plugs 1230/1120 are USB. Although the plugs 1120/1230 are illustrated as male and ports 1225/1235 are shown as female, one skilled in the art will recognize that the opposite is possible (plugs 1120/1230 may be female and ports 1225/1235 may be male).

The host 1205 includes ED drivers 1220 for performing enumeration and enabling communication with the security device 1210. Similarly, the security device 1210 includes ED drivers 1245 for performing enumeration and enabling communication with the external device 1110.

In one embodiment, the security device 1210 includes a programmable hardware appliance capable of enforcing security policies to protect against malicious code such as viruses,

spyware, adware, Trojan Horses, etc. and to protect against transfer of private data. In one embodiment, the security device 1210 is configured to protect both the host 1205 and the external device 1215. In one embodiment, the security device 1210 is configured to protect only one of the external device 1110 or the host 1205. Additional details of the security device 1210 are provided with reference to Figures 13 and 14.

Figure 13 is a block diagram illustrating details of the security device 1210, in accordance with an embodiment of the present invention. The security device 1210 include a processor 1305, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 1315. The security device 1210 further includes an ED plug 1230, an ED port 1235, a communications interface 1310, storage 1320 such as an EEPROM, and memory 1325 such as Random-Access Memory (RAM) or Read Only Memory (ROM), each coupled to the communications channel 1315. The communications interface 1310 may be coupled to a network such as the internet. One skilled in the art will recognize that, although the storage 1320 and memory 1325 are illustrated as different units, the data storage device 1320 and memory 1325 can be parts of the same unit, distributed units, virtual memory, etc. The term "memory" herein is intended to cover all data storage media whether permanent or temporary. One skilled in the art will recognize that the security device 1210 may include additional components, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc.

As shown, memory 1325 stores an operating system 1330 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, Unix OS, Linux OS, etc. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology. The memory 1325 also stores ED drivers 1245 and a security system 1335. The ED drivers 1245 may include standard drivers for standard external devices 1110 and proprietary drivers for proprietary external devices 1110. The ED drivers 1245 may be transferred onto the

memory 1325 via ED plug 1230. The security system 1335 includes code for enforcing security policies on data transfer actions between the host 1205 and external device 1110.

Figure 14 is a block diagram illustrating details of a security system 1335, in accordance with an embodiment of the present invention. The security system 1335 includes a security manager 1405, security engines 1410, security policies 1415, and security data 1420.

In one embodiment, the security manager 1405 includes code for performing enumeration, namely, to identify the external device 1110 or external device 1110 type and to identify the corresponding ED driver 1245 capable of establishing communication between the security device 1210 and the external device 1110. The security manager 1405 also includes code to control execution of the various security engines 1410 based on the security policies 1415 and security data 1420 to evaluate data transfer requests or other device requests. Further, the security manager 1405 includes code to communicate with the host 1205, which will be the source of the data transfer and/or other requests.

In one embodiment, the security engines 1410 includes code for securing the transfer of data between the host 1205 and the external device 1110 based on the security policies 1415 and security data 1420. The security engines 1410 may include firewalls, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. The security engines 1410 may also include data privacy modules to enforce data privacy policies 1415. Each security engine 1410 may have dedicated security policies 1415 and security data 1420 to indicate which procedures, URLs, system calls, content, ID, etc. the data requested for transfer may contain or whether the data requested for transfer is considered nontransferable (or nontransferable without additional security measure such as a password and ID).

To provide a higher security level, the security engines 1410 may implement content analysis and risk assessment algorithms. In one embodiment, a security engine 1410 assigns a weight and rank for every transfer object based on its type, complexity, richness in abilities, source, etc. The security engine 1410 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 1410 may assign weight to objects

based on the category of the source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 1410 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 1410 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

Thus, upon receiving a data transfer and/or other request from the host 1205, the security manager 1405 will launch the appropriate security engines 1410 based on the security policies 1415. For example, the security policies 1415 may be configured not to allow specific ActiveX controls to be loaded from the host 1205 onto the external device 1110. The security policies 1415 may be configured not to allow data transfer from private folders on the host 1205 to the external device 1110. The security manager 1405 will launch the appropriate security engines 1410 to assure that these example security policies 1415 are met. Further, the security engines 1410 may use security data 1420, which may include definition files of malicious ActiveX controls, locations of private folders, etc.

Although not shown, the security system 1335 may include additional components such as the preboot flash 520 with OS and applications, the remote management module 550, the distribution module 555, and the backup module 560 discussed above with reference to Figure 5. Other components are also possible.

Figure 15 is a block diagram illustrating a secure data exchange system 1500, in accordance with another embodiment of the present invention. The secure data exchange system 1500 includes a security device 1505 communicatively coupled to the host 1520 via an ED plug 1515 on the security device 1505 and a first ED port 1525 on the host 1520. The secure data exchange system 1500 also includes an external device 1110 communicatively coupled to the host 1520 via the ED plug 1120 on the external device 1110 and a second ED port 1535 on the host 1520.

Because the external device 1110 is not directly coupled to the security device 1505, the security device 1505 is not physically intercepting the data transfer requests between the external device 1110 and the host 1520. Accordingly, in this embodiment, the host 1520 includes a redirect driver 1530, which is configured to redirect data transfer requests between the external device 1110 and the host 1520 regardless of data transfer direction. In one embodiment, the security device 1505 may be configured to protect only one of the external device 1110 or the host 1520. Further, in one embodiment, the security device 1505 does not contain any ED drivers, e.g., ED drivers 1245.

In one embodiment, if the security device 1505 is not coupled to the host 1520, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110. In one embodiment, the host 1520 is configured not to communicate with the external device 1110 until the security device 1505 is coupled to the host 1520. In one embodiment, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110 only if additional security measures are taken, such as receipt of a password and ID, or until the security device 1505 is coupled to the host 1520.

In one embodiment, the host 1520 may conduct enumeration of the security device 1505 upon connection of the security device 1505 to the ED port 1525. Upon identifying the security device 1505 or security device 1505 type, the host 1520 may initiate the redirect driver 1530 to redirect all data transfer requests or other external device 1110 requests from all other ED ports 1535 to the security device 1505. In one embodiment, the redirect driver 1530 only accepts data transfer requests from the security device 1505, which presents the requests of the external device 1110 as a proxy. In one embodiment, the redirect driver 1530 performs data transfer requests received from the external device 1110 only after the security device 1505 has conducted its check and given its authorization. Other protocols are also possible.

Figure 16 is a flowchart illustrating a method 1600 of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention. The method 1600 begins in step 1605 with the security device 1505 being connected to the first ED

port 1525 of the host 1520. The external device 1110 in step 1610 is connected to the second ED port 1535 of the host 1520. The host 1505 in step 1615 performs enumeration techniques to identify the security device 1505 and the external device 1110 and to install the appropriate drivers 1530/1540 to enable communication with the security device 1505 and the external device 1110. The redirect driver 1530 in step 1620 receives a data transfer request from either the host 1505 to the external device 1110 or from the external device 1110 to the host 1505. The redirect driver 1530 in step 1625 redirects the data transfer request to the security device 1505, which in step 1630 enforces its security policies (antivirus, antispyware, anti-adware, data privacy, etc.) on the data transfer request. The security device 1505 in step 1635 determines whether the data transfer request passes the security policies. If so, then the security device 1505 in step 1640 authorizes the data transfer request and the host 1520 in step 1645 performs the data transfer request. If not, then the security device 1505 in step 1650 rejects the data transfer request. Method 1600 then ends.

It will be appreciated that, in one embodiment, the security device 1210/1505 may be implemented as part of the host 1205/1520, e.g., within the housing of the host 1205/1520 and/or as a security procedure executed by the host 1205/1520.

Dynamic Isolation

Figure 17 shows a prior art network system 1700 having a hardware-based firewall. The network system 1700 includes internal computers 1705a and 1705b, a first network interface card (NIC) 1710, a hardware-based firewall 1715 that performs network address translation (NAT), a second NIC 1720, an external network 1725 (such as the Internet), and external computers 1730a and 1730b.

The firewall 1715 is a hardware-based firewall, such as Check Point FW-1 or Cisco PIX. The firewall uses two different network ports (the first NIC 1720 and the second NIC 1720) to separate and isolate the internal computers 1705a and 1705b from the external network 1720. The firewall 1715 uses network address translation (NAT) to translate the Internet Protocol (IP) address of the internal computer 1705a (denoted as IP address x) and the IP address of the

internal computer 1705b (denoted as IP address y) into a public IP address z, thus hiding the IP addresses of the internal computers 1705a and 1705b. The firewall 1715 performs a similar translation on the Media Access Control (MAC) addresses of the internal computers 1705a and 1705b.

The network system 1700 provides a higher level of security than PC software-based firewalls (such as Microsoft Windows Personal Firewall and Check Point ZoneAlarm) running on the internal computers 1705a and 1705b themselves, since PC software-based firewalls do not hide the IP and MAC addresses of the internal computers.

Figure 18 shows a prior art network system 1800 having a software-based firewall. The network system 1800 includes an external network 1805 (such as the Internet), one or more NICs 1810 (denoted as 1810a, 1810b, ... 1810n), a Network Driver Interface Specification (NDIS) driver 1815 that acts as an interface between layer 2 (the data link layer) and layer 3 (the network layer), an intermediate driver 1820 (such as MINIPort in the Microsoft Windows operating system), a software-based firewall 1825, an operating system 1830, and one or more applications 1835 (denoted as 1835a, 1835b, ... 1835m). The operating system 1830 contains a TCP/IP protocol suite 1840.

In operation, the intermediate driver 1820 directs traffic arriving from the NICs 1810 and NDIS driver 1815 to the software-based firewall 1825. The software-based firewall 1825 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to the operating system 1830.

The network system 1800 does not use a hardware-based firewall. Only one of the NICs 1810 needs to be used at any given time. However, the IP and MAC addresses of the NICs 1810 (which are visible to the external network 1805) are the same IP and MAC addresses that are viewed and used by the applications 1835 (i.e., there is no address isolation between the applications 1835 and the external network 1805).

Figure 19 shows a network system 1900 that performs dynamic address isolation, in accordance with an embodiment of the present invention. The network system 1900 includes an external network 1905 (such as the Internet), one or more NICs 1910 (denoted as 1910a, 1910b, ... 1910n), an NDIS driver 1915 that acts as an interface between layer 2 (the data link layer) and layer 3 (the network layer), an intermediate driver 1920, a software-based or hardware-based firewall 1925, an operating system 1930, and one or more applications 1935 (denoted as 1935a, 1935b, ... 1935m). The operating system 1930 contains the TCP/IP protocol suite 1940. The intermediate driver 1920 includes a NAT engine 1945, which contains a translations table for IP and MAC addresses.

The NICs 1910, NDIS driver 1915, intermediate driver 1920, firewall 1925, operating system 1930, and applications 1935 may be installed in a mobile device 310. The firewall 1925 may be an external firewall 1925 connected to the intermediate driver 1920 by a Universal Serial Bus (USB) connection, a wireless connection, or another network wire connection. For example, the firewall 1925 may be part of the mobile security system 345.

In operation, the intermediate driver 1920 receives all data packets arriving from the NICs 1910 and NDIS driver 1915, and routes each data packet to the NAT engine 1945. The NAT engine 1945 uses Dynamic Host Configuration Protocol (DHCP) to dynamically isolate the IP addresses of the applications 1935 from the external network 1905. As shown in Figure 19, the dynamic NAT engine 1945 translates the IP address of the application 1935 (IP address x) to a different IP address (IP address z) while interfacing with the NIC, and translates the IP address z back to the IP address x when sending data to the operating system 1930. Thus, the intermediate driver 1920 provides IP address z to the external network 1905, while isolating IP address x from the external network. The NAT engine 1945 performs a similar translation on MAC addresses, if necessary. As shown, the NAT engine 1945 is part of the intermediate driver 1920. However, one skilled in the art will recognize that the NAT engine 1945 may be located elsewhere, e.g., on the mobile security system 345, part of the firewall 1925, etc.

After the NAT engine 1945 translates the IP address, the intermediate driver 1920 directs each data packet to the firewall 1925. The firewall 1925 decides what to do with each data

packet (allow, deny, or reject) and permits only the allowed data packets to proceed to the operating system 1930. The intermediate driver 1920 receives each allowed data packet back from the firewall 1925 and routes each allowed data packet to an application 1935.

For outgoing data packets, the intermediate driver 1920 receives each data packet from the application 1935 and routes each data packet to the NAT engine 1945. The NAT engine 1945 translates the IP and/or MAC address associated with the data packet as described above. The intermediate driver 1920 then receives each data packet (containing the translated IP and/or MAC address) back from the NAT engine 1945 and routes each data packet to the external network 1905.

In this way, the network system 1900 is able to isolate the IP and MAC addresses of internal computers/applications from the external network 1905, while not requiring the use of a hardware-based firewall or more than one NIC. Network isolation and separation is achieved even if the firewall lacks more than one NIC.

Thus, a connection between a mobile security system 345 and a mobile device 310 may be implemented while using the principles of NAT and DHCP, so that end-user applications running on the mobile device 310 will "see" protected virtual IP and MAC addresses, while devices connected to the external network see different physical IP and MAC addresses. The present invention provides similar protection and IP hiding that a hardware-based firewall having two network ports (internal and external) provides to a mobile device, but without the need to use a hardware-based firewall and two or more network ports.

Figure 23 is a flowchart of a method 2300 of routing a data communication from an external network (such as the external network 1905) to an application (such as application 1935), in accordance with an embodiment of the present invention. In step 2305, a NIC (such as NIC 1910) receives a data communication from the external network. Data specifying an external IP address and an external MAC address are embedded in the data communication. In step 2310, the data communication is routed to an intermediate driver (such as the intermediate driver 1920),

which in turn routes the data communication to a NAT engine (such as the NAT engine 1945). The NAT engine contains a translations table for IP and MAC addresses.

In step 2315, the NAT engine uses DHCP to translate the external IP and MAC addresses embedded in the data communication into internal IP and MAC addresses. The NAT engine then substitutes the internal IP and MAC addresses for the external IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2320, the intermediate driver routes the data communication to a firewall (such as the firewall 1925). In step 2325, the firewall analyzes the data communication for malicious code. In step 2330, the firewall decides what to do with the data communication. If the data communication was found to contain malicious code, then the method 2300 proceeds to step 2335. In step 2335, the firewall rejects the data communication and prevents it from proceeding to the application. The method 2300 then ends.

If the data communication was not found to contain malicious code, then the method 2300 proceeds to step 2340. In step 2340, the firewall allows the data communication. The intermediate driver receives the data communication back from the firewall and routes the data communication to the application. The method 2300 then ends.

Figure 24 is a flowchart of a method 2400 of routing a data communication from an application (such as application 1935) to an external network (such as the external network 1905), in accordance with an embodiment of the present invention. In step 2405, the application initiates a data communication. The application may embed data specifying an internal IP address and an internal MAC address in the data communication. In other embodiments, the internal IP address and the internal MAC address may be embedded by an operating system (such as the operating system 1930).

In step 2410, the data communication is routed to an intermediate driver (such as the intermediate driver 1920), which in turn routes the data communication to a NAT engine (such

as the NAT engine 1945). The NAT engine contains a translations table for IP and MAC addresses. In step 2415, the NAT engine uses DHCP to translate the internal IP and MAC addresses embedded in the data communication into external IP and MAC addresses. The NAT engine then substitutes the external IP and MAC addresses for the internal IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2420, the internal driver routes the data communication to the external network via a NIC (such as NIC 1910). The method 2400 then ends.

Hybrid Firewall

Figure 20 shows a prior art network system 2000 having separate network and personal firewalls. The network system 2000 includes an external network 2005 (such as the Internet), a network firewall 2010, and personal computers 2015 (denoted as 2015a, 2015b, etc.). The network firewall 2010 may reside on an external device or computer. The network firewall 2010 comprises a first NIC 2020, a NAT gateway 2025 and a second NIC 2030. Each personal computer 2015 comprises a personal firewall 2035 (denoted as 2035a, 2035b, etc.) and an application 2040 (denoted as 2040a, 2040b, etc.).

In operation, the network firewall 2010 uses the NAT gateway 2025 to translate the IP address of the personal computer 2015a (denoted as IP address x) and the IP address of the personal computer 2015b (denoted as IP address y) into a public IP address z, and thus hide the IP addresses of the personal computers 2105. The network firewall 2010 performs a similar translation on the MAC addresses of the personal computers 2015. The network firewall 2010 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. Because the network firewall 2010 is earlier in the network than the personal firewall 2035, it can stop malicious code before it enters the system 2000. However, because the network firewall 2010 is application insensitive and at a lower layer of the information stack, its processes for malicious code detection are limited.

The personal firewall 2035 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. Because the personal firewall 2035 is application sensitive and at a higher layer of the information stack, its processes for malicious code detection can be more thorough and focused.

Figure 21 shows a network system 2100 comprising a hybrid firewall 2110 in accordance with an embodiment of the present invention. The network system 2100 includes an external network 2105 (such as the Internet), a hybrid network/personal firewall 2110, and personal computers 2115 (denoted as 2115a, 2115b, etc.).

The hybrid firewall 2110 may reside on an external device or computer. In other embodiments, the hybrid firewall 2110 may reside on the mobile security system 345, shown in Figures 10A-10C. The hybrid firewall 2110 comprises a first NIC 2120, a NAT engine 2125 and a second NIC 2130.

Each personal computer 2115 comprises an agent 2135 (denoted as 2135a, 2135b, etc.) and one or more applications 2140 (denoted as 2140a, 2140b, etc.). As shown in Figure 21, the network system 2100 comprises only two personal computers 2115, but in other embodiments the network system 2100 may comprise more than two personal computers.

In operation, the hybrid firewall 2110 uses the NAT engine 2125, which contains a translations table for IP and MAC addresses, to translate the IP address of the personal computer 2115a (denoted as IP address x) and the IP address of the personal computer 2115b (denoted as IP address y) into a public IP address z, and thus hide the IP addresses of the personal computers. The network firewall 2110 performs a similar translation on the MAC addresses of the personal computers 2115.

The hybrid firewall 210 is capable of performing both the network firewall and personal firewall security measures. Because the hybrid firewall 2010 is at the same level as the traditional network firewall 2035, it can stop malicious code before it enters the system 2100.

Further, because the hybrid firewall 2110 is application sensitive, the hybrid firewall 2110 can perform the processes of the traditional personal firewall 2035.

To enable the hybrid firewall 2110 to be application sensitive, the agents 2135 send packets of data to the hybrid firewall 2110, each packet comprising data identifying the application 2140 associated with the packet. Because each packet comprises data identifying the application 2140 that is associated with the packet, the hybrid firewall 2110 can act as a personal firewall 2035 to handle application-level security. Then, the hybrid firewall 2110 can transmit a subset of the data packets, by extracting at least the application-identifying data, to the external network 2105.

Figure 22 shows a network system 2200 comprising a hybrid firewall 2210 and configured according to the embodiment of the present invention shown in Figure 10A. The network system 2200 includes an external network 2205 (such as the Internet), a hybrid network/personal firewall 2210, and a mobile device 2215.

The hybrid firewall 2210 may reside on an external device in a pocket-size, handheld-size, keychain-size, or possibly smaller housing. The hybrid firewall 2210 comprises an ED plug 2245 (such as a USB plug) for communicating with an ED port 2230 (such as a USB port) contained within the mobile device 2215. The hybrid firewall 2210 also comprises a NAT engine 2225. In other embodiments, the hybrid firewall 2210 may be installed in the mobile device 2215, or connected to the mobile device 2215 by a wireless or another network wire connection.

The mobile device 2215 comprises a NIC 220, the ED port 2230, an agent 2235, one or more applications 2240, and an intermediate driver 2250 (such as MINIPort in the Microsoft Windows operating system). As shown in Figure 22, the network system 2200 comprises only one mobile device 2215 and hybrid firewall 2210, but in other embodiments the network system 2200 may comprise more than one mobile device and hybrid firewall.

In operation, the intermediate driver 2250 directs traffic arriving from the NIC 2220 to the hybrid firewall 2210 via the ED port 2230 and ED plug 2245. The hybrid firewall 2210 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to an application 2240.

The hybrid firewall 2210 uses the NAT engine 2225, which contains a translations table for IP and MAC addresses, to translate the IP address of the mobile device 2215 into a public IP address, and thus hide the IP address of the mobile device 2215. The hybrid firewall 2210 performs a similar translation on the MAC address of the mobile device 2215.

The application 2240 can send packets of data via the ED port 2230 and ED plug 2235 to the hybrid firewall 2210 for transmission to the external network 2205. The agent 2235 associates data identifying the application 2240 with the packets of data that are sent to the hybrid firewall 2210. Each packet thus comprises data identifying the application 2240 associated with the packet. Because each packet comprises data identifying the application 2240 associated with the packet, the hybrid firewall 2210 can act as a personal firewall to handle application security.

Figure 25 is a flowchart of a method 2500 of routing a data communication from an external network (such as the external network 2105 or 2205) to an application (such as application 2140 or 2240), in accordance with an embodiment of the present invention. In step 2505, a NIC (such as NIC 2120 or 2220) receives a data communication from the external network. Data specifying an external IP address and an external MAC address are embedded in the data communication. In step 2510, the data communication is routed to a hybrid network/personal firewall (such as the firewall 2110 or 2210) that comprises a NAT engine (such as the NAT engine 2125 or 2225) containing a translations table for IP and MAC addresses. The hybrid firewall is at the same level as a traditional network firewall and is application sensitive.

In step 2515, the NAT engine uses DHCP to translate the external IP and MAC addresses embedded in the data communication into internal IP and MAC addresses. The NAT engine then substitutes the internal IP and MAC addresses for the external IP and MAC addresses in the

data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2520, the hybrid firewall associates the data communication with an application. The hybrid firewall makes this association based upon data packets previously received by the firewall that comprised application-identifying information.

In step 2525, the hybrid firewall analyzes the data communication for malicious code. Because the hybrid firewall is at the same level as a traditional network firewall, it can stop malicious code before it reaches a computer (such as computer 2115 or 2215). Further, because the hybrid firewall is application sensitive, the hybrid firewall can perform the function of a traditional personal firewall to handle application-level security.

In step 2530, the firewall decides what to do with the data communication. If the data communication was found to contain malicious code, then the method 2500 proceeds to step 2535. In step 2535, the firewall rejects the data communication and prevents it from proceeding to the application. The method 2500 then ends.

If the data communication was not found to contain malicious code, then the method 2500 proceeds to step 2540. In step 2540, the firewall allows the data communication, and the data communication is routed to the application. The method 2500 then ends.

Figure 26 is a flowchart of a method 2600 of routing a data communication from an application (such as application 2140 or 2240) to an external network (such as the external network 2105 or 2205), in accordance with an embodiment of the present invention. In step 2605, the application initiates a data communication. The application may embed data specifying an internal IP address and an internal MAC address in the data communication. In other embodiments, the internal IP address and the internal MAC address may be embedded by an operating system or by an agent (such as the agent 2135 or 2235) running on a computer.

In step 2610, data identifying the application is embedded in the data communication. This step may be performed by the application, by an operating system, or by an agent (such as the agent 2135 or 2235) running on a computer. In one embodiment, an agent running on the same computer as the application creates packets of data, each packet comprising data identifying the application associated with the packet. Because each packet comprises data identifying the application that is associated with the packet, a downstream hybrid firewall (such as the firewall 2110 or 2210) can act as a personal firewall to handle application-level security.

In step 2615, the data communication is routed to a hybrid network/personal firewall (such as the firewall 2110 or 2210) that comprises a NAT engine (such as the NAT engine 2125 or 2225) containing a translations table for IP and MAC addresses. The hybrid firewall is at the same level as a traditional network firewall and is application sensitive.

In step 2620, the hybrid firewall extracts and removes the application-identifying information from the data communication. In step 2625, the NAT engine uses DHCP to translate the internal IP and MAC addresses embedded in the data communication into external IP and MAC addresses. The NAT engine then substitutes the external IP and MAC addresses for the internal IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2630, the data communication (minus data identifying the application, internal IP address, and internal MAC address) is routed to the external network via a NIC (such as NIC 2120 or 2220). The method 2600 then ends.

The foregoing description of the preferred embodiments of the present invention is by way of example only, and other variations and modifications of the above-described embodiments and methods are possible in light of the foregoing teaching. Although the network sites are being described as separate and distinct sites, one skilled in the art will recognize that these sites may be a part of an integral site, may each include portions of multiple sites, or may include combinations of single and multiple sites. The various embodiments set forth herein may be implemented utilizing hardware, software, or any desired combination thereof. For that

matter, any type of logic may be utilized which is capable of implementing the various functionality set forth herein. Components may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. Connections may be wired, wireless, modem, etc. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

CLAIMS

1. A computer comprising:

an application associated with an application address;

a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network;

a network address translation engine configured to translate between the application address and a public address; and

a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address.

2. The computer of claim 1, wherein the network address translation engine is part of the driver.

3. The computer of claim 1, wherein the network address translation engine is part of a firewall.

4. The computer of claim 3, wherein the firewall is located on a mobile security system.

5. The computer of claim 1, wherein the network address translation engine is configured to use Dynamic Host Configuration Protocol.

6. The computer of claim 1, wherein the computer is configured to send data packets identifying the application to a firewall, and the firewall is configured to handle both network-level security and application-level security.

7. A system comprising:

a network interface;

a firewall in communication with the network interface configured to handle both network-level security and application-level security; and

a computer in communication with the firewall, having one or more applications, and being configured to send data packets identifying the one or more applications to the firewall.

8. The system of claim 7, wherein:

each data packet is associated with one of the one or more applications; and

each data packet comprises data identifying the application associated with the data packet.

9. The system of claim 8, wherein the firewall is configured to use the data identifying the application associated with the data packet to handle application-level security, to create a data packet subset by removing the data identifying the application from the data packet, and to send the data packet subset to an external network.

10. The system of claim 7, wherein the network interface is configured to receive incoming data from an external network, and to route the incoming data to the firewall.

11. The system of claim 7, wherein:

each application is associated with at least one address; and

the firewall is configured to dynamically isolate the address from an external network.

12. The system of claim 11, wherein the firewall is configured to dynamically isolate the address from the external network through the use of Dynamic Host Configuration Protocol.

13. A method within a personal computer of processing incoming data associated with a public address, the method comprising:

receiving the data from an external network;

translating the public address into an internal address associated with an application;

analyzing the data for malicious code; and

routing the data to the application if the data does not comprise malicious code.

14. The method of claim 13, wherein the analyzing step comprises analyzing the data for malicious code at both the network level and the application level.

15. The method of claim 13, wherein the translating step uses Dynamic Host Configuration Protocol.

16. A method within a computer of processing outgoing data, the method comprising:

receiving outgoing data from an application, the application being associated with an internal address;

translating the internal address into a public address; and

routing at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network.

17. The method of claim 16, wherein the translating step uses Dynamic Host Configuration Protocol.

18. The method of claim 16, further comprising:

configuring the outgoing data into one or more data packets;

associating each of the one or more data packets with the application; and

embedding application-identifying data in each of the one or more data packets.

19. The method of claim 18,

further comprising creating one or more data packet subsets by removing the application-identifying data from each of the one or more data packets,

wherein the routing step comprises routing the one or more data packet subsets to the external network.

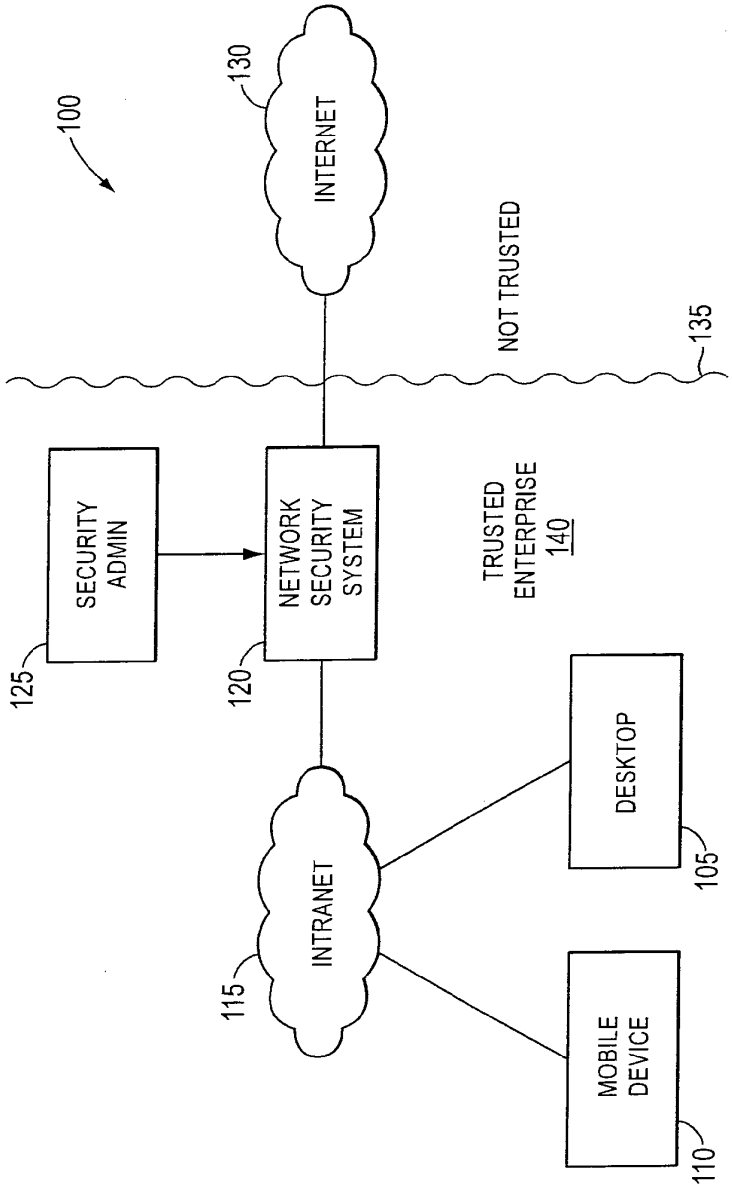


FIG. 1
(PRIOR ART)

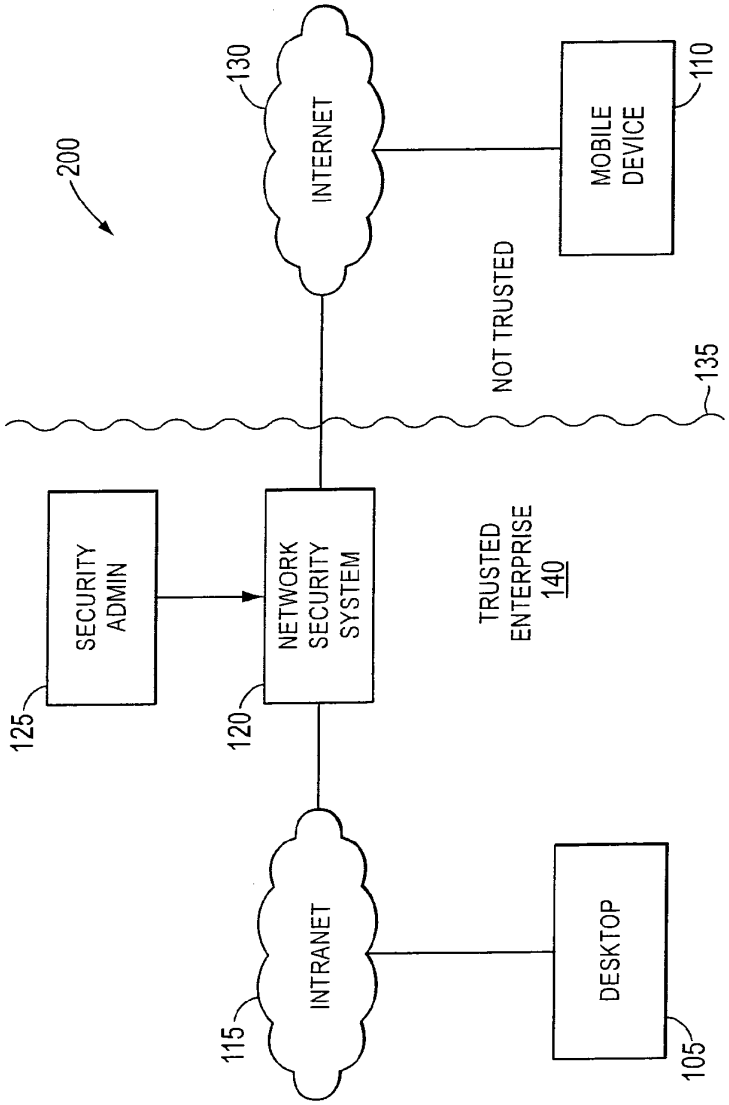


FIG. 2
(PRIOR ART)

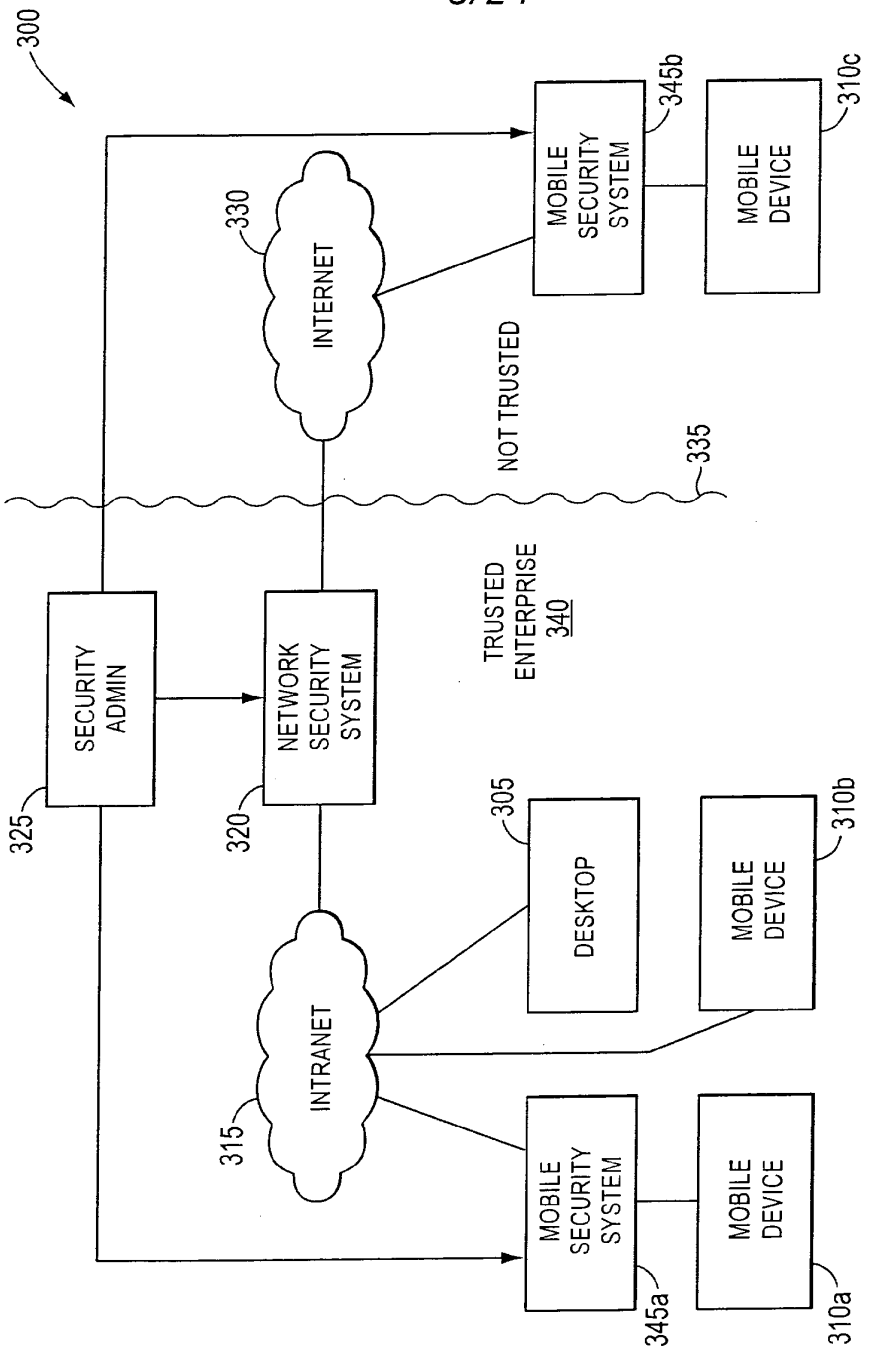

300
MOBILE SECURITY SYSTEM
345b
MOBILE DEVICE
310c
330
INTERNET
NOT TRUSTED
335
TRUSTED ENTERPRISE 340
SECURITY ADMIN
325
NETWORK SECURITY SYSTEM
320
305
DESKTOP
MOBILE DEVICE
310b
INTRANET
315
MOBILE SECURITY SYSTEM
345a
MOBILE DEVICE
310a

FIG. 3

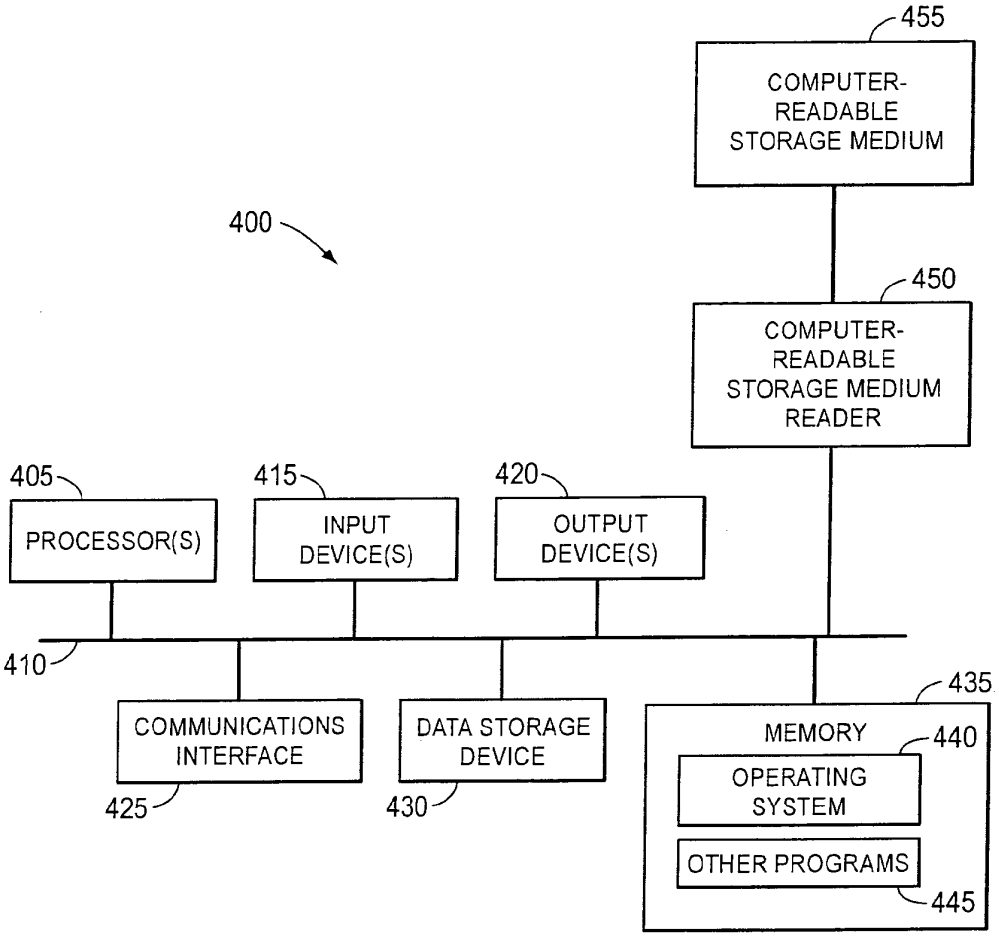

455
COMPUTER-READABLE STORAGE MEDIUM
400
450
COMPUTER-READABLE STORAGE MEDIUM READER
405
PROCESSOR(S)
415
INPUT DEVICE(S)
420
OUTPUT DEVICE(S)
410
435
COMMUNICATIONS INTERFACE
425
DATA STORAGE DEVICE
430
MEMORY
440
OPERATING SYSTEM
OTHER PROGRAMS
445

FIG. 4

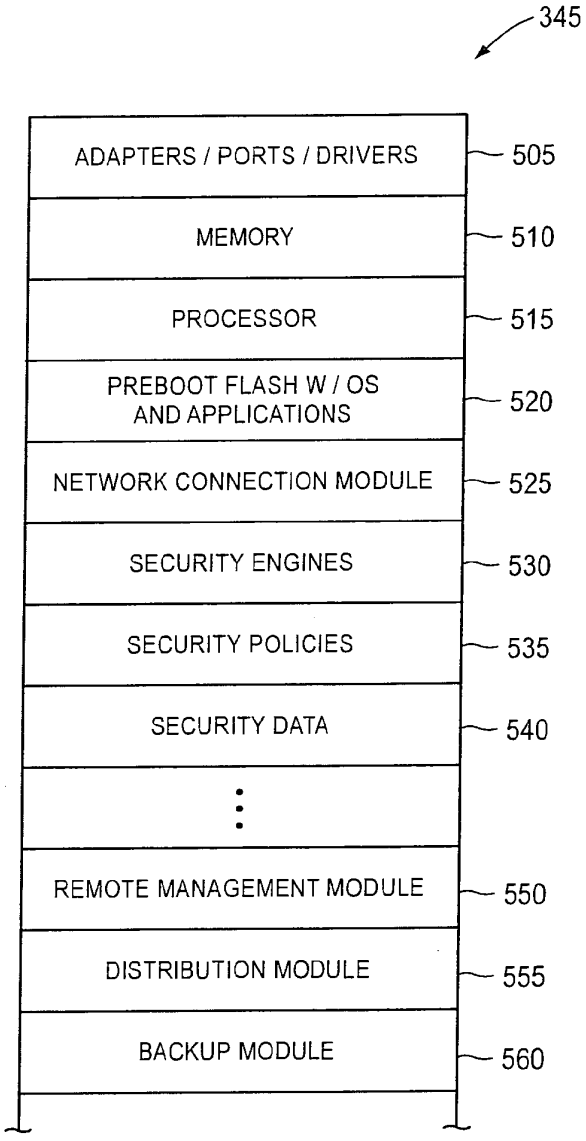

345
ADAPTERS / PORTS / DRIVERS
505
MEMORY
510
PROCESSOR
515
PREBOOT FLASH W / OS AND APPLICATIONS
520
NETWORK CONNECTION MODULE
525
SECURITY ENGINES
530
SECURITY POLICIES
535
SECURITY DATA
540
REMOTE MANAGEMENT MODULE
550
DISTRIBUTION MODULE
555
BACKUP MODULE
560

FIG. 5

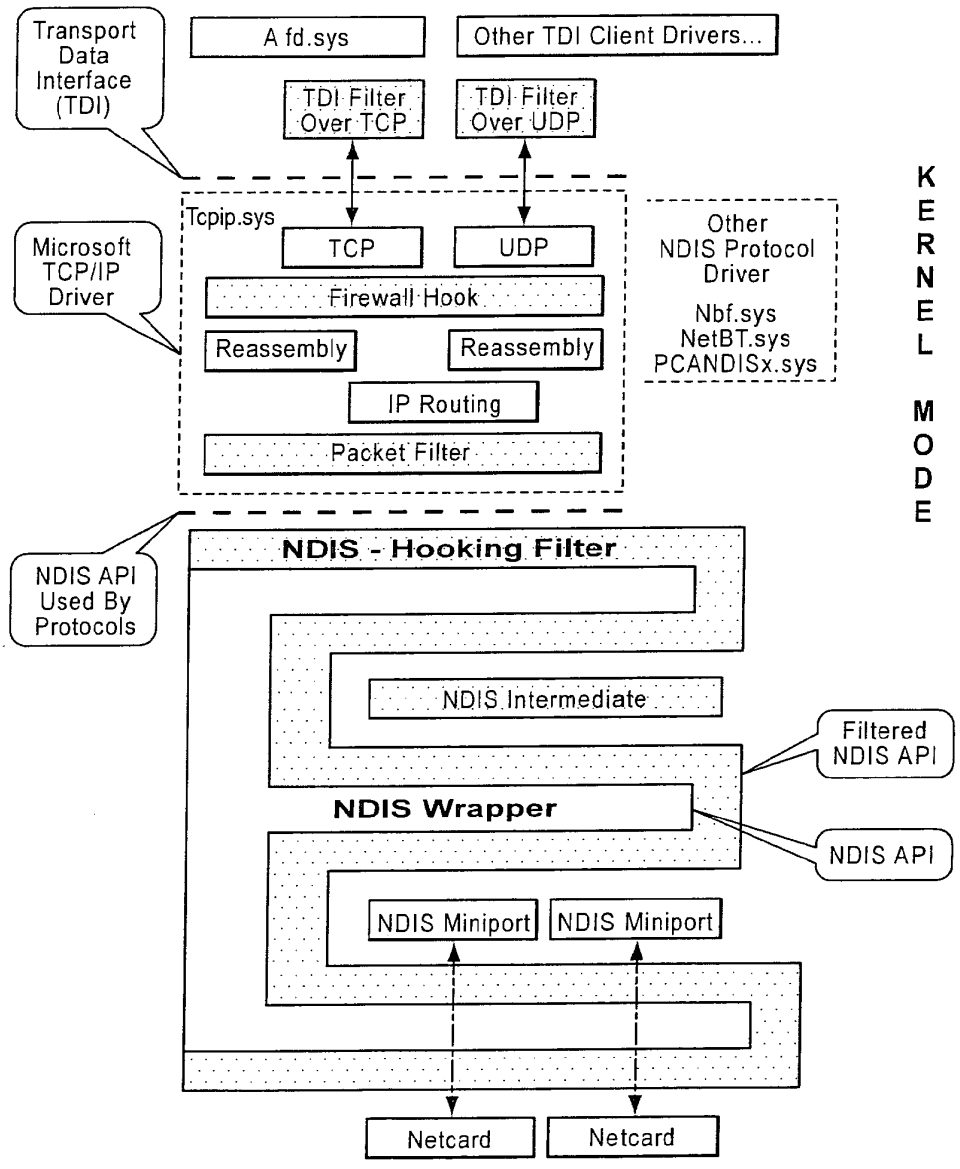

Transport Data Interface (TDI)
A fd.sys
Other TDI Client Drivers...
TDI Filter Over TCP
TDI Filter Over UDP
Tcpip.sys
TCP
UDP
Microsoft TCP/IP Driver
Firewall Hook
Reassembly
Reassembly
IP Routing
Packet Filter
Other NDIS Protocol Driver
Nbf.sys
NetBT.sys
PCANDISx.sys
KERNEL MODE
NDIS API Used By Protocols
NDIS - Hooking Filter
NDIS Intermediate
Filtered NDIS API
NDIS Wrapper
NDIS API
NDIS Miniport
NDIS Miniport
Netcard
Netcard

FIG. 6

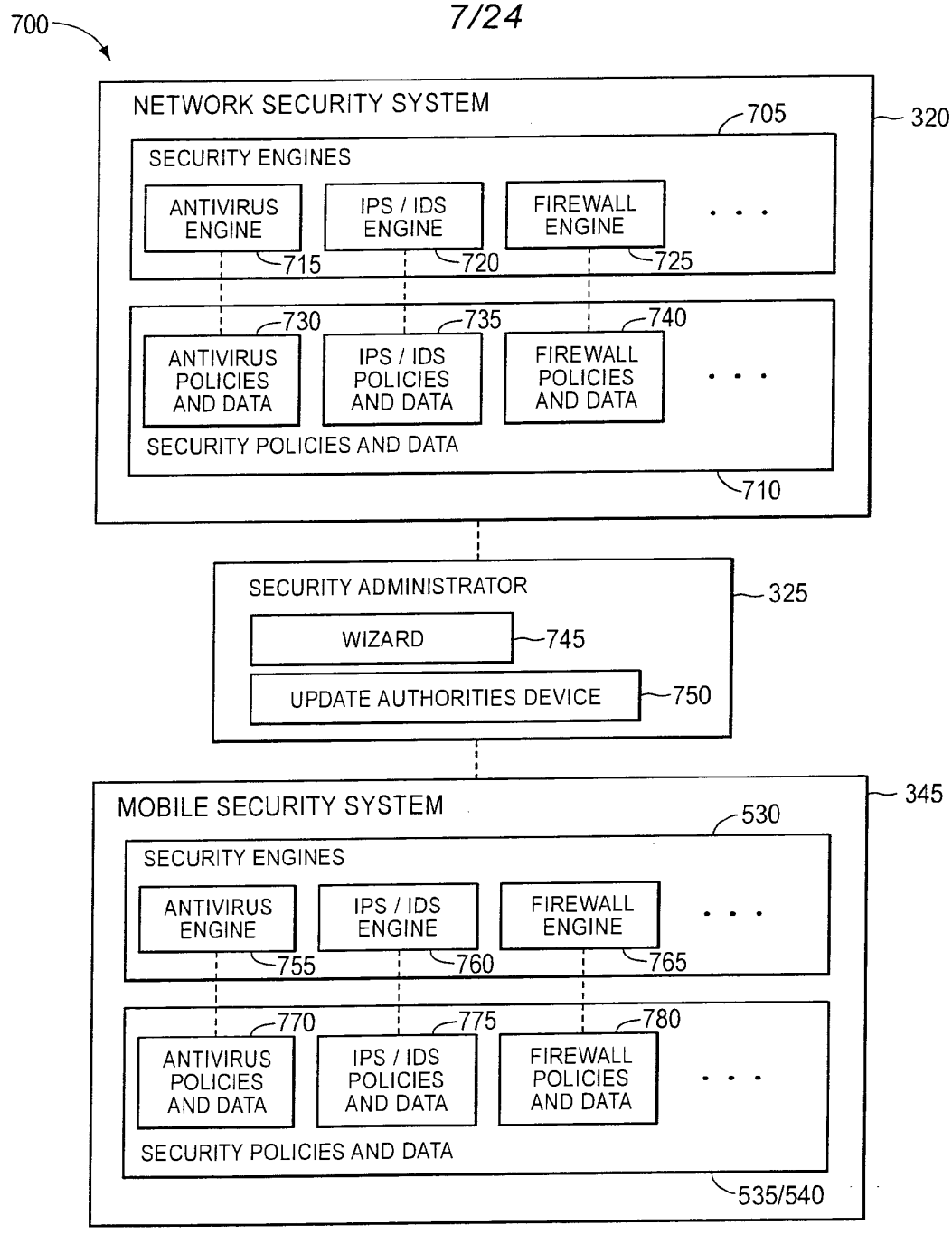

700
NETWORK SECURITY SYSTEM
705
320
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
715
720
725
730
735
740
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
710
SECURITY ADMINISTRATOR
325
WIZARD
745
UPDATE AUTHORITIES DEVICE
750
MOBILE SECURITY SYSTEM
345
530
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
755
760
765
770
775
780
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
535/540

FIG. 7

8/24

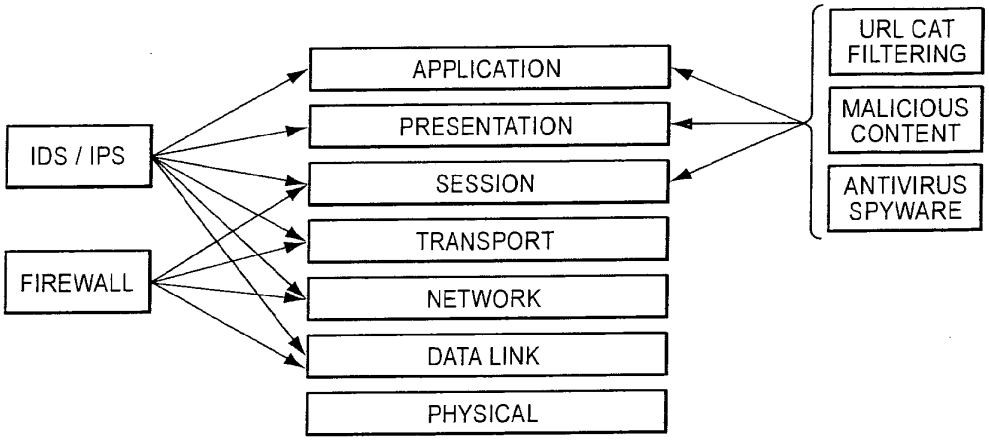


FIG. 8

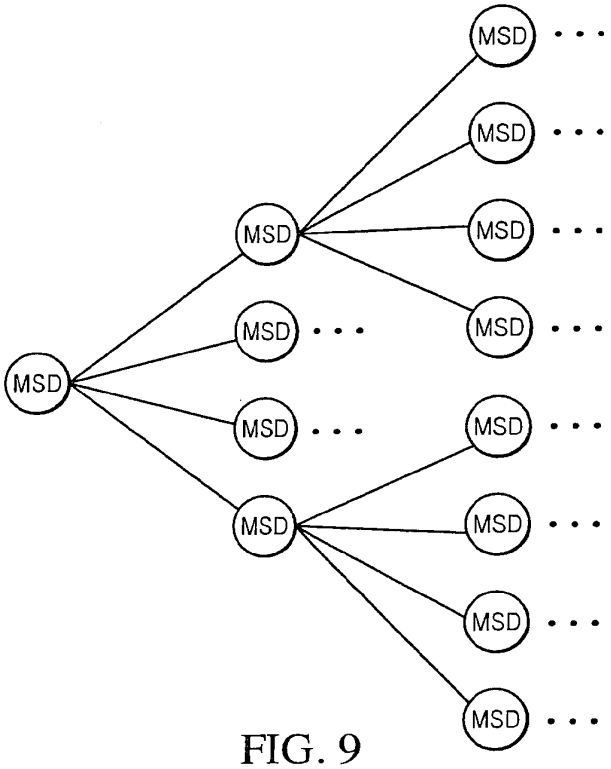


FIG. 9

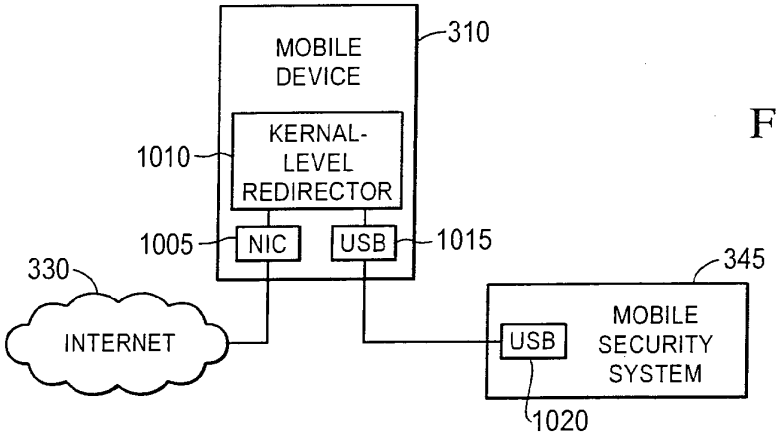


FIG. 10A

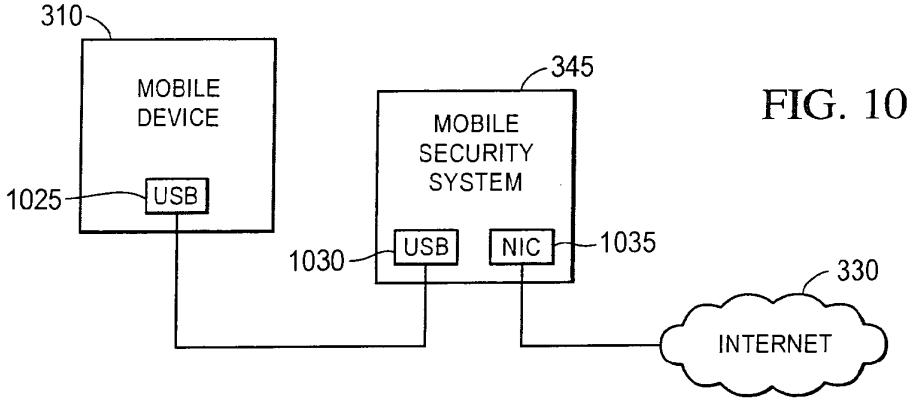


FIG. 10B

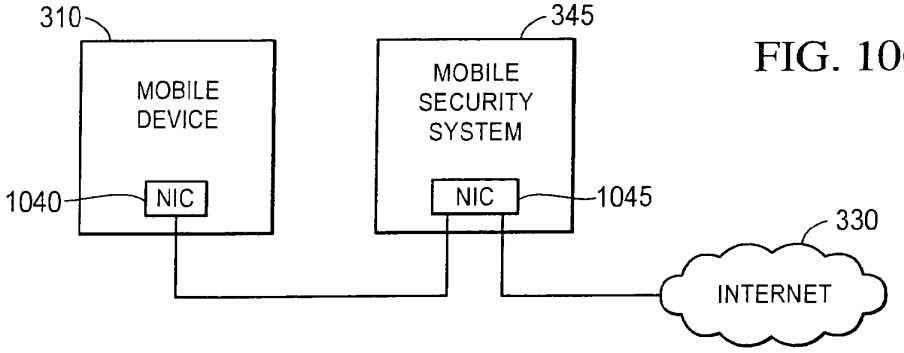


FIG. 10C

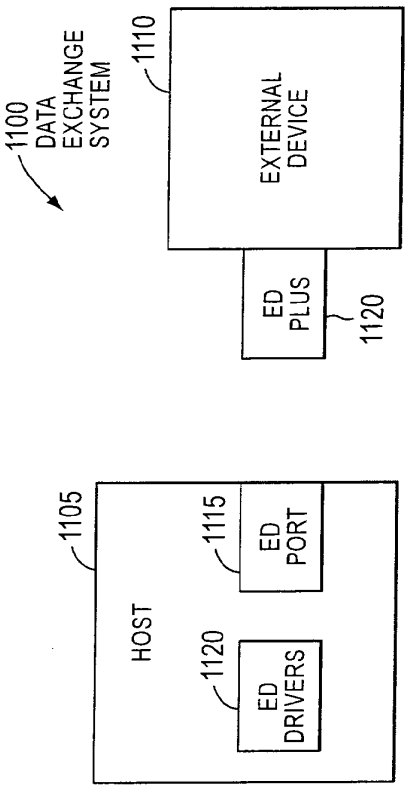


FIG. 11
(PRIOR ART)

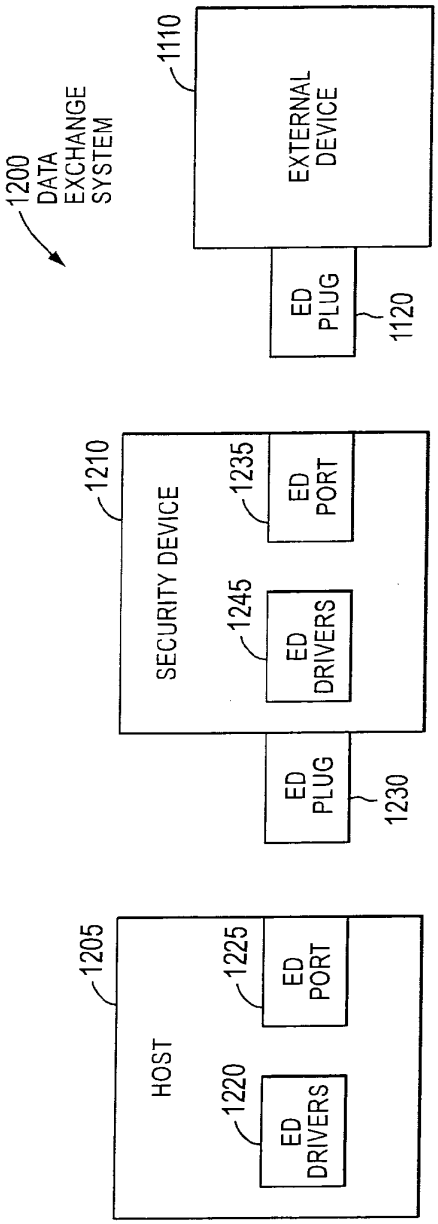


FIG. 12

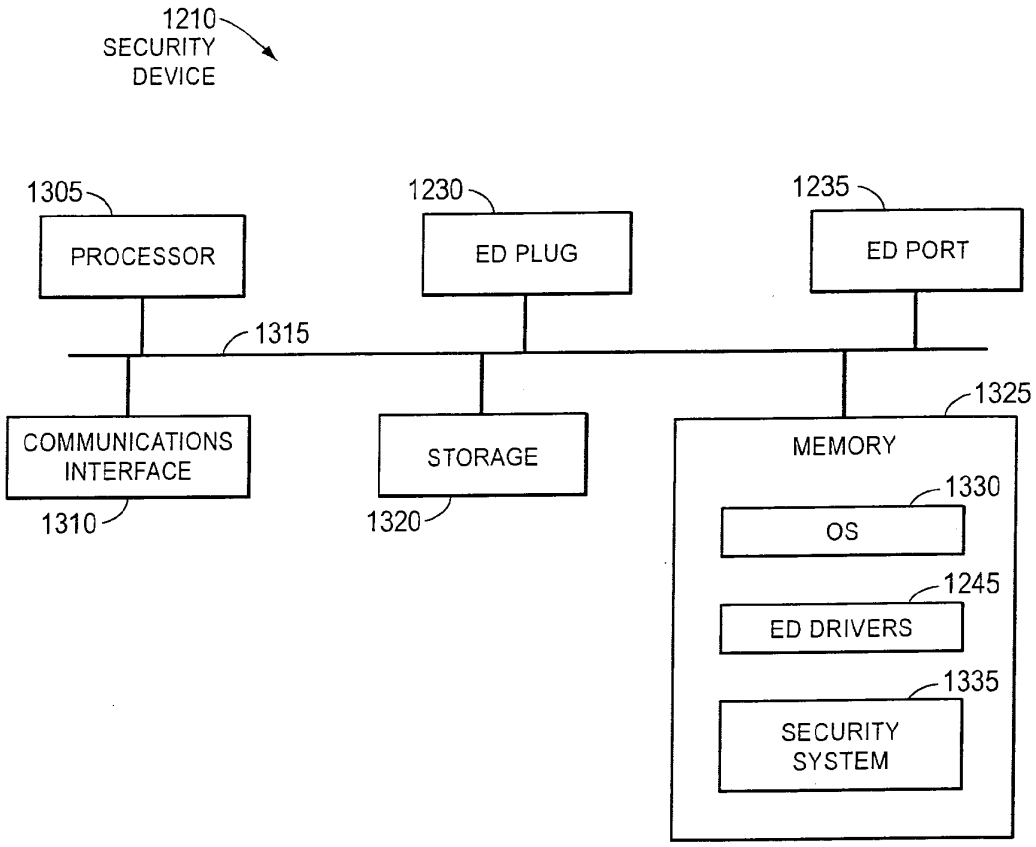

1210
SECURITY DEVICE
1305
PROCESSOR
1230
ED PLUG
1235
ED PORT
1315
COMMUNICATIONS INTERFACE
1310
STORAGE
1320
1325
MEMORY
1330
OS
1245
ED DRIVERS
1335
SECURITY SYSTEM

FIG. 13

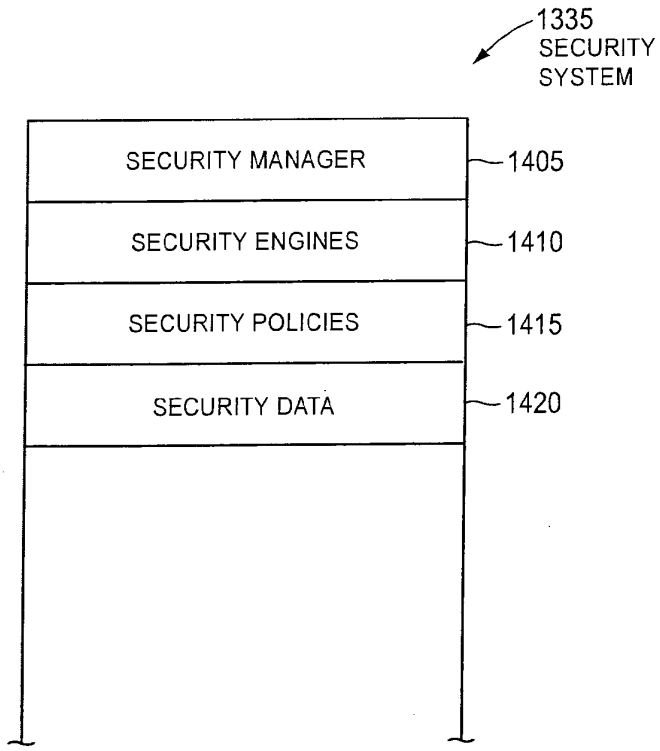

1335
SECURITY
SYSTEM
SECURITY MANAGER
1405
SECURITY ENGINES
1410
SECURITY POLICIES
1415
SECURITY DATA
1420

FIG. 14

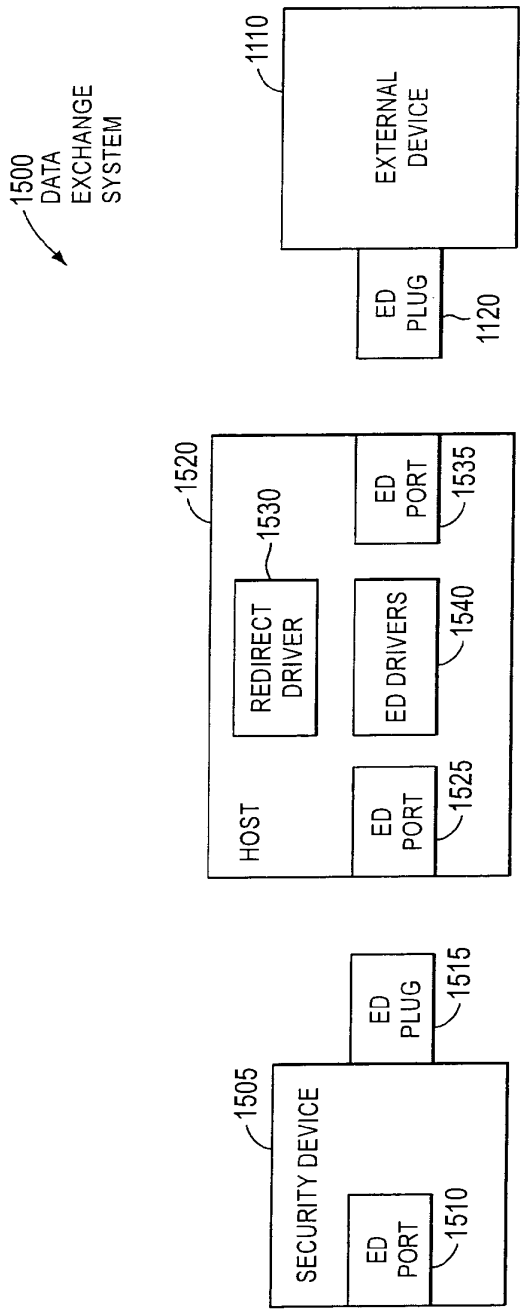

1500
DATA
EXCHANGE
SYSTEM
1110
EXTERNAL
DEVICE
ED
PLUG
1120
1520
1530
REDIRECT
DRIVER
ED
PORT
1535
ED DRIVERS
1540
HOST
ED
PORT
1525
ED
PLUG
1515
1505
SECURITY DEVICE
ED
PORT
1510

FIG. 15

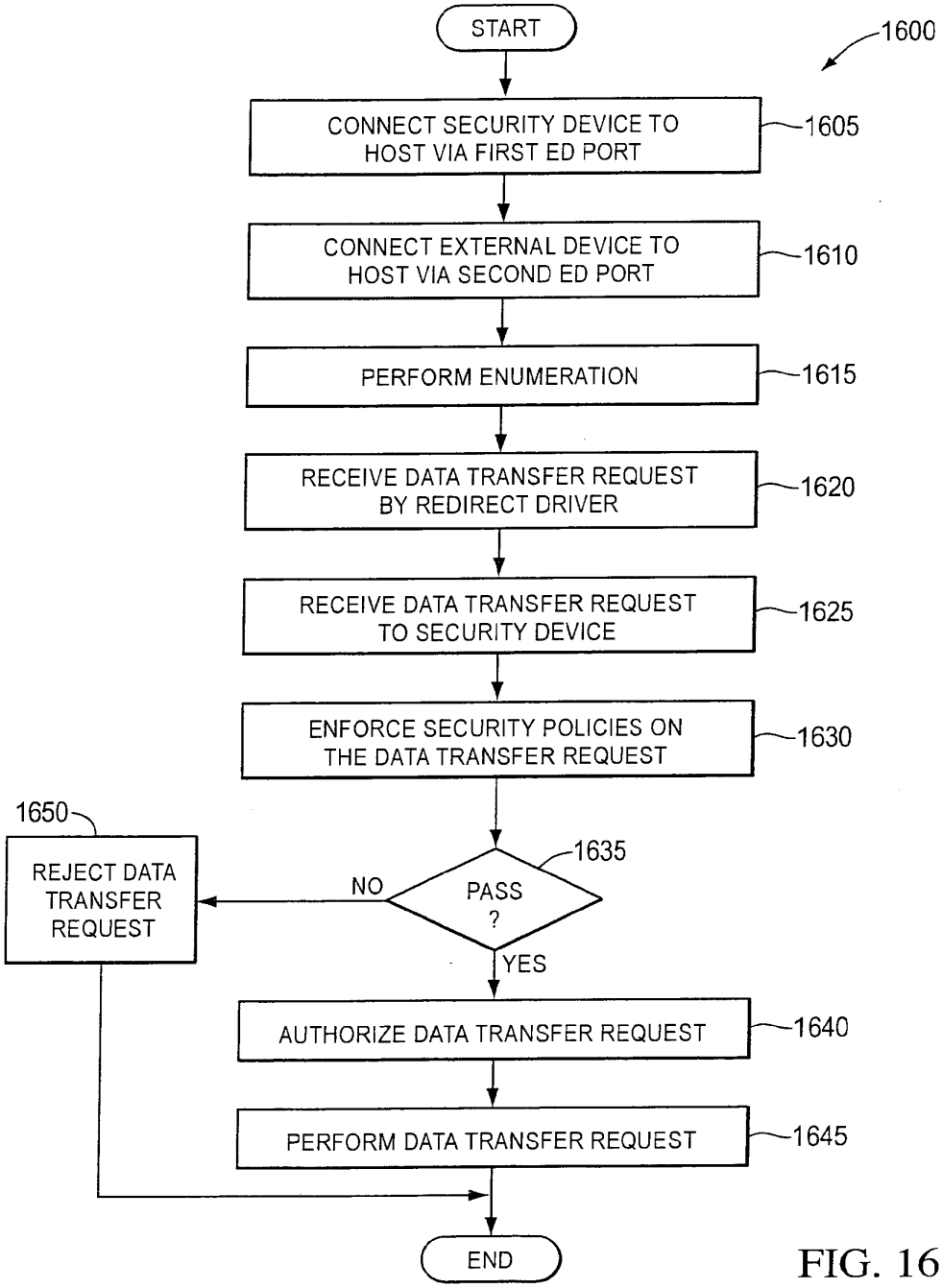

START
1600
CONNECT SECURITY DEVICE TO HOST VIA FIRST ED PORT
1605
CONNECT EXTERNAL DEVICE TO HOST VIA SECOND ED PORT
1610
PERFORM ENUMERATION
1615
RECEIVE DATA TRANSFER REQUEST BY REDIRECT DRIVER
1620
RECEIVE DATA TRANSFER REQUEST TO SECURITY DEVICE
1625
ENFORCE SECURITY POLICIES ON THE DATA TRANSFER REQUEST
1630
1650
REJECT DATA TRANSFER REQUEST
NO
PASS ?
1635
YES
AUTHORIZE DATA TRANSFER REQUEST
1640
PERFORM DATA TRANSFER REQUEST
1645
END

FIG. 16

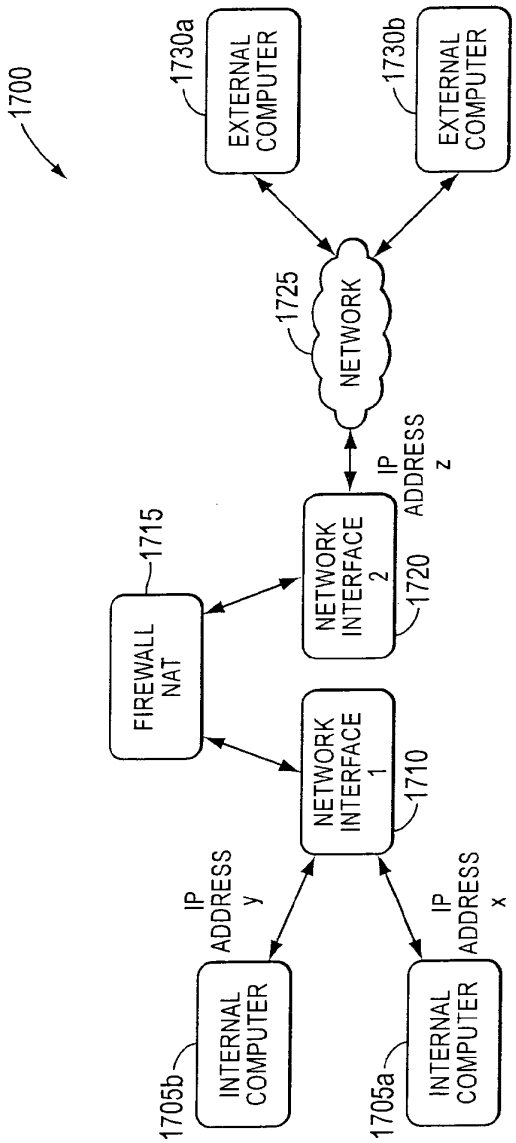


FIG. 17
(PRIOR ART)

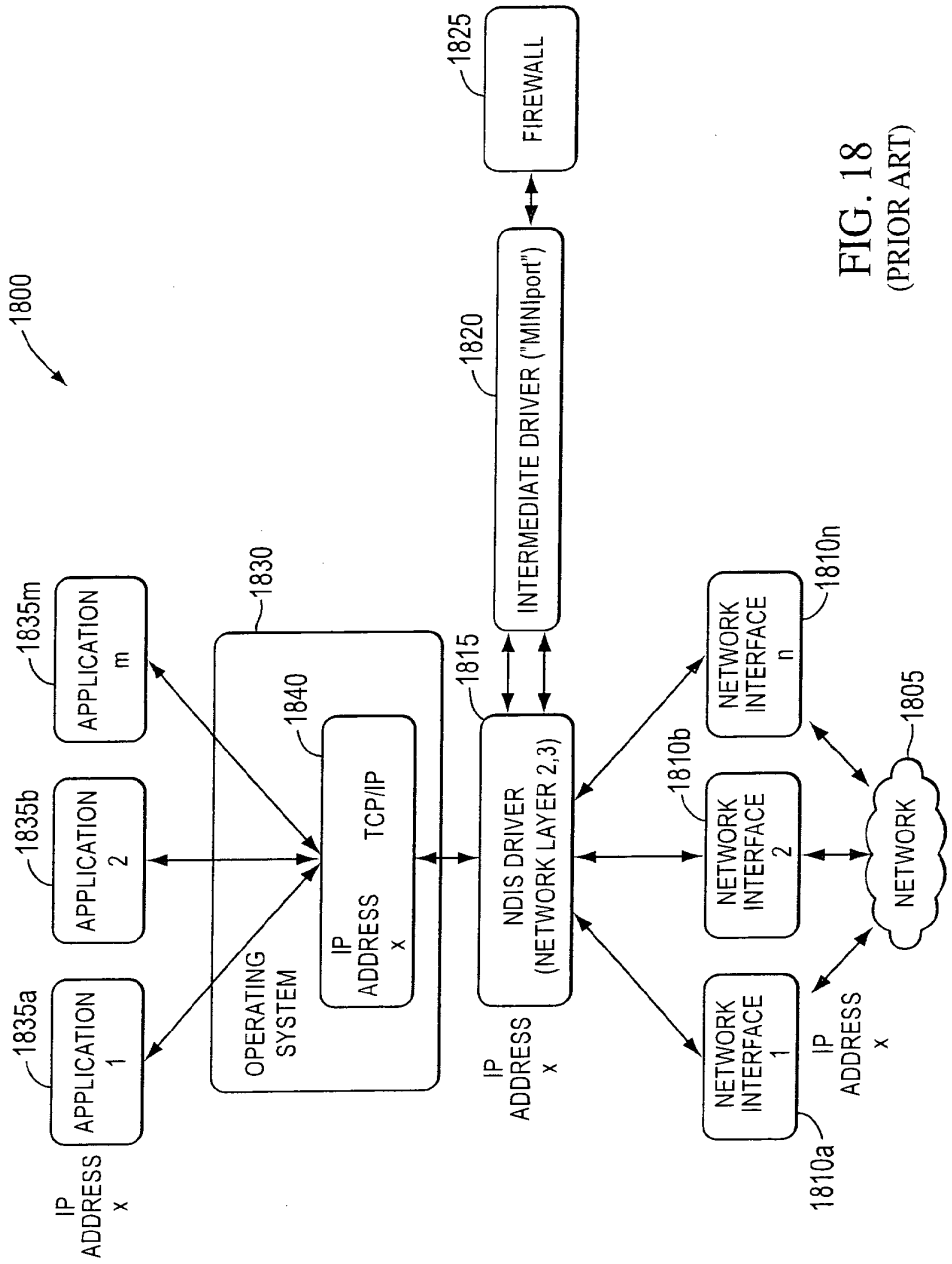


FIG. 18
(PRIOR ART)

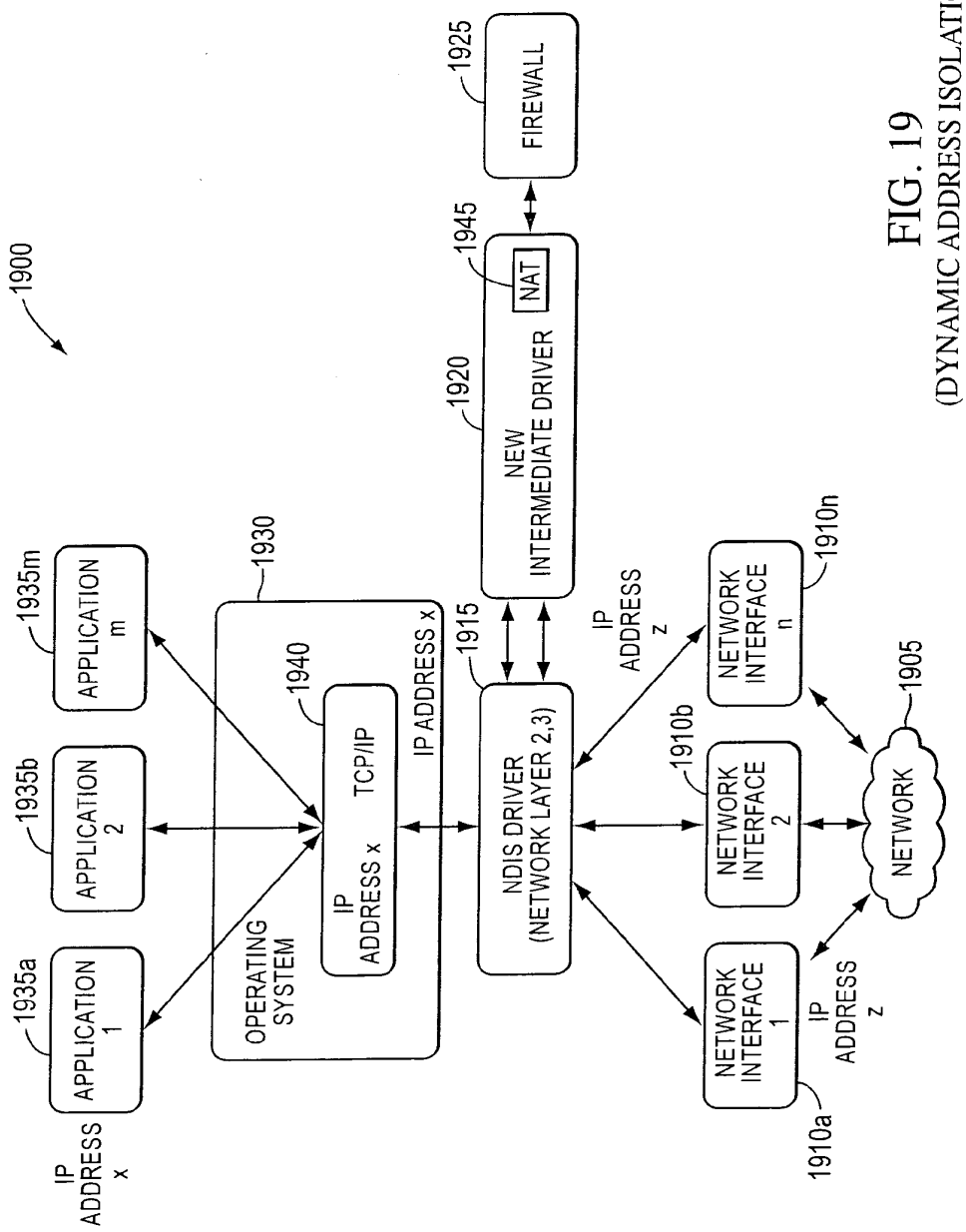


FIG. 19
(DYNAMIC ADDRESS ISOLATION)

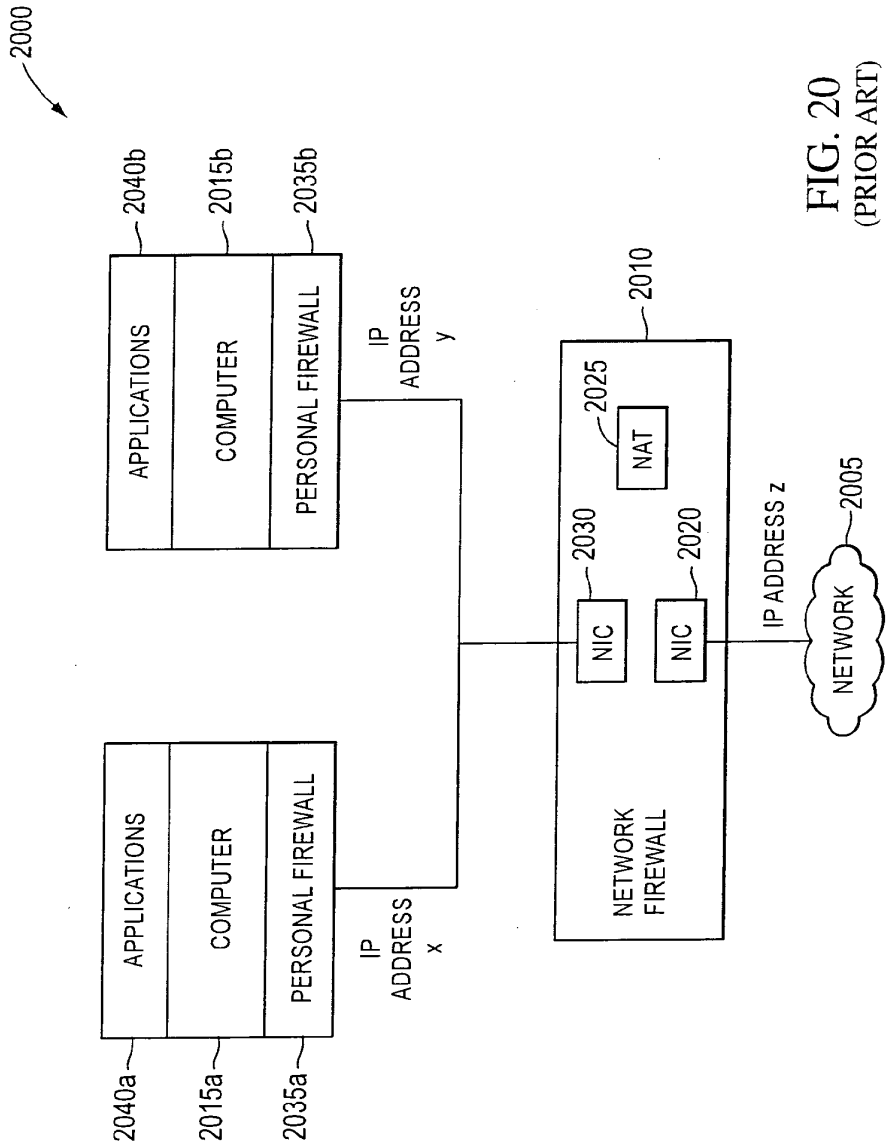


FIG. 20
(PRIOR ART)

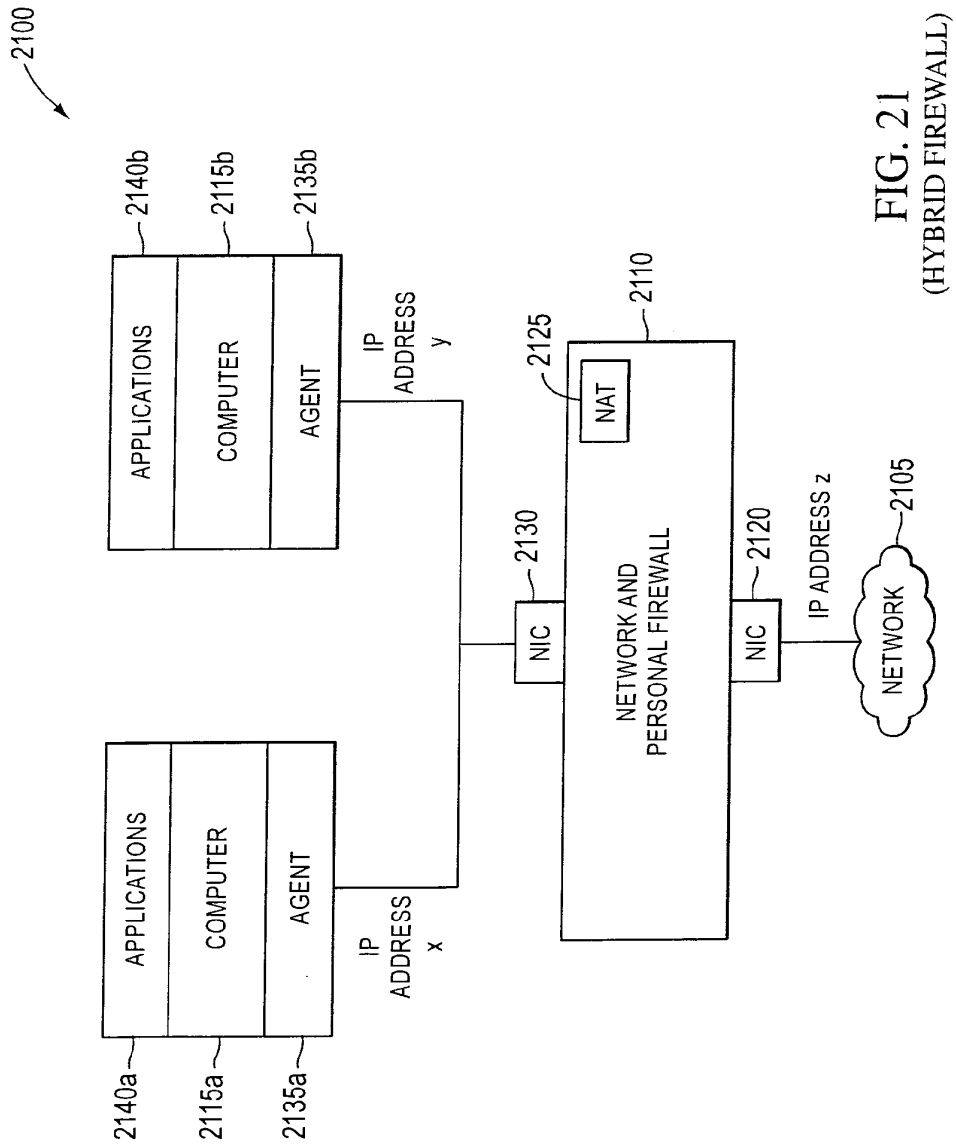


FIG. 21
(HYBRID FIREWALL)

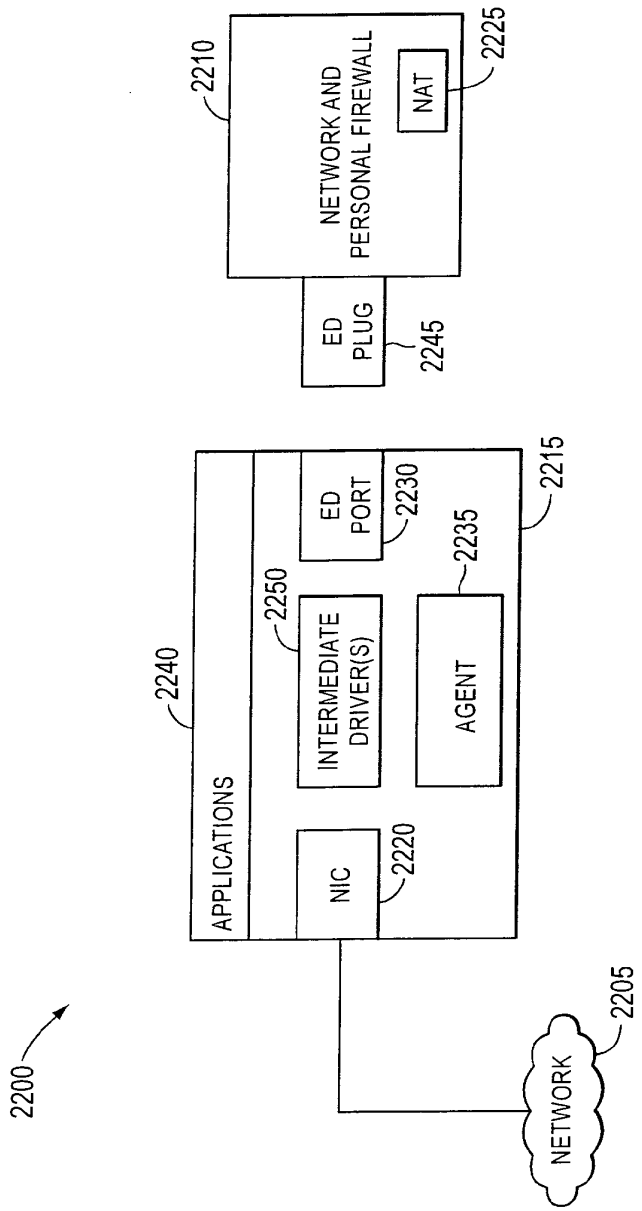


FIG. 22
(HYBRID FIREWALL EXAMPLE)

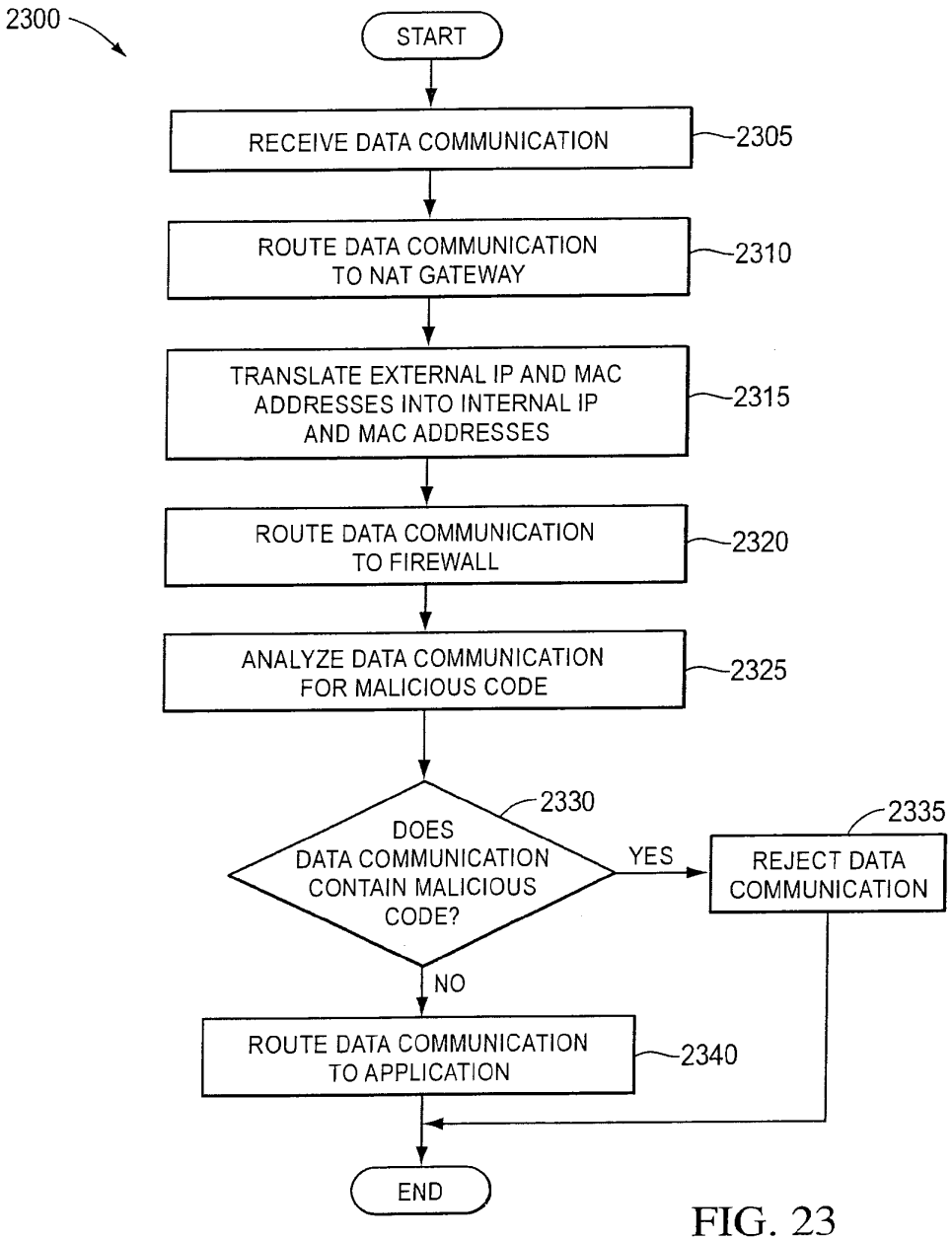

2300
START
RECEIVE DATA COMMUNICATION
2305
ROUTE DATA COMMUNICATION TO NAT GATEWAY
2310
TRANSLATE EXTERNAL IP AND MAC ADDRESSES INTO INTERNAL IP AND MAC ADDRESSES
2315
ROUTE DATA COMMUNICATION TO FIREWALL
2320
ANALYZE DATA COMMUNICATION FOR MALICIOUS CODE
2325
DOES DATA COMMUNICATION CONTAIN MALICIOUS CODE?
2330
YES
REJECT DATA COMMUNICATION
2335
NO
ROUTE DATA COMMUNICATION TO APPLICATION
2340
END

FIG. 23

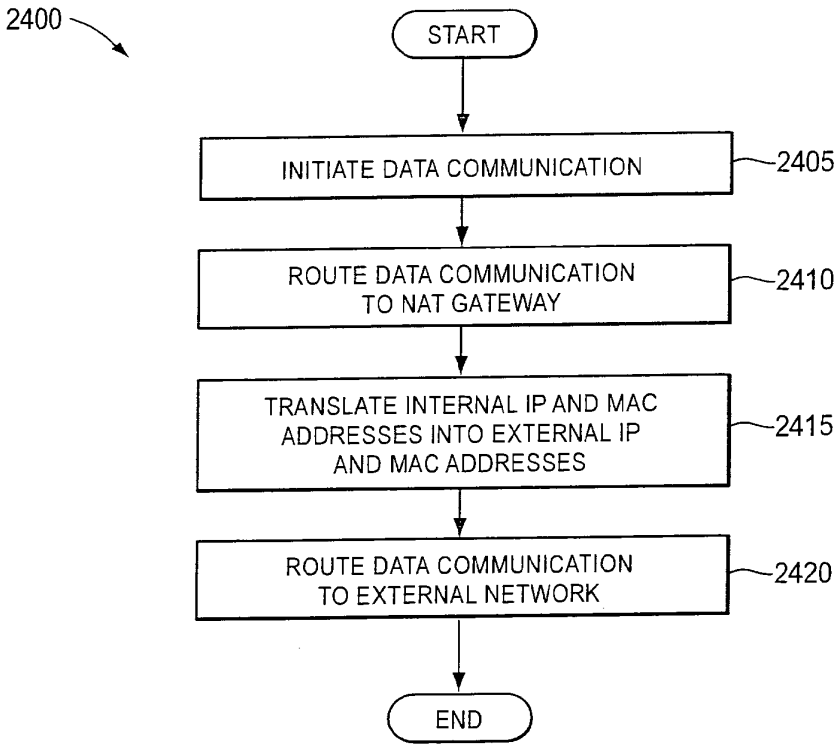

2400
START
INITIATE DATA COMMUNICATION
2405
ROUTE DATA COMMUNICATION TO NAT GATEWAY
2410
TRANSLATE INTERNAL IP AND MAC ADDRESSES INTO EXTERNAL IP AND MAC ADDRESSES
2415
ROUTE DATA COMMUNICATION TO EXTERNAL NETWORK
2420
END

FIG. 24

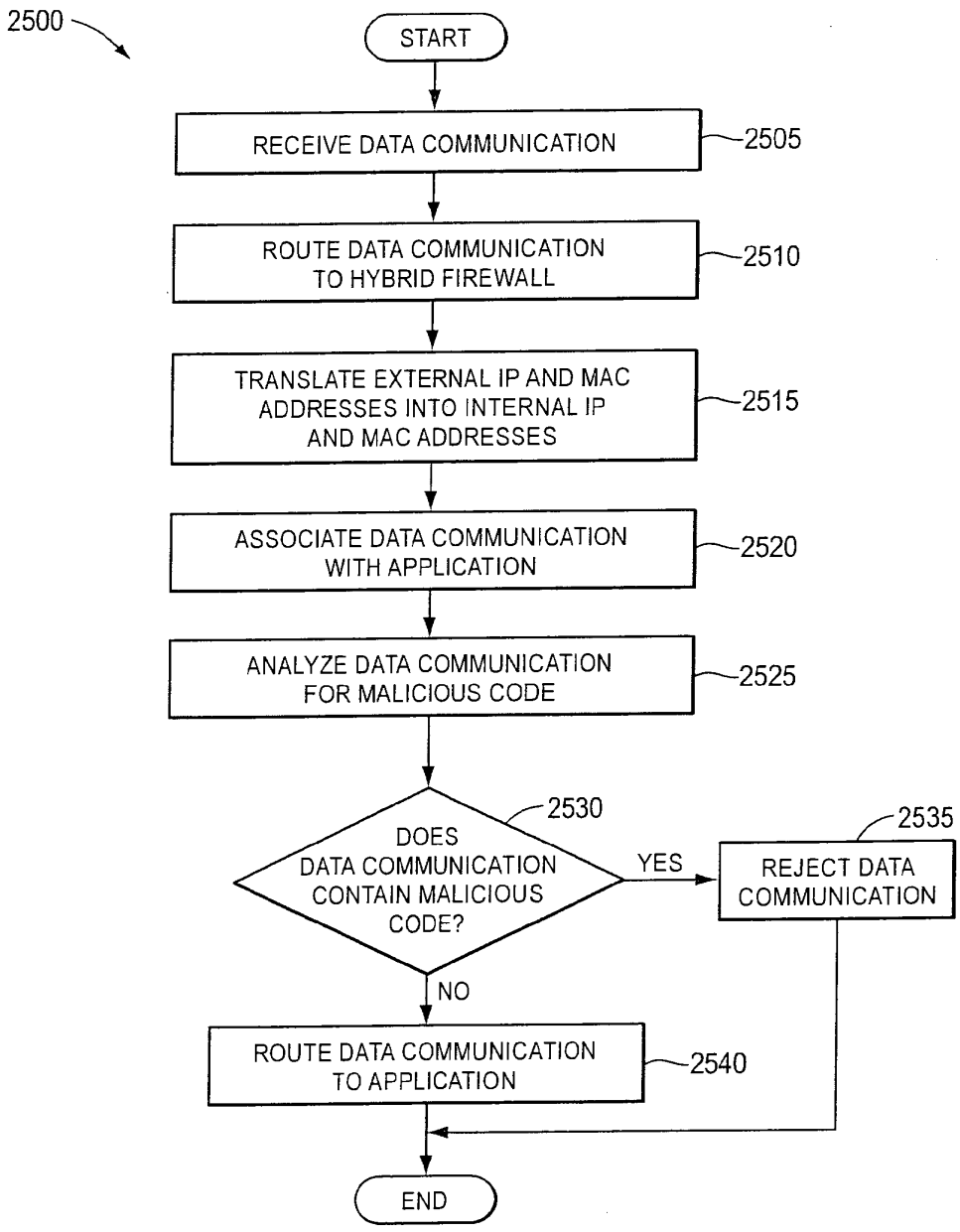

2500
START
RECEIVE DATA COMMUNICATION
2505
ROUTE DATA COMMUNICATION TO HYBRID FIREWALL
2510
TRANSLATE EXTERNAL IP AND MAC ADDRESSES INTO INTERNAL IP AND MAC ADDRESSES
2515
ASSOCIATE DATA COMMUNICATION WITH APPLICATION
2520
ANALYZE DATA COMMUNICATION FOR MALICIOUS CODE
2525
DOES DATA COMMUNICATION CONTAIN MALICIOUS CODE?
2530
YES
REJECT DATA COMMUNICATION
2535
NO
ROUTE DATA COMMUNICATION TO APPLICATION
2540
END

FIG. 25

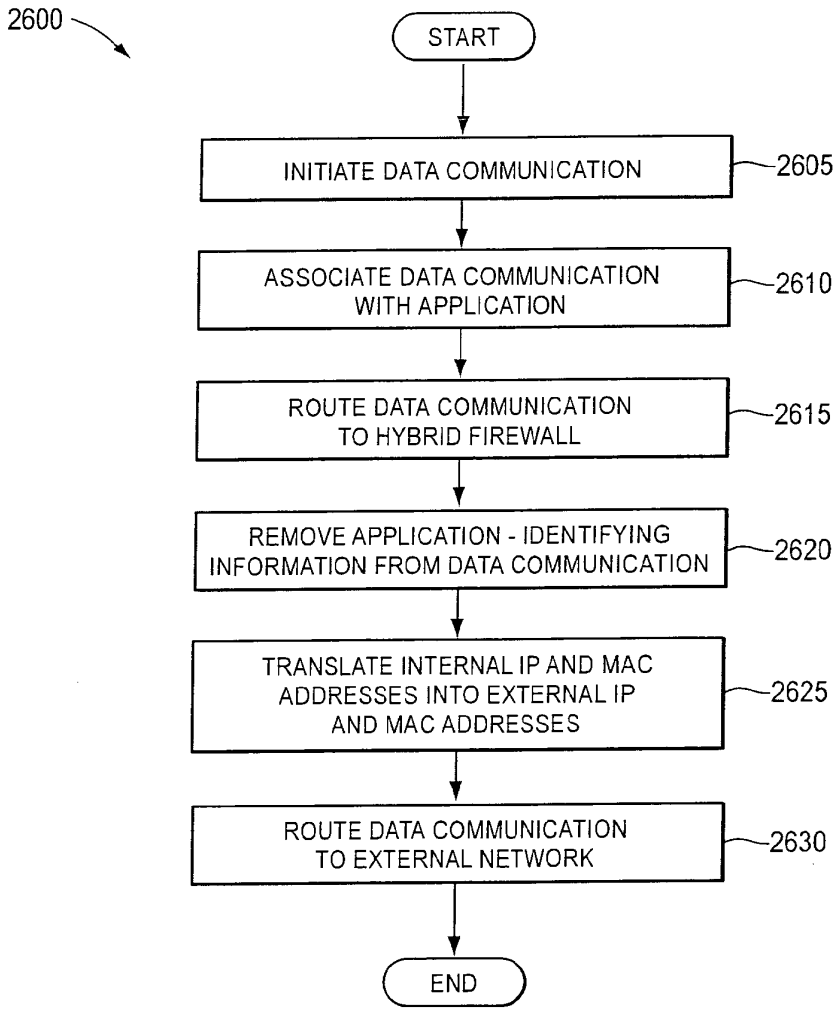

2600
START
INITIATE DATA COMMUNICATION
2605
ASSOCIATE DATA COMMUNICATION WITH APPLICATION
2610
ROUTE DATA COMMUNICATION TO HYBRID FIREWALL
2615
REMOVE APPLICATION - IDENTIFYING INFORMATION FROM DATA COMMUNICATION
2620
TRANSLATE INTERNAL IP AND MAC ADDRESSES INTO EXTERNAL IP AND MAC ADDRESSES
2625
ROUTE DATA COMMUNICATION TO EXTERNAL NETWORK
2630
END

FIG. 26

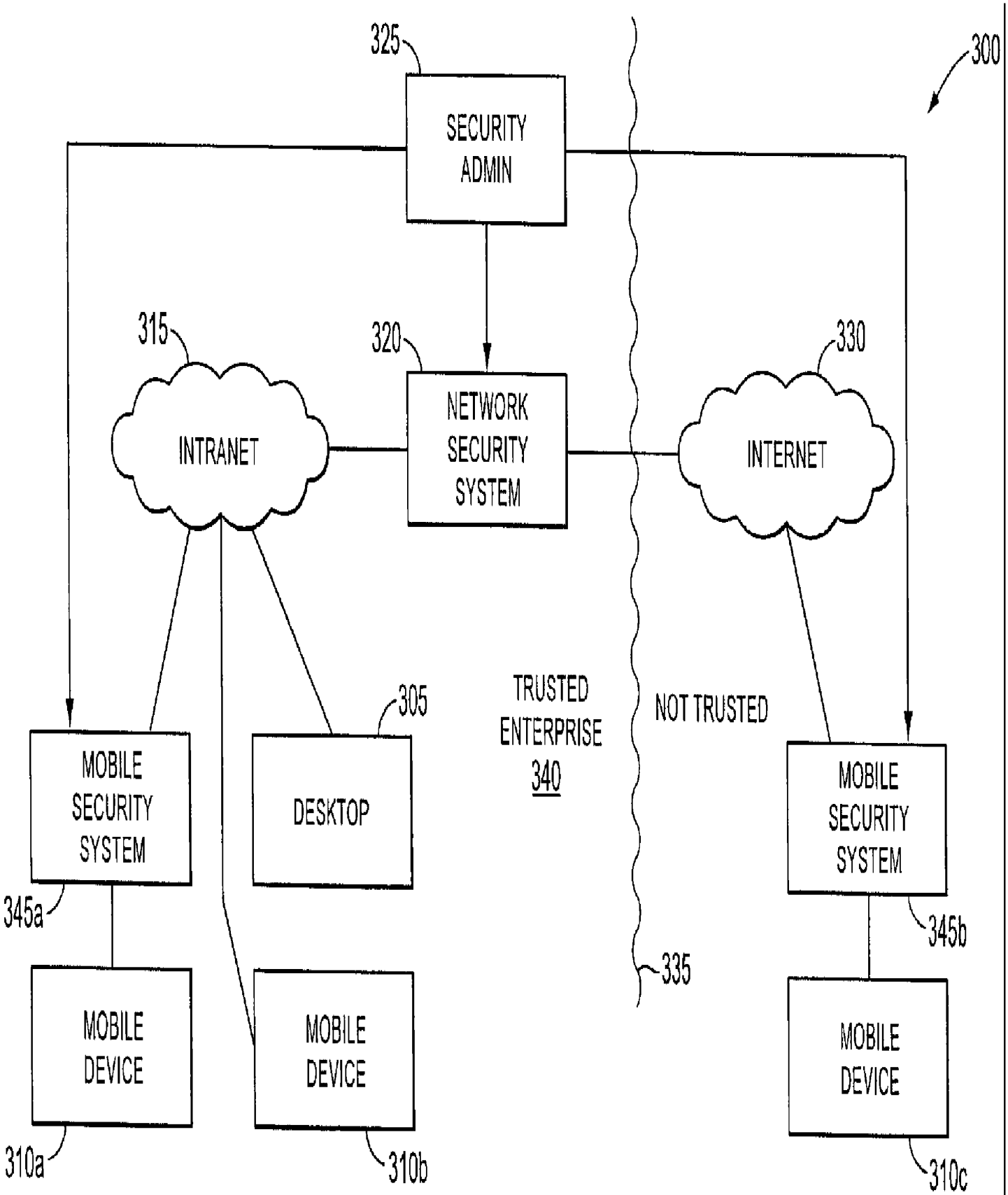

325
300
SECURITY ADMIN
315
320
330
INTRANET
NETWORK SECURITY SYSTEM
INTERNET
TRUSTED ENTERPRISE 340
NOT TRUSTED
305
MOBILE SECURITY SYSTEM
DESKTOP
MOBILE SECURITY SYSTEM
345a
345b
335
MOBILE DEVICE
MOBILE DEVICE
MOBILE DEVICE
310a
310b
310c

FIG. 3

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 850 575 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.10.2007 Bulletin 2007/44

(51) Int Cl.:
H04M 15/28 *(2006.01)* ***H04M 17/00*** *(2006.01)*
H04Q 7/32 *(2006.01)* *H04Q 7/38* *(2006.01)*

(21) Application number: **06252276.8**

(22) Date of filing: **27.04.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventor: **Rybak, Michal A.**
Kitchener, Ontario, N2R 1B1 (CA)

(74) Representative: **Fennell, Gareth Charles et al**
Kilburn & Strode
20 Red Lion Street
London WC1R 4PJ (GB)

(54) Method and apparatus for monitoring and controlling wireless resource usage

(57) A mobile communications device (116) comprises a wireless resource usage module (216) operable to assist the user of the mobile communications device (116) and/or his or her employer in monitoring and/or controlling the level of resources consumed by the user in a billing period.

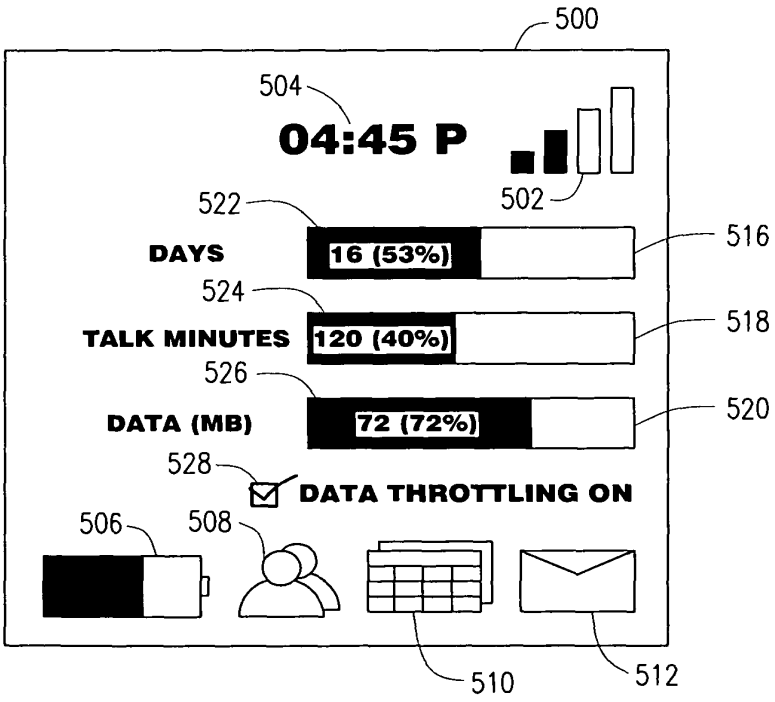


FIG. 7

EP 1 850 575 A1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD OF THE APPLICATION

[0001] The present disclosure generally relates to wireless packet data service networks. More particularly, and not by way of any limitation, the present disclosure is directed to a mobile communications device and related data service network employing features suitable for monitoring and controlling wireless service usage.

BACKGROUND

[0002] Wireless service is generally offered by wireless service providers according to certain wireless service access plans. Most wireless service access plans include limitations as to the quantity of wireless access available in a given time. For example, a first wireless service access plan may provide for a certain number of cellular telephone voice minutes per month. Certain plans provide for unlimited cellular voice minutes during off-peak periods along with a limited number of minutes available during peak periods. Wireless service access plans may also provide for specified levels of wireless data access per month. While cellular telephone minutes are generally quantified in minutes per month, wireless data access is generally quantified in some units of bandwidth per month (e.g., megabytes per month). In either event, a wireless service provider will generally continue to provide service above the specified level, but will charge an additional premium for the usage above the level specified in the wireless service access plan.

SUMMARY OF THE DISCLOSURE

[0003] In one embodiment, the present disclosure is directed to a method for monitoring resource usage of a mobile communications device comprising the steps of acquiring a mobile communication plan profile associated with a subscriber, the plan profile including at least a value representing a limit of mobile communication resource usage within a specified calendar period; acquiring resource consumption data relative to the specified calendar period; calculating usage statistics based on the resource consumption data and the plan profile; and presenting the usage statistics to an entity.

[0004] In another embodiment, the present disclosure is directed to a mobile communications device comprising at least one storage area for containing a mobile communication service plan profile associated with a subscriber, the mobile communication service plan profile including at least a value representing a limit of mobile communication resource usage within a specified period; at least one storage area for containing resource consumption data relative to the specified period; and a wireless resource usage control module for calculating usage statistics based on the resource consumption data and the service plan profile.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] A more complete understanding of the embodiments of the present disclosure may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0006] Figure 1 depicts an exemplary network environment including a wireless packet data service network wherein an embodiment of the present disclosure may be practiced;

[0007] Figure 2 depicts a software architectural view of a mobile communications device operable to route incoming messages according to one embodiment;

[0008] Figure 3 depicts a block diagram of a mobile communications device operable to route incoming messages according to one embodiment;

[0009] Figure 4 depicts a flow chart for a method of monitoring and controlling wireless service access according to one embodiment; and

[0010] Figure 5 depicts a screen shot of a mobile communications device according to one embodiment;

[0011] Figure 6 depicts a screen shot of a mobile communications device according to a second embodiment;

[0012] Figure 7 depicts a screen shot of a mobile communications device having an embodiment of the usage monitoring application open;

[0013] Figure 8 depicts a screen shot of a usage monitoring application embodiment suitable for monitoring the wireless usage of a group of users; and

[0014] Figure 9 depicts a flow chart of a usage throttling method according to one embodiment.

DETAILED DESCRIPTION OF THE DRAWINGS

[0015] A system and method of the present disclosure will now be described with reference to various examples of how the embodiments can best be made and used. Like reference numerals are used throughout the description and several views of the drawings to indicate like or corresponding parts, wherein the various elements are not necessarily drawn to scale.

[0016] Referring now to the drawings, and more particularly to Figure 1, depicted therein is an exemplary network environment 100 including a wireless packet data service network 112 wherein an embodiment of the present system may be practiced. An enterprise network 102, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), wide area network (WAN) or metropolitan area network (MAN), et cetera, for serving a plurality of corporate users.

[0017] A number of application servers 104-1 through 104-N disposed as part of the enterprise network 102 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management, and the like. Accordingly, a diverse array of personal information ap-

pliances such as desktop computers, laptop computers, palmtop computers, et cetera, although not specifically shown in Figure 1, may be operably networked to one or more of the application servers 104-i, i = 1, 2,...,N, with respect to the services supported in the enterprise network 102.

[0018] Additionally, a remote services server 106 may be interfaced with the enterprise network 102 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable mobile communications device 116. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 108, as well as the wireless packet data service network 112 operable with mobile communications device 116 via suitable wireless network infrastructure that includes a base station (BS) 114 .

[0019] In one embodiment, a trusted relay network 110 may be disposed between the Internet 108 and the infrastructure of wireless packet data service network 112. By way of example, mobile communications device 116 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers, et cetera.

[0020] For purposes of the present disclosure, the wireless packet data service network 112 may be implemented in any known or heretofore unknown mobile communications technologies and network protocols. For instance, the wireless packet data service network 112 may be comprised of a General Packet Radio Service (GPRS) network that provides a packet radio access for mobile devices using the cellular infrastructure of a Global System for Mobile Communications (GSM)-based carrier network. In other implementations, the wireless packet data service network 112 may comprise an Enhanced Data Rates for GSM Evolution (EDGE) network, an Integrated Digital Enhanced Network (IDEN), a Code Division Multiple Access (CDMA) network, or any 3rd Generation (3G) network.

[0021] By way of providing an exemplary embodiment, the teachings of the present disclosure will be illustrated within the network environment 100, although those skilled in the art should readily recognize that the scope of the present disclosure is not limited thereby. Furthermore, a plan information server 109 may be coupled to any of the networks 102, 108, 110, 112 described above for purposes of the present disclosure as will be set forth below in greater detail.

[0022] Figure 2 depicts a software architectural view of a mobile communications device according to one embodiment. A multi-layer transport stack (TS) 206 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network.

[0023] As illustrated in the embodiment of Figure 2, an integration layer 204A is operable as an interface between a radio layer 202 and the transport stack 206 of mobile communications device 116. Likewise, another integration layer 204B is provided for interfacing between the transport stack 206 and a user applications layer 207 supported on the mobile communications device 116, e.g., email 208, calendar/scheduler 210, contact management 212 and browser 214. Although not specifically shown, the transport stack 206 may also be interfaced with the operating system of mobile communications device 116. In another implementation, the transport stack 206 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device. As seen in Figure 2, a usage control module 216 is coupled to radio layer 202 and transport stack 206. Usage control module 216 is operable to assist the user of mobile communications device 116 in controlling his or her usage of wireless services in a manner described more fully below.

[0024] The bottom layer (Layer 1) of the transport stack 206 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 100 shown in Figure 1. For example, when a mobile communications device roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the mobile communications device. The remaining two layers of the transport stack 206, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively.

[0025] Figure 3 depicts a block diagram of a mobile communications device according to one embodiment. It will be recognized by those skilled in the art upon reference hereto that although an embodiment of mobile communications device 116 may comprise an arrangement similar to one shown in Figure 3, there can be a number of variations and modifications, in hardware, software or firmware, with respect to the various modules depicted. Accordingly, the arrangement of Figure 3 should be taken as illustrative rather than limiting with respect to the embodiments of the present disclosure.

[0026] A microprocessor 302 providing for the overall control of an embodiment of mobile communications device 116 is operably coupled to a communication subsystem 304 which includes a receiver 308 and transmitter 314 as well as associated components such as one or more local oscillator (LO) modules 310 and a processing module such as a digital signal processor 312. As will be apparent to those skilled in the field of communications, the particular design of the communication module 304 may be dependent upon the communications network with which the mobile communications device 116 is intended to operate.

[0027] In one embodiment, the communication module 304 is operable with both voice and data communica-

tions. Regardless of the particular design, however, signals received by antenna 306 through base station 114 are provided to receiver 308, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, analog-to-digital (A/D) conversion, and the like. Similarly, signals to be transmitted are processed, including modulation and encoding, for example, by digital signal processor 312, and provided to transmitter 314 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over the air-radio interface via antenna 316.

[0028] Microprocessor 302 also interfaces with further device subsystems such as auxiliary input/output (I/O) 318, serial port 320, display 322, keyboard 324, speaker 326, microphone 328, random access memory (RAM) 330, a short-range communications subsystem 332, and any other device subsystems generally labeled as reference numeral 333. To control access, a Subscriber Identity Module (SIM) or Removable User Identity Module (RUIM) interface 334 is also provided in communication with the microprocessor 302.

[0029] In one implementation, SIM/RUIM interface 334 is operable with a SIM/RUIM card having a number of key configurations 344 and other information 346 such as identification and subscriber-related data. Operating system software and transport stack software may be embodied in a persistent storage module (i.e., non-volatile storage) such as Flash memory 335. In one implementation, Flash memory 335 may be segregated into different areas, e.g., storage area for computer programs 336 as well as data storage regions such as device state 337, address book 339, other personal information manager (PIM) data 341, and other data storage areas generally labeled as reference numeral 343. Usage control module 216 is operably connected to flash memory 335, including transport stack 206, as shown. In one exemplary implementation, the logic associated with the usage control module 216 is operable to access one or more storage areas, e.g., non-volatile storage areas 335, that contain various values relative to monitoring resource usage (i.e., resource consumption data) as will be set forth below. Additionally, the logic associated with the usage control module 216 is operable to access the subscriber's usage plan profile (e.g., a cellular telephone voice communication service plan profile, a wireless data transmission service plan profile, etc., which may be locally stored (e.g., in non-volatile areas), or downloaded, or otherwise available to the mobile communications device) for purposes of effectuating resource usage monitoring and/or throttling.

[0030] Figure 4 depicts a flow chart detailing the operation of usage control module 216 according to one embodiment. The process begins in block 400 with acquisition of the subscriber's usage plan profile, which includes at least one resource usage limit. Such limits may include, for example, limits as to the total number of on-peak cellular voice minutes per month, limits as to the total number of megabytes of data per month and/or limits as to the number of short messaging service (SMS) messages sent per month, as examples.

[0031] After the usage plan profile is acquired in block 400, the present date and time is acquired in block 402, along with the date and time of the beginning of the current billing period in block 404. Generally, the billing period will be one month and will begin at 12:00 am on a particular day of each month, but there is nothing within the spirit and scope of the present disclosure limiting the methods herein to such an arrangement. Given the date and time for the beginning of the current period and the current date and time, the usage control module 216 can determine the elapsed time since the beginning of the current billing period, as elaborated in block 406.

[0032] The date and time for the end of the current billing period is acquired in block 408. Given the date and time of the beginning of the current billing period and the date and time of the end of the current billing period, the usage control module 216 can calculate the total time of the current billing period, as elaborated in block 410.

[0033] The usage control module 216 acquires the quantity of current period usage of at least one limited wireless resource in block 412. This resource may be on-peak cellular voice minutes, megabytes of data or quantity of SMS messages, as examples. Given the total amount of the wireless resource available in the current billing period and the total amount of usage of that wireless resource so far in the current billing period, the usage control module 216 calculates, in block 414, a usage quotient representing the proportion of the resource which has already been consumed in the current billing period. For example, if the subscriber's service plan provides for 200 on peak minutes per month and the subscriber has used 100 minutes, the usage quotient would equal 100/200, or 50%.

[0034] In a similar manner, the usage control module 216 calculates, using the quantity of time elapsed in the current billing period and the total length of the current billing period, an elapsed days quotient representing the proportion of time in the current billing period which has already elapsed. For example, if the current month has 30 days, and 9 days have elapsed, the elapsed days quotient would equal 9/30, or 30%. This step is elaborated in block 416. The usage quotient and elapsed days quotient may be displayed to the user or provided to a management entity (block 418).

[0035] Process flow subsequent to block 418 is dependent on the relative values of the calculated statistics such as the usage quotient and the elapsed days quotient. If the proportion of the resource consumed in the current billing period is at or below the proportion of time elapsed in the current billing period, then the subscriber is unlikely to exceed the limit specified in the service plan and no corrective action is necessary. If, however, the proportion of the resource consumed in the current billing period exceeds the proportion of time elapsed so far in the current billing period, then the subscriber is consum-

ing the limited resource at a rate making it likely that he or she will exceed the limit specified in the service plan, and corrective action may be necessary, as elaborated in detail below.

[0036] In decision block 420, usage control module 216 inquires as to whether the usage quotient (designated E) is greater than the elapsed days quotient (designated F). If the usage quotient is not greater than the elapsed days quotient, then there is not significant cause for alarm and process flow proceeds to decision block 422. If the usage quotient is greater than the elapsed days quotient, then there is cause for alarm and process flow proceeds to block 424.

[0037] In the event that the subscriber is on track to meet or undershoot his or her usage limit for the current billing period, and process flow has proceeded to decision block 422, the usage control module 216 determines whether the subscriber's wireless access is currently being "throttled" by the usage control module 216. In other words, usage control module 216 determines whether prior usage conditions have placed usage control module 216 in a mode in which it is restricting the subscriber's access to wireless services. Such a restriction may include, for example, a reduced data transfer rate, or some limit as to the number of cellular voice minutes or SMS messages available per day or per hour.

[0038] If the subscriber's wireless access is not being throttled by usage control module 216, then process flow proceeds to block 428, wherein the current cycle of the wireless access control process comes to an end. If the subscriber's wireless access is, however, being throttled by usage control module 216 due to a previous overrun, then process flow proceeds to block 426, wherein usage control module 216 adjusts the wireless access parameters for mobile communications device 116.

[0039] In certain embodiments, adjustment of the throttled wireless access parameters may entail removal of all throttling of wireless access once the usage quotient equals or is less than the elapsed days quotient. In other embodiments, adjustment of the wireless access parameters may entail a reduction in the degree of throttling proportional to the difference between the usage quotient and the elapsed days quotient. In such an embodiment, so long as the usage quotient is only slightly lower than the elapsed days quotient, a certain level of throttling may continue to be imposed, with the goal of generating a "buffer" of wireless resources. In any event, after adjustment of the wireless access parameters, process flow proceeds to block 428, where the current cycle of the wireless access control process ends.

[0040] Returning to block 420, when the usage quotient exceeds the elapsed days quotient, reflecting the fact that the subscriber is consuming wireless resources at a rate expected to result in a budget overrun, process flow will proceed from block 420 to block 424. In block 424, usage control module 216 will determine whether the subscriber or some other party has activated an alarm function. The usage control module may have the capability to provide wireless usage overrun alarms to the subscriber and/or to other individuals or components in a network. If the alarm function is activated, process flow proceeds to block 430, wherein at least one alarm is generated to at least one individual or network component, and then to block 432. This alarm may be of any a number of types, including audio, video and tactile alarms. If the alarm function is deactivated, process flow proceeds directly to block 432.

[0041] In block 432, usage control module 216 determines whether the wireless resource throttling function has been activated, either by the subscriber or by some other individual or component. If the wireless resource throttling function has not been activated, process flow proceeds directly to block 428, where the current cycle of the wireless access control process ends. If the wireless resource throttling function has been activated, process flow proceeds to block 434.

[0042] In block 434, usage control module 216 adjusts wireless access parameters in order to control consumption of one or more wireless resources by the subscriber. As described above, in certain embodiments, the throttling may take the form of a pre-set usage limit imposed whenever throttling is deemed necessary. In other embodiments, the usage limit may vary within a range. The usage limit may vary, for example, according to the difference between the usage quotient and the elapsed days quotient. In such an arrangement, where the usage quotient of a wireless resource exceeds the elapsed days by 10%, the usage control module may reduce the maximum rate of consumption of the wireless resource by a proportional percentage, which could be 10%, 20% or 5%, as examples. In certain embodiments, the degree of throttling may be linearly proportional to the degree of projected overrun, while in others the degree of throttling may be geometrically proportional, so that minor overruns would have negligible effects on bandwidth, which would become increasingly dramatic as usage overruns increased. Any and all of the above are within the spirit and scope of the present disclosure. After the parameters are adjusted by the specific algorithm employed, process flow then proceeds from block 434 to block 428, where the current cycle ends.

[0043] Figure 5 depicts one embodiment of a user interface screen 500 for a mobile communications device. For example, screen 500 displays information to the user of mobile communications device 116. Certain information, such as time readout 504, will generally be presented on screen 500 in textual format. In order to maximize special efficiency, however, other information is presented on screen 500 in a graphical format including a set of descriptive icons. Representative icons shown on screen 500 include a wireless signal strength icon 502, a battery strength icon 506, contacts icon 508, calendar icon 510, message icon 512 and wireless resource usage icon 514.

[0044] Each of icons 502, 506, 508, 510, 512, 514 has a specific function within mobile communications device 116, and each may generally be associated with a spe-

cific software application. Contacts icon 508, for example, may generally be associated with a software application such as contact management application 212 (shown in Figure 2), while calendar icon 510 and message icon 512 may be associated with calendar/scheduler application 210 and email application 208, respectively.

[0045] Wireless resource usage icon 514 is exemplified with three separate horizontal bars that may represent different parameters depending on the application. In one embodiment, one bar may represent the passage of time over the billing period, a second bar may represent peak cellular voice minutes used in the current billing period and a third bar may represent data bandwidth used in the current billing period. By comparing the size of bars representing wireless resource usage to the size of bars representing the passage of time, a subscriber can monitor his or her rate of usage. In alternate embodiments, the bars may represent other parameters, which may include the number of off-peak cellular telephone voice minutes used and/or the number of SMS messages sent/received in the current billing period, as examples.

[0046] An alternative embodiment of a display screen is shown in Figure 6 and designated 600. Display screen 600 is similar to screen 500, having a signal strength meter icon 602, a current time display 604, a battery strength meter icon 606, a contacts icon 608, a calendar icon 610 and a message icon 612, each of which corresponds to a similar icon depicted in Figure 5. In contrast to display screen 500, display screen 600 has a rotary wireless resource usage icon 614 in place of the horizontal bar wireless resource usage icon 514 shown in Figure 5. In place of linear bars, wireless resource usage icon 614 employs rotary elements, including a needle pivoting about the center of the icon and a sector and marker disposed at the circumference thereof. Any of the elements may represent any of the parameters heretofore described.

[0047] Figure 7 depicts display screen 500 at a separate point in time at which an embodiment of the user interface application for usage control module 216 is open. An elapsed days graphical indicator 516 reflects the proportion of the current billing period elapsed as compared to the total span of the current billing period. Similarly, voice minutes graphical indicator 518 and data resources graphical indicator 520 reflect the proportion of each resource consumed as compared to the total amount of each resource available in the current billing period. Textual indicators 522, 524, 526 provide the same information as graphical resource indicators 516, 518, 520, but in alphanumeric rather than graphical format.

[0048] By comparing the state of resource indicators 518, 520, 524, 526 to elapsed days indicators 516, 522, a subscriber can quickly determine whether his or her rate of usage is likely to exceed the allotted resources for the current billing period. In order to assist the subscriber in controlling resource usage, a throttling indicator 528 reflects whether or not wireless bandwidth throttling is currently activated. In certain embodiments, throttling may be controlled by the subscriber, while in other embodiments throttling may be controlled partly or completely by a process external to mobile communications device 116 or by another individual.

[0049] Display screen 500 as shown in Figure 7 is only representative of one embodiment of the present disclosure. Alternative embodiments may incorporate additional information or less information. In certain embodiments, for example, the throttling indicator 528 may reflect a variable quantity representing the degree of throttling being imposed on wireless communications rather than functioning as a simple on/off indicator as shown in Figure 7. In certain other embodiments, an alarm control indicator may be included as part of the display. These and other variations are within the spirit and scope of the present disclosure.

[0050] Figure 8 depicts a display screen 850 designed to assist enterprise managers in controlling wireless resource usage at the department level. A set of employees having mobile communications devices are displayed in tabular format. For a first employee, Alex Jones, a set of resource bars 852, 854, 856 are shown reflecting the level of Alex Jones' usage of certain wireless resources in the current billing period. The information for an employee also includes his or her name 858, employee number 860 and telephone number 862. The information also includes a throttling control indicator 864. In certain embodiments, throttling control indicator 864 may only reflect whether throttling is activated on the employee's mobile communications device, while in other embodiments it may control whether throttling is activated. While not specifically described for each person shown, the same information is presented for each of the seven individuals, as seen in Figure 8.

[0051] A department summary is included in the lower-right corner of Figure 8, which reflects the total resource usage for the department. This information is provided via graphical resource usage indicators 880, 882, 884 along with textual resource usage indicators 886, 888 and an estimated budget overrun amount 890. Given this information, a manager can budget, and in certain cases control, wireless resource usage within his or her department.

[0052] Corporate control of resource usage can be employed in a number of ways. In certain embodiments, a manager may be given the power to disallow resource usage above a certain limit, which may be expressed in minutes, megabytes or dollars, as examples. A manager may also be tasked with the option to allow unlimited usage through the admin tool. In certain embodiments, the management console may show data for one or more users spanning multiple billing periods. Assuming a user is consistently over or under one or more of his or her allocated resource limits, the management console may highlight the user to the manager for possible plan alteration.

[0053] In embodiments employing some form of usage

throttling mechanism, the manner of usage throttling can vary depending on the application. One method of throttling is depicted in Figure 9. According to the embodiment of Figure 9, throttling is imposed when data usage is higher than expected, while a data boost may be provided when data usage is lower than expected.

[0054] Process flow begins in block 902 and proceeds from there to decision block 904. In decision block 904, a data usage control module, which may include logic or software instructions, determines whether data usage has been greater than expected. If usage is greater than expected, process flow is directed to block 906, where the data usage control module slows down the data transfer rate. If usage is not greater than expected, process flow is directed to decision block 908.

[0055] In decision block 908, data usage control module determines whether usage is less than expected. If data usage is less than expected, process flow is directed to block 910, where the data usage control module speeds up the data transfer rate. If data usage is not less than expected, no throttling mechanism is imposed process flow is directed to block 912, where the process ends.

[0056] As those of skill in the art will appreciate, the present disclosure encompasses a wide variety of individual embodiments and applications within its broader teachings. For example, in certain embodiments, a mobile communications device may be operable to query for a period beginning and period end (or beginning and duration) and from this information measure the elapsed time by comparing the difference from the beginning to the current time on the device against the duration. Also, the device may be operable to measure consumption since the beginning of the billing period.

[0057] In an alternate embodiment, a server may supply the proportion between the resources used and resources available as well as between the time elapsed and time available directly to the device, such that little or no computation is required on the device itself. In certain embodiments, a system may be operable to work with non-periodic "pay as you go" plans. Such a system may, for example, display a portion of used vs. total available resources since the last resource purchase, where the used indicator resets to 0 at the time of purchase. Alternatively, the system may display the remaining resources as a bulk quantity. The current available resources may be acquired from a server, or the system can maintain its own running total by adding up all the purchases and subtracting out the measured usage. In addition, such a "pay as you go" system may display the remaining number of days, projected based on the current consumption rate.

[0058] In certain applications, a combination of the above may be employed. Where, for example, a customer has purchased a monthly plan which provides for a certain level of resources while allowing for the pre-purchase of additional resources during the billing period, the elapsed time vs. time period display would remain, though the resource usage bars could actually go "backward" to reflect the additional resource capacity available after additional resources are purchased.

[0059] In certain embodiments, the resource usage bars may change in appearance if maximum resource usage is exceeded. According to one embodiment, the bar length is proportional to the usage percentage up until 100% of resource usage is reached. After 100% of available resource usage is exceeded, the bar length may then be proportional to the fraction of the planned 100% vs. the running total usage. In certain embodiments, the color or other appearance characteristic of the bars may change at this transition. Further, the device may be operable to display the current price or expense per unit time being incurred by usage of the resource.

[0060] The device may be operable to take into account any periods during which additional resource usage does not incur additional cost under the current billing plan. These may include, for example, nights and weekends. When the device is operating within an unlimited usage period, the usage indicator may be hidden or grayed out.

[0061] Billing plan details stored within the device or elsewhere may contain information about any number of overlapping conditional periods. The server may simply provide the current utilization ratios directly. Alternately, the server may provide static information about the plan, such as the starting and ending conditions for a given period, which may include the time of day or day of the week. From this information, the device could then determine the period within which it is operating and the quantity of resources consumed. Alternately, the device may calculate the ratios from durations and current consumption and elapsed time values provided by the server.

[0062] In certain embodiments, the device may be operable to display the level of resource utilization incurred within a number of different periods without respect to the period within which the device is currently operating.

[0063] In certain embodiments, the device may roam to a network on which it does not have pre-allocated resources. In this situation, the device is in a similar situation to that in which all pre-paid resources have been consumed. In this situation, the device may be operable to begin displaying the immediate rate of resource usage in either resource terms or monetary terms.

[0064] It is believed that the operation and construction of the embodiments of the present disclosure will be apparent from the Detailed Description set forth above. While the exemplary embodiments shown and described may have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present disclosure as set forth in the following claims.

Claims

1. A method for monitoring resource usage of a mobile communications device (116) comprising the steps of:

   acquiring (400) a mobile communication plan profile associated with a subscriber, the plan profile including at least a value representing a limit of mobile communication resource usage within a specified calendar period;
   acquiring (402, 404, 408, 412) resource consumption data relative to the specified calendar period;
   calculating (414, 416) usage statistics based on the resource consumption data and the plan profile; and
   presenting (418) the usage statistics to an entity.

2. The method of claim 1 wherein the specified calendar period is a month.

3. The method of claim 1 wherein at least a portion of the resource consumption data represents cellular telephone usage in minutes.

4. The method of claim 1 wherein at least a portion of the resource consumption data represents wireless data usage in megabytes.

5. The method of claim 1 wherein the usage statistics are displayed to a user of the mobile communications device.

6. The method of claim 1 wherein an alert is generated depending on the usage statistics.

7. A mobile communications device (116) comprising:

   at least one storage area (335) for containing a mobile communication service plan profile associated with a subscriber, the mobile communication service plan profile including at least a value representing a limit of mobile communication resource usage within a specified period;
   at least one storage area (335) for containing resource consumption data relative to the specified period; and
   a wireless resource usage control module (216) for calculating usage statistics based on the resource consumption data and the service plan profile.

8. The mobile communications device (116) of claim 7 wherein at least a portion of the resource consumption data represents cellular telephone usage in minutes.

9. The mobile communications device (116) of claim 7 wherein at least a portion of the resource consumption data represents wireless data usage in megabytes.

10. The mobile communications device (116) of claim 7 wherein the wireless resource usage control module (216) is operable to throttle the amount of bandwidth provided depending on the usage statistics.

11. The mobile communications device (116) of claim 7 wherein the wireless resource usage control module (216) is operable to generate an alert depending on the usage statistics.

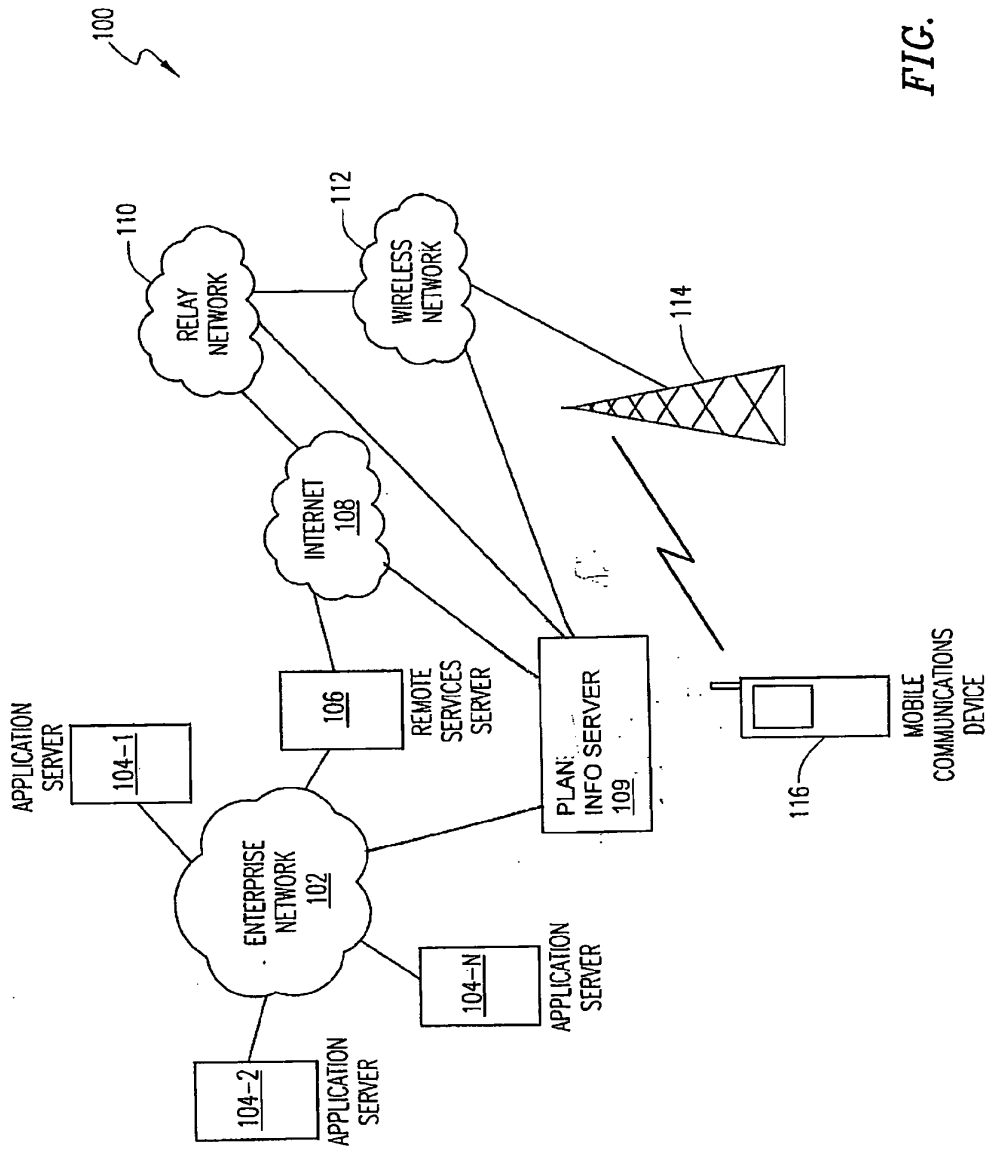

100
110
RELAY NETWORK
112
WIRELESS NETWORK
114
INTERNET 108
106
REMOTE SERVICES SERVER
PLAN INFO SERVER 109
APPLICATION SERVER
104-1
ENTERPRISE NETWORK 102
104-N
APPLICATION SERVER
104-2
APPLICATION SERVER
116
MOBILE COMMUNICATIONS DEVICE

FIG. 1

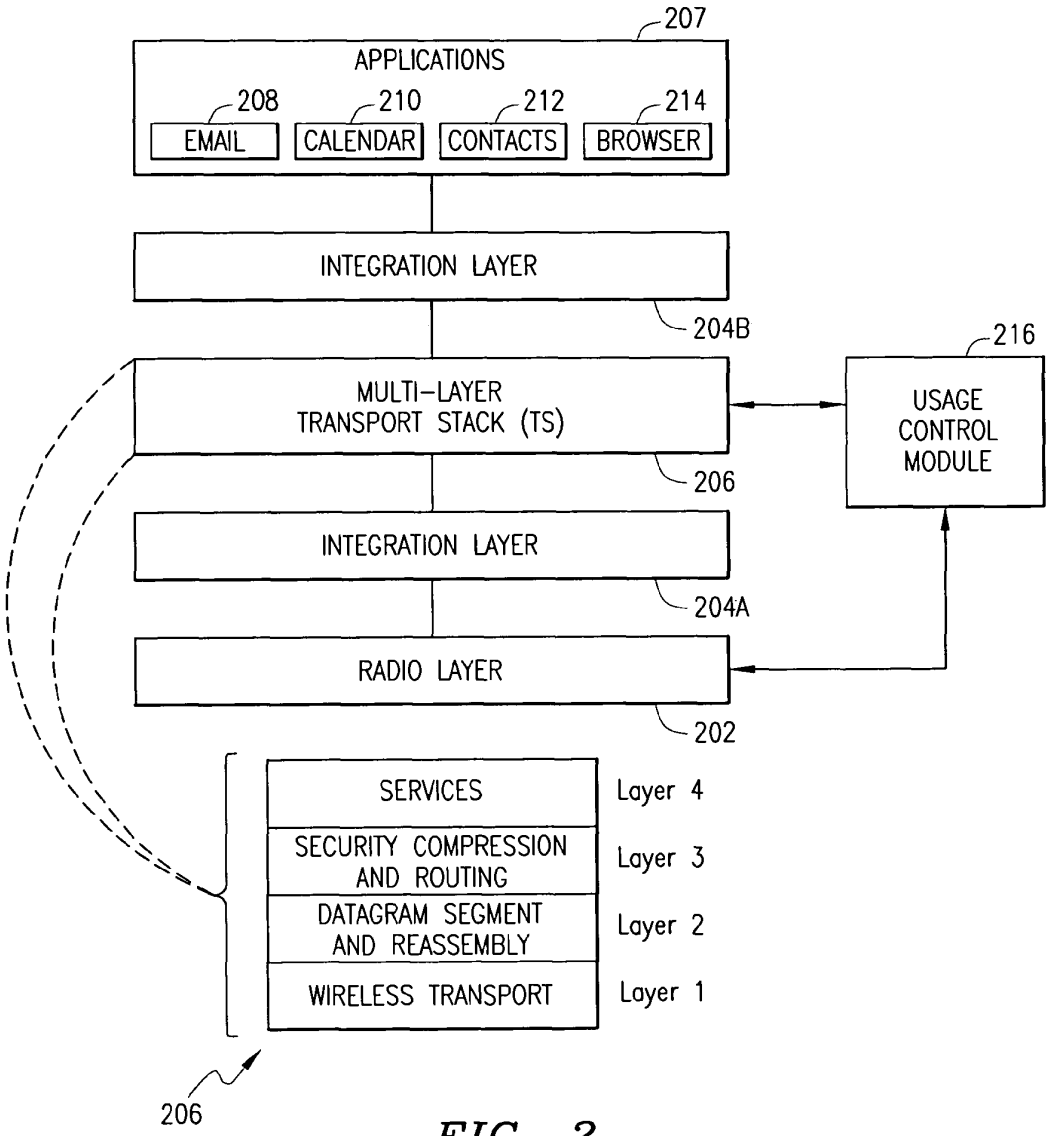

207
APPLICATIONS
208
EMAIL
210
CALENDAR
212
CONTACTS
214
BROWSER
INTEGRATION LAYER
204B
216
MULTI-LAYER
TRANSPORT STACK (TS)
USAGE
CONTROL
MODULE
206
INTEGRATION LAYER
204A
RADIO LAYER
202
SERVICES
Layer 4
SECURITY COMPRESSION
AND ROUTING
Layer 3
DATAGRAM SEGMENT
AND REASSEMBLY
Layer 2
WIRELESS TRANSPORT
Layer 1
206

FIG. 2

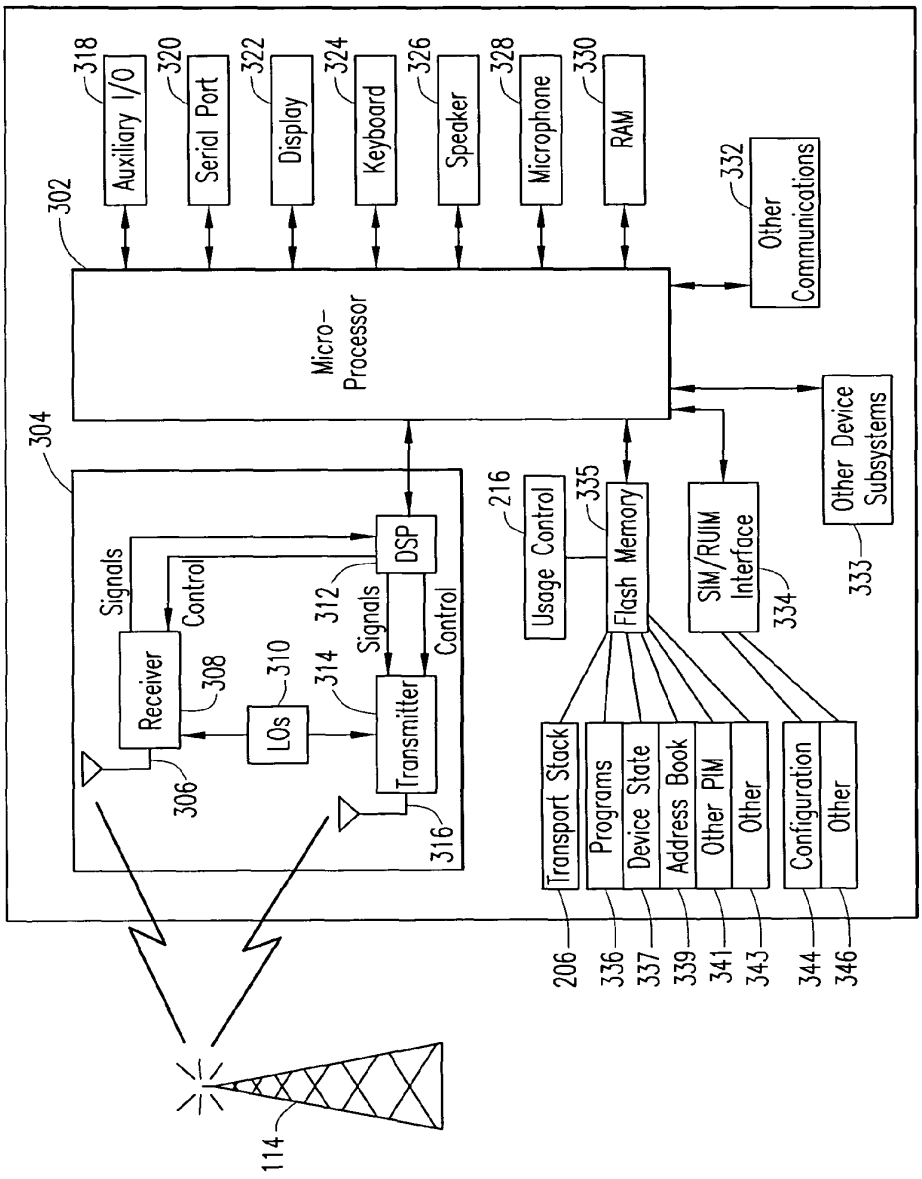

318
Auxiliary I/O
320
Serial Port
322
Display
324
Keyboard
326
Speaker
328
Microphone
330
RAM
332
Other Communications
302
Micro-Processor
304
Signals
Control
Receiver
308
306
LOs
310
314
312
Signals
DSP
Control
Transmitter
316
216
Usage Control
335
Flash Memory
SIM/RUIM Interface
334
Other Device Subsystems
333
Transport Stack
Programs
Device State
Address Book
Other PIM
Other
Configuration
Other
206
336
337
339
341
343
344
346
114

FIG. 3

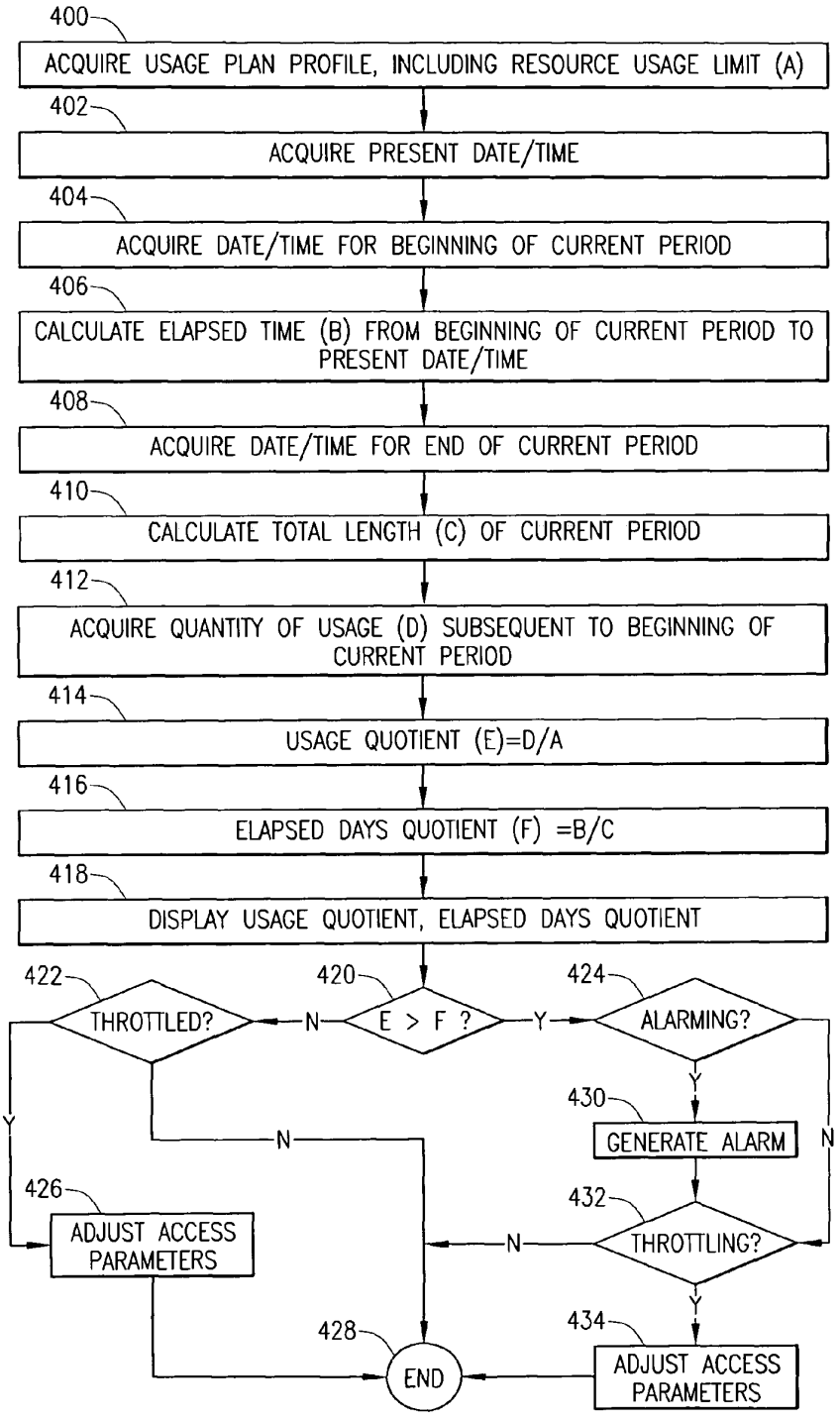

400
ACQUIRE USAGE PLAN PROFILE, INCLUDING RESOURCE USAGE LIMIT (A)
402
ACQUIRE PRESENT DATE/TIME
404
ACQUIRE DATE/TIME FOR BEGINNING OF CURRENT PERIOD
406
CALCULATE ELAPSED TIME (B) FROM BEGINNING OF CURRENT PERIOD TO PRESENT DATE/TIME
408
ACQUIRE DATE/TIME FOR END OF CURRENT PERIOD
410
CALCULATE TOTAL LENGTH (C) OF CURRENT PERIOD
412
ACQUIRE QUANTITY OF USAGE (D) SUBSEQUENT TO BEGINNING OF CURRENT PERIOD
414
USAGE QUOTIENT (E)=D/A
416
ELAPSED DAYS QUOTIENT (F) =B/C
418
DISPLAY USAGE QUOTIENT, ELAPSED DAYS QUOTIENT
420
E > F ?
N
Y
422
THROTTLED?
Y
N
426
ADJUST ACCESS PARAMETERS
424
ALARMING?
Y
N
430
GENERATE ALARM
432
THROTTLING?
N
Y
434
ADJUST ACCESS PARAMETERS
428
END

FIG. 4

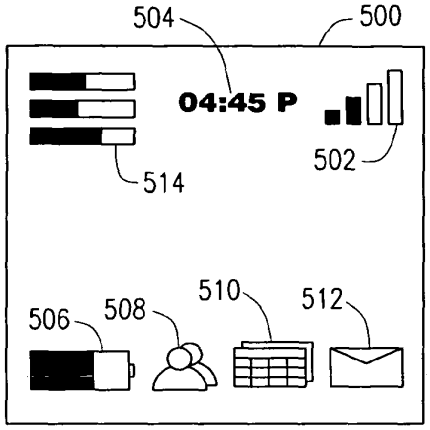


FIG. 5

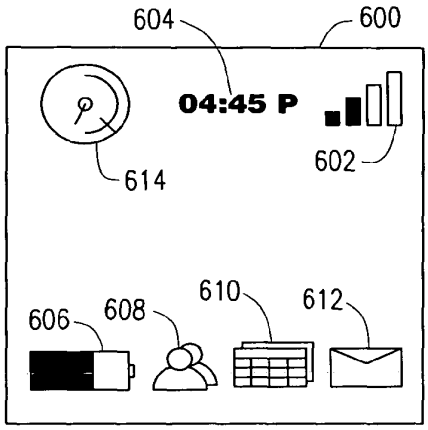


FIG. 6

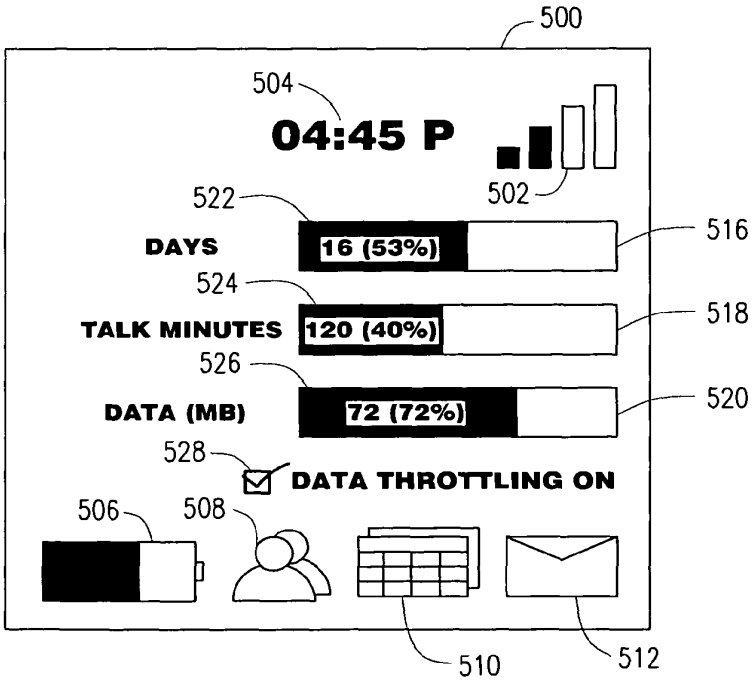


FIG. 7

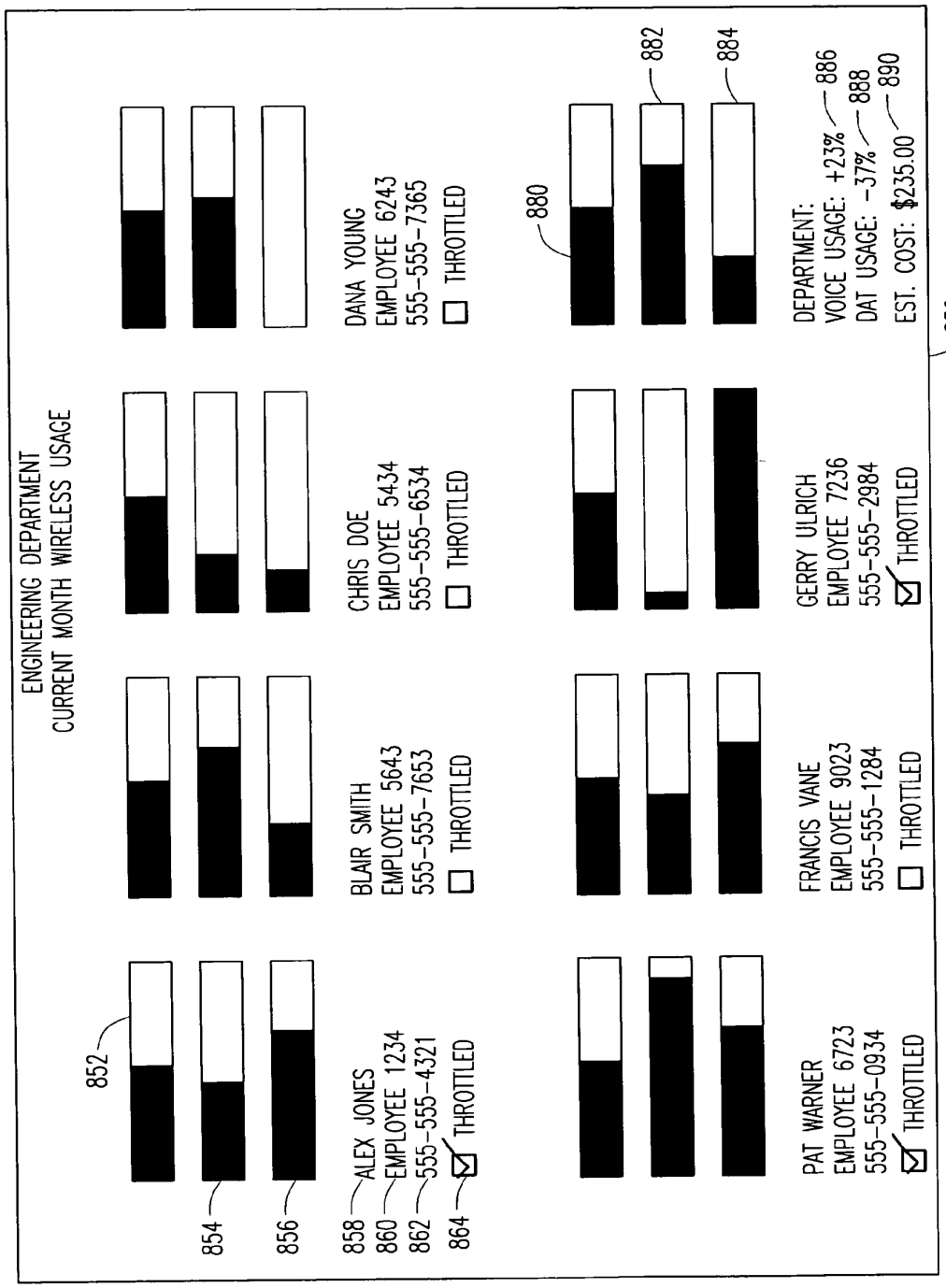

ENGINEERING DEPARTMENT
CURRENT MONTH WIRELESS USAGE
852
854
856
858 ALEX JONES
860 EMPLOYEE 1234
862 555-555-4321
864 THROTTLED
BLAIR SMITH
EMPLOYEE 5643
555-555-7653
THROTTLED
CHRIS DOE
EMPLOYEE 5434
555-555-6534
THROTTLED
DANA YOUNG
EMPLOYEE 6243
555-555-7365
THROTTLED
880
882
884
PAT WARNER
EMPLOYEE 6723
555-555-0934
THROTTLED
FRANCIS VANE
EMPLOYEE 9023
555-555-1284
THROTTLED
GERRY ULRICH
EMPLOYEE 7236
555-555-2984
THROTTLED
DEPARTMENT:
VOICE USAGE: +23%
DAT USAGE: -37%
EST. COST: $235.00
886
888
890
850

FIG. 8

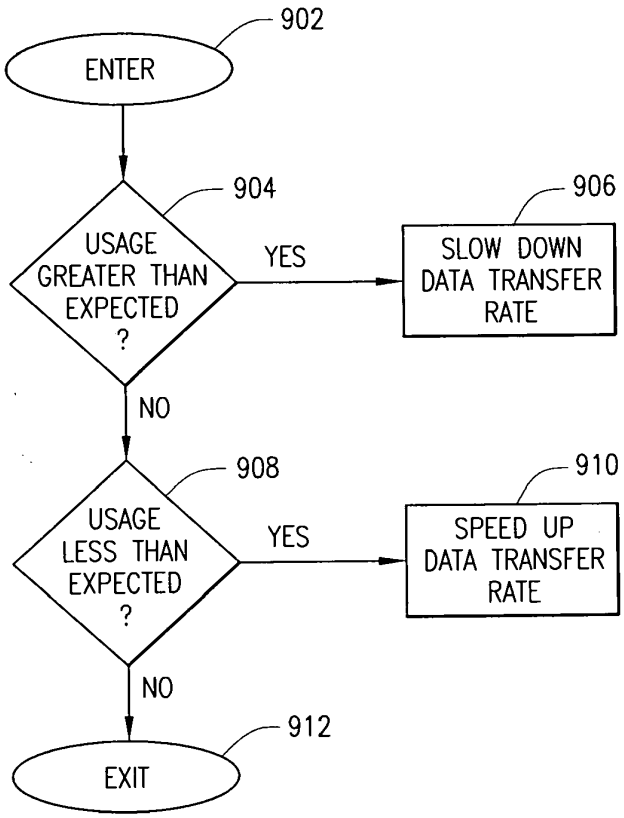

902
ENTER
904
USAGE GREATER THAN EXPECTED ?
YES
906
SLOW DOWN DATA TRANSFER RATE
NO
908
USAGE LESS THAN EXPECTED ?
YES
910
SPEED UP DATA TRANSFER RATE
NO
912
EXIT

FIG. 9

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 2276

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2001/055961 A1 (NAKAJIMA TAKETOSI) 27 December 2001 (2001-12-27) * paragraphs [0023] - [0046] * * figures 1,2 *	1,2,4-7, 9-11	INV. H04M15/28 H04M17/00 ADD. H04Q7/32 H04Q7/38
X	WO 00/70860 A (ERICSSON, INC) 23 November 2000 (2000-11-23) * page 8, line 6 - page 9, line 16 * * page 12, line 13 - page 17, line 17 * * figures 3,4,9,10,11A,11B *	1-9,11	
X	EP 1 528 781 A (BOUYGUES TELECOM) 4 May 2005 (2005-05-04) * paragraphs [0002], [0003], [0019] - [0032], [0034], [0040], [0045] * * figures 1-6 *	1-5,7-9	
X	WO 02/058326 A (TELEFONAKTIEBOLAGET L M ERICSSON ; ERICSSON, ANDREAS) 25 July 2002 (2002-07-25) * page 3, line 13 - page 6, line 15 * * page 8, lines 9-25 * * figures 1-3 *	1,2,4-7, 9,11	TECHNICAL FIELDS SEARCHED (IPC) H04M H04Q
X	WO 2004/030390 A (BRIGHT STAR TECHNOLOGIES, INC; BEKANICH, JOSEPH) 8 April 2004 (2004-04-08) * page 15, line 22 - page 21, line 21 * * page 26, line 14 - page 27, line 20 * * figures 8-13 *	1-9,11	
X	US 2002/151293 A1 (TYSOR ARTHUR JAMES) 17 October 2002 (2002-10-17) * paragraphs [0022] - [0048] * * figures 3,5A,5B,6 *	1-3,5-8, 11	

-/--

1 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 June 2006	Kanlis, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 2276

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2006/000994 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; MOTTE, STEFAAN; MASSCHELEIN, MARC) 5 January 2006 (2006-01-05) * page 3, line 31 - page 6, line 18 * -----	7,9,10	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 June 2006	Kanlis, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 06 25 2276

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-06-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001055961 A1	27-12-2001	CN 1305268 A	25-07-2001
		GB 2364213 A	16-01-2002
		HK 1036703 A1	30-06-2005
		JP 3509670 B2	22-03-2004
		JP 2001168916 A	22-06-2001
WO 0070860 A	23-11-2000	AT 303038 T	15-09-2005
		AU 4465100 A	05-12-2000
		CN 1361974 A	31-07-2002
		DE 60022181 D1	29-09-2005
		DE 60022181 T2	01-06-2006
		EP 1179262 A1	13-02-2002
		JP 2003500904 T	07-01-2003
		US 6493547 B1	10-12-2002
EP 1528781 A	04-05-2005	FR 2861942 A1	06-05-2005
WO 02058326 A	25-07-2002	JP 2004517586 T	10-06-2004
WO 2004030390 A	08-04-2004	NONE	
US 2002151293 A1	17-10-2002	NONE	
WO 2006000994 A	05-01-2006	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Electronic Acknowledgement Receipt

EFS ID:	23540615
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	18-SEP-2015
Filing Date:	15-NOV-2013
Time Stamp:	16:35:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1.pdf	615065 41aa96985d4e2860567f62da3c2f522b9cfd81ae	no	11

Warnings:	
Information:	

2	Foreign Reference	2066_Fujitsu.pdf	856885 72e75495c5d83e30e4fbefee0e38a1bb25a5405f	no	22
Warnings:					
Information:					
3	Foreign Reference	2067_Kyocera.pdf	641903 024bbc366c4ffca0d6206fd9400790e51cab71c3	no	27
Warnings:					
Information:					
4	Foreign Reference	2068_Citrix.pdf	14110049 6b5308424d6052f222f99c6297e0f2cd005b02d2	no	118
Warnings:					
Information:					
5	Foreign Reference	2069_CN1508734A.pdf	3021193 c8818fe2ac00cd927bb1eb76517cffb16566e7c4	no	24
Warnings:					
Information:					
6	Foreign Reference	2070_CA2688553.pdf	2542550 eaac858569669488781074475 9dc83d1126bb215	no	72
Warnings:					
Information:					
7	Foreign Reference	2071_EP1850575A1.pdf	306349 f0b875706a2088fd443e7a61ffec5c6632823551	no	18
Warnings:					
Information:					
8	Non Patent Literature	3044_Jing.pdf	233308 23bf275a591ba14bba9ea0e8edf96ff232de6df3	no	41
Warnings:					
Information:					
9	Non Patent Literature	3045_Rivadeneyra.pdf	140975 e344ac7c8eee7e286c50068b497b45c8a4dbefbe	no	11
Warnings:					
Information:					
10	Non Patent Literature	3046_loopt.pdf	380265 711a9ba25d7f71b9274655d90ad2022e3b79c85c	no	17
Warnings:					
Information:					

11	Non Patent Literature	3047_MobilInternet.pdf	168840 0ed6b3905753995265d6ebaf790a5696b8b5efb3	no	3
Warnings:					
Information:					
12	Non Patent Literature	3048_GoldCoast.pdf	164580 e7407b7a4570d9ebfc790e44249d0cdb07f36182	no	2
Warnings:					
Information:					
13	Non Patent Literature	3049_Richtel.pdf	92162 6eecd8013a6328084fb9f16f25afc3b9619c9dee	no	3
Warnings:					
Information:					
14	Non Patent Literature	3050_Kim.pdf	94063 d57c26581b209a675dcd915b2be9c9e56a005a1f	no	4
Warnings:					
Information:					
15	Non Patent Literature	3051_Koutsopoulou.pdf	113527 7992fa4c1d1306edb1de247f743fd1ce8b1f3e7d	no	9
Warnings:					
Information:					
16	Non Patent Literature	3052_Sun.pdf	102743 66e9aab3798130ba2a58b46d24cec206617531de	no	8
Warnings:					
Information:					
17	Non Patent Literature	3053_Sabat.pdf	389581 c6862777fa3e8b3a13a7509f02610e154cf4299d	no	31
Warnings:					
Information:					
18	Non Patent Literature	3054_Nuzman.pdf	580822 f0c09248f7c9794a5ea827b4d574c49719823113	no	19
Warnings:					
Information:					
		Total Files Size (in bytes):	24554860		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6438575	B1	2002-08-20	Khan et al.	
	2	6578076	B1	2003-06-10	Putzolu, David Matthew	
	3	6697821	B2	2004-02-24	Ziff et al.	
	4	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	5	6982733	B1	2006-01-03	McNally et al.	
	6	6983370	B2	2006-01-03	Eaton et al.	
	7	7084775	B1	2006-08-01	Smith, Michael R.	
	8	7133695	B2	2006-11-07	Beyda, William J.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7222304	B2	2007-05-22	Beaton et al.	
	10	7260382	B1	2007-08-21	Lamb et al.	
	11	7271765	B2	2007-09-18	Stilp et al.	
	12	7318111	B2	2008-01-08	Zhao, Wen	
	13	7561899	B2	2009-07-14	Lee, Changseok	
	14	7627872	B2	2009-12-01	Hebeler et al.	
	15	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	16	7685530	B2	2010-03-23	Sherrard et al.	
	17	7760137	B2	2010-07-20	Martucci et al.	
	18	7843843	B1	2010-11-30	Papp III et al.	
	19	7925778	B1	2011-04-12	Wijnands et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	21	7937450	B2	2011-05-03	Janik, Craig M.	
	22	8010082	B2	2011-08-30	Sutaria et al.	
	23	8019846	B2	2011-09-13	Roelens et al.	
	24	8050705	B2	2011-11-01	Sicher et al.	
	25	8064418	B2	2011-11-22	Maki, Lasse	
	26	8086791	B2	2011-12-27	Caulkins, Jason	
	27	8103285	B2	2012-01-24	Kalhan, Amit	
	28	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
	29	8200200	B1	2012-06-12	Belser et al.	
	30	8229914	B2	2012-07-24	Ramer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	8233433	B2	2012-07-31	Kalhan, Amit	
	32	8249601	B2	2012-08-21	Emberson et al.	
	33	8259692	B2	2012-09-04	Bajko, Gabor	
	34	8406736	B2	2013-03-26	Das et al.	
	35	8489110	B2	2013-07-16	Frank et al.	
	36	8495181	B2	2013-07-23	Venkatraman et al.	
	37	8514927	B2	2013-08-20	Sundararajan et al.	
	38	8522249	B2	2013-08-27	Beaule, Stephane	
	39	8532610	B2	2013-09-10	Manning Cassett et al.	
	40	8571598	B2	2013-10-29	Valavi, John J.	
	41	8631428	B2	2014-01-14	Scott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	8634425	B2	2014-01-21	Gorti et al.	
	43	8701015	B2	2014-04-15	Bonnat, Pierre	
	44	8739035	B2	2014-05-27	Trethewey, Jim	
	45	8804517	B2	2014-08-12	Oerton, Kevin John	
	46	8825109	B2	2014-09-02	Montemurro et al.	
	47	8831561	B2	2014-09-09	Sutaria et al.	
	48	8880047	B2	2014-11-04	Konicek et al.	
	49	8930238	B2	2015-01-06	Coffman et al.	
	50	8949597	B1	2015-02-03	Reeves et al.	
	51	8977284	B2	2015-03-10	Reed, Mark J.	
	52	9014973	B2	2015-04-21	Ruckart, John	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040259534	A1	2004-12-23	Chaudhari et al.	
	2	20060072451	A1	2006-04-06	Ross, Alan D.	
	3	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	4	20070192460	A1	2007-08-16	Choi et al.	
	5	20070293191	A1	2007-12-20	Mir et al.	
	6	20070294410	A1	2007-12-20	Pandya et al.	
	7	20080050715	A1	2008-02-28	Golczewski et al.	
	8	20080080457	A1	2008-04-03	Cole, Terry L.	
	9	20080282319	A1	2008-11-13	Fontijn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	10	20090049518	A1	2009-02-19	Roman et al.	
	11	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	12	20100151866	A1	2010-06-17	Karpov et al.	
	13	20100248719	A1	2010-09-30	Scholaert, Hugh	
	14	20110145920	A1	2011-06-16	Mahaffey et al.	
	15	20130326356	A9	2013-12-05	Zheng et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	2	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	3	101815275A	CN	A	2010-08-25	Yang, Liu		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	4	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐
	5	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	6	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	2	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐
	3	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	4	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	5	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-06-18
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04M 1/00 (2006.01)
H04M 1/21 (2006.01)
G04G 5/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200410099356.1

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1801829A

[22] 申请日 2004.12.30
[21] 申请号 200410099356.1
[71] 申请人 昆达电脑科技（昆山）有限公司
地址 215300 江苏省昆山市昆山出口加工区
[72] 发明人 许世法

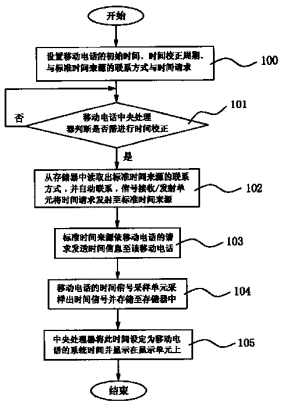
权利要求书 1 页 说明书 3 页 附图 2 页

[54] 发明名称

移动电话时间自动校正方法

[57] 摘要

本发明揭示一种移动电话时间自动校正方法，该移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信号的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，该方法主要通过设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，当需进行时间校正时，该移动电话自动将时间请求发送至标准时间来源，并取得标准时间，而后将该标准时间设定为移动电话的系统时间，从而令移动电话使用一般的石英振荡器亦可满足较高的时间精度，从而利于降低移动电话成本，并不影响移动电话的体积。



1、一种移动电话时间自动校正方法，该移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信息的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，其特征在于该时间自动校正方法包括如下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话的存储器中；

移动电话中央处理器判断是否需进行时间校正，如否则继续判断；

如需进行时间校正，则移动电话自动发射请求信号至标准时间来源；

标准时间来源依请求发送时间信息至该移动电话；

移动电话的时间信号采样单元采样出时间信号并存储至存储器中；

中央处理器将该时间设定为移动电话的系统时间。

2、如权利要求1所述的移动电话时间自动校正方法，其特征在于:该方法还包括将移动电话的系统时间显示在显示单元上的步骤。

3、如权利要求1或2所述的移动电话时间自动校正方法，其特征在于：该标准时间来源为声询台。

4、如权利要求3所述的移动电话时间自动校正方法，其特征在于：该移动电话内设有语音产生单元与语音辨识单元，行动电话中预先设有的时间询问请求为询问时间的声音信号。

5、如权利要求4所述的移动电话时间自动校正方法，其特征在于：当移动电话呼叫声询台后，移动电话通过语音产生单元提出时间询问请求。

6、如权利要求5所述的移动电话时间自动校正方法，其特征在于：声询台依请求发送的时间信号至移动电话，该信号经过移动电话的语音产生单元发出，并且移动电话的语音辨识单元采样出时间信号并存储至存储器中。

7、如权利要求1或2所述的移动电话时间自动校正方法，其特征在于：该标准时间来源为移动电话服务供应网络。

8、如权利要求7所述的移动电话时间自动校正方法，其特征在于：该移动电话中预先设有的时间询问请求为询问时间的短信。

9、如权利要求8所述的移动电话时间自动校正方法，其特征在于：移动电话从存储器中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元将询问时间的短信发射至移动电话服务供应纲络。

10、如权利要求9所述的移动电话时间自动校正方法，其特征在于：移动电话服务供应纲络以短信形式发送标准时间至该移动电话，移动电话的时间信号采样单元采样出时间信号并存储至存储器中。

移动电话时间自动校正方法

【技术领域】

本发明有关一种时间自动校正方法，尤其是应用于移动电话中的时间自动校正方法。

【背景技术】

随着通讯技术的发展，具有时钟功能的移动电话普及率日益提高，其中时钟的准确性在移动电话的实际使用中的重要性日益提高，如现在的备忘录、闹钟等功能的实现均依靠时钟的准确性。而目前时钟的精确性主要取决于时钟电路中使用的振荡器的精度，而目前多使用普通的石英振荡器，其频率误差在±20-50ppm（百万分之20-50），如以20ppm的误差为例，每天产生的时间误差将为1.728秒，而一年的时间误差则累积为630.72秒，将达10.5分钟之久，故会给使用者带来一定的不便。

针对该问题，业界采取使用较高精度的石英振荡器或使用微调电容或类似的元件对普通振荡器的频率进行微调的二种方法。第一种方法的不足在于：即使使用高精度的石英振荡器，振荡电路的负载电容依存在差别，所以实际上不可能得到与石英振荡器相同的高精度，因此无论使用多么昂贵的元件，也不可能得到高准确度的时间。第二种方法的不足之处在于：虽然使用一般的石英振荡器成本不会太高，但是需要频率调节装置，如微调电容器，这引起了部件成本增加和令频率调节过程较为繁琐的缺陷，特别是元件数量的增加会导致对移动电话小型化的妨碍。

有鉴于此，实有必要提供一种既不会增加移动电话成本，且不影响移动电话体积的移动电话时间自动校正方法。

【发明内容】

本发明目的在于提供一种既不会增加移动电话成本，且不影响移动电话体积的移动电话时间自动校正方法。

为实现上述目的，实施本发明的移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信号的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，本发明移动电话时间的自动校正方法包括以下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话的存储器中；

移动电话中央处理器判断是否需进行时间校正，如否则继续判断；

如需进行时间校正，则移动电话自动发射请求信号至标准时间来源；

标准时间来源依请求发送时间信息至该移动电话；

移动电话的时间信号采样单元采样出时间信号并存储至存储器中；

中央处理器将该时间设定为移动电话的系统时间。

较佳地，该标准时间来源为声询台，移动电话通过呼叫声询台提出时间请求，并且声询台发送的时间信号至移动电话，该信号经过移动电话的语音产生单元发出，并且移动电话的语音辨识单元采样出时间信号并存储至存储器中。

较佳地，该标准时间来源为移动电话服务供应网络，移动电话通过发送短信至移动电话服务供应纲络提出时间请求，并且移动电话服务供应纲络发送标准时间至该移动电话，移动电话的时间信号采样单元采样出时间信号并存储至存储器中。

与现有技术相比较，本发明利用移动电话联系外部的标准时间来源定期对移动电话的系统时间进行校正，从而可定期将时间误差及时消除，因此即使移动电话的时钟电路采用一般的石英振荡器，也不会给使用者造成不便，如此不需采用较为昂贵的石英振荡器或其它的微调电容器等，因此不会增加移动电话的成本，并且也不会对移动电话的小型化形成妨碍。

为对本发明的目的、构造特征及其功能有进一步的了解，兹配合附图详细说明如下：

【附图说明】

图 1 为本发明移动电话的组成框图。

图 2 为本发明移动电话时间自动校正方法的流程图。

【具体实施方式】

以下将结合图 1 与图 2 对本发明的进行详细说明，在以下说明中是以行动电话为例进行说明，该技术领域的普通技术人员应可理解，实施本发明的电子装置并不局限于移动电话，如具有无线通信功能的智能电话及个人数字助理（PDA）均可应用本发明。

请参阅图 1 所示，实施本发明的移动电话 1 包括：

信号接收/发射单元 10，用于发射与接收无线通讯信号；

时间信号采样单元 11，与信号接收/发射单元 10 耦接，用以将接收信号中的时间信号采样出；

存储器 12，用以存储移动电话 1 的系统程序、时间校正周期、标准时间来源的联系方式及移动电话 1 的最初设定时间；

显示单元 14，用以显示移动电话 1 的系统时间；

中央处理器 13，与上述各单元耦接，用以控制以上不同单元的运作。

请参阅图 2 所示，本发明的移动电话 1 的时间自动校正方法包括以下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话 1 的存储器 12 中，其中时间校正周期可设定为一周或一个月，而标准时间来源可为声询台，如中国大陆的 114 查询台或中国台湾的 104 报时台（步骤 100）；

移动电话 1 中央处理器 13 判断是否需进行时间校正，即从最初设定的时间起，是否经过设定的时间校正周期的时间，如否则继续判断（步骤 101）；

如需进行时间校正，即从最初设定的时间起，已经过设定的时间校正周期的时间，则移动电话 1 的中央处理器 13 执行自动联系功能，即从存储器 12 中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元 10 将时间请求发射至标准时间来源（步骤 102）；

标准时间来源依移动电话 1 的请求发送时间信息至该移动电话 1(步骤 103）；

移动电话 1 的时间信号采样单元 11 采样出时间信号并存储至存储器 12 中（步骤 104）；

中央处理器 13 将此时间设定为移动电话 1 的系统时间并显示在显示单元 14 上（步骤 105)。

较佳地，当该标准时间来源为声询台时，而移动电话 1 内设有语音产生单元与语音辨识单元，步骤 100 中包括预先在移动电话 1 内设定时间询问请求，如可为询问时间的声音信号，步骤 102 具体包括以下步骤：当移动电话 1 呼叫声询台后，移动电话 1 通过语音产生单元提出时间询问请求，而步骤 103 相应包括以下步骤：声询台依次请求发送的时间信号至移动电话 1，该信号经过移动电话 1 的语音产生单元发出，并且移动电话 1 的语音辨识单元采样出时间信号并存储至存储器 12 中。

较佳地，当该标准时间来源为移动电话服务供应网络，步骤 100 中包括预先在移动电话 1 内设定时间询问请求，如可为询问时间的短信，步骤 102 具体包括以下步骤：移动电话 1 从存储器 12 中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元 10 将询问时间的短信发射至移动电话服务供应纲络，而步骤 103 相应包括以下步骤：移动电话服务供应纲络以短信形式发送标准时间至该移动电话 1，移动电话的时间信号采样单元 11 采样出时间信号并存储至存储器 12 中。

与现有技术相比较，本发明利用移动电话联系外部的标准时间来源定期对移动电话的系统时间进行校正，从而可定期将时间误差及时消除，因此即使移动电话的时钟电路采用一般的石英振荡器，也不会给使用者造成不便，如此不需采用较为昂贵的石英振荡器或其它的微调电容器等，因此不会增加移动电话的成本，并且也不会对移动电话的小型化形成妨碍。

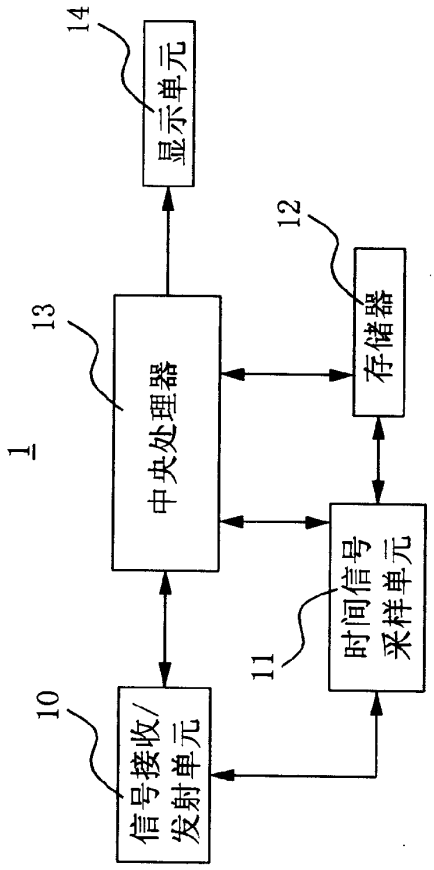


图1

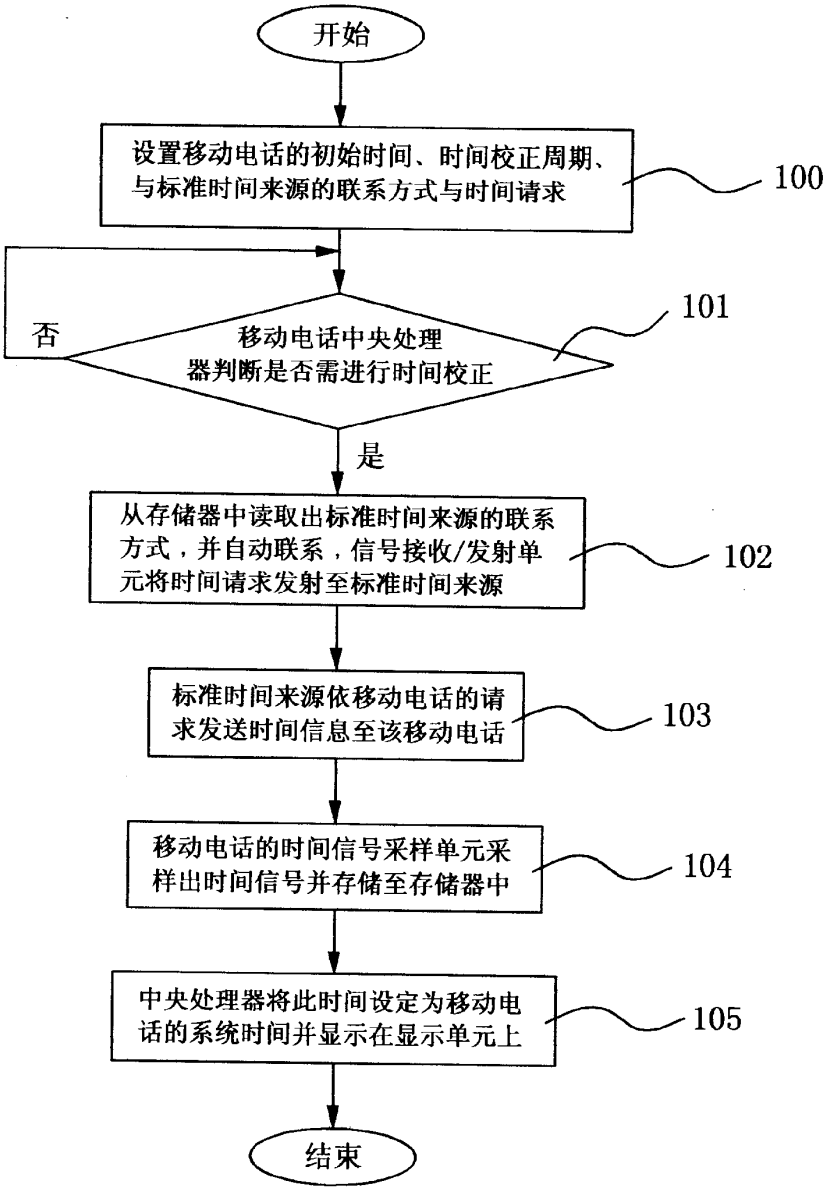

开始
设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求
100
否
移动电话中央处理器判断是否需进行时间校正
101
是
从存储器中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元将时间请求发射至标准时间来源
102
标准时间来源依移动电话的请求发送时间信息至该移动电话
103
移动电话的时间信号采样单元采样出时间信号并存储至存储器中
104
中央处理器将此时间设定为移动电话的系统时间并显示在显示单元上
105
结束

图2

Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Mobile phone time automatic correction method

CN 1801829 A

Publication number	CN1801829 A
Publication type	Application
Application number	CN 200410099356
Publication date	Jul 12, 2006
Filing date	Dec 30, 2004
Priority date	Dec 30, 2004
Inventors	许世法
Applicant	昆达电脑科技(昆山)有限公司
Export Citation	BiBTeX, EndNote, RefMan

Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

Said invention provides a mobile telephone time autocorrection method. It contains signal reception / transmitting unit, time signal sampling unit memory unit, central processing unit and display unit, said method mainly setting mobile telephone initial time, time adjustment cycle, and standard time source connection mode and time request , when need proceeding time correction, said mobile telephone automatically transmitting time request to standard time source and taking standard time then configuring said standard time as system time of mobile telephone to reach higher time precision by using normal quartz oscillator.

DESCRIPTION translated from Chinese

Mobile phone time automatic calibration method

TECHNICAL FIELD The present invention relates to a method of automatic correction of the time, especially for mobile phones in the automatic time correction method.

BACKGROUND OF THE INVENTION With the development of communication technology, mobile phone penetration has a clock function increasing importance of the accuracy of the clock and the actual use of mobile phones increasing, as now realize memo, alarm clock and other functions both rely on the accuracy of the clock. At present, the accuracy of the clock depends on the accuracy of the clock oscillator used in the circuit, and the current multi-use ordinary quartz oscillator frequency error at ± 20-50ppm (20-50 ppm), as to 20ppm error, for example, the time error will be generated every 1.728 seconds, while the one-year time error accumulation is 630.72 seconds, to reach 10.5 minutes long, it will bring some inconvenience to users.

To solve this problem, the industry adopted the use of high precision quartz oscillator or use a trimmer capacitor or similar elements of the common oscillator frequency tuning of the two methods. The first method is inadequate: even when using high-precision quartz oscillator, the oscillation circuit of the load capacitance according to the presence of differences, so this is actually impossible to obtain the same high-precision crystal oscillator, and therefore regardless of 11 more expensive components, it is impossible to obtain a highly accurate time. Deficiencies of the second method comprising: using a general quartz oscillator although cost is not too high, but requires a frequency adjustment means, such as a trimmer capacitor, causing an increase in component cost and make the process more complicated frequency adjusting defects, particularly is an increase in the number of components will result in miniaturization of mobile phones interfere.

In view of this, there is a need to provide both a mobile phone without increasing the cost, and does not affect the time the mobile phone automatic calibration method for a mobile phone volume.

SUMMARY OF THE INVENTION The present invention aims to provide a mobile phone without increasing either the cost, and does not affect the time the mobile phone automatic calibration method for a mobile phone volume.

CLAIMS (10) translated from Chinese

A mobile phone automatic time correction method, the mobile phone includes a signal receiving / transmitting unit receives the signal and the transmitted signal, the received signal samples from the time information in the time signal sampling unit that stores the time information and the setting information memory, the central processor and display unit, characterized in that the automatic time correction method comprising the steps of: setting an initial time a mobile phone, the correction time period, and the contacts for the source of the standard time and time request, and such data is stored in memory of the mobile phone; mobile phone to determine whether the need for a central processor time correction, otherwise continue as judge; For the time correction, the mobile phone automatically transmit a request signal to the standard time source; transmission time information source standard time upon request to the mobile phone; mobile phone time signal sampling means sampling and storing the time signal into the memory; central processing time is set to the system time of the mobile phone.

The mobile phone automatic time correction method according to claim 1, characterized in that: the method further comprises the mobile telephone system time is displayed on the display unit in step.

Automatic time correction method for a mobile phone according to claim 1 or claim 2, wherein: the standard time for the sound source exercise station.

The mobile phone automatic time correction method according to claim 3, characterized in that: the mobile phone equipped with a voice generating unit and a voice recognition unit, the mobile phone has to call a pre-request signal into sound inquiry time .

The mobile phone automatic time correction method according to claim 4, wherein: when the mobile telephone calling sound exercise station, mobile phone unit made by voice time inquiry request is generated.

Identification of the mobile phone and the speech sound exercise station by a time request signal to the mobile phone, the mobile phone voice signal through generating unit issued: The mobile phone automatic time correction method according to claim 5, characterized in that means sampling and storing the time signal into the memory.

To achieve the above object, a mobile phone embodiment of the present invention includes a signal receiving / transmitting unit receives the signal and the transmitted signal, a time signal sampling time signal sampling unit from the received signal, the memory storing the time information and setting information, Automatic time correction method for a mobile phone central processor and a display unit, the present invention comprises the steps of: setting the mobile phone of the initial time, the correction time period, and the contacts for the source of the standard time and time request, and such data stored in the mobile phone memory; the central processor determines whether the mobile phone need to be time correction, otherwise continue as judge;

For a time correction, the mobile phone automatically transmit a request signal to the standard time source; Standard Time time information sources according to the request of the mobile phone; mobile phone signal sampling unit time sampling the time signal and storage to memory; a central processing The time is set to a mobile telephone system time.

Preferably, the standard time for the sound source exercise station, mobile telephone inquiry station calling sound made by the time the request, and the time the signal transmitted by the acoustic exercise station to the mobile phone, the signal through the mobile phone voice generating unit is issued, and the mobile phone sampling the speech recognition unit time signal and stores into the memory.

The mobile phone automatic time correction method according to claim 1 or claim 2, wherein: the standard time source for cellular phone service network.

Mobile phone time automatic calibration method according to claim 7, characterized in that: the mobile phone in advance of the time provided for the inquiry message query request time.

The mobile phone automatic time correction method according to claim 8, wherein: the mobile phone reads from the memory the standard time source contact, and automatic contact, signal receiving / transmitting unit transmitting the inquiry message time Mobile phone service providers to network in.

Mobile phone time automatic calibration method as claimed in claim 9, wherein: the mobile phone service provider network in order to send a message in the form of standard time to the mobile phone, mobile phone signal sampling unit time sampling the time signal and stores to memory.

Preferably, the standard time source for mobile phone service provider networks, mobile phone by sending an SMS to a mobile phone service network in time to make the request, and the mobile phone service provider network in standard time sent to the mobile phone, mobile phone time signal sampling means sampling the time signal and stores into the memory.

Compared with the prior art, the present invention is the use of a mobile phone outside the regular standard time source mobile phone system time is corrected, thereby periodically time error promptly eliminated so that even if the mobile phone is generally of a clock circuit using a quartz oscillator nor will cause inconvenience to the user, so the need to adopt a more expensive quartz oscillator or other fine-tuning capacitor, etc., it will not increase the cost of mobile phones, and nor will it interfere with the formation of the miniaturization of mobile phones.

For the purposes of this invention, the structural features and functions have a better understanding, with a detailed description of the drawings hereby follows: BRIEF DESCRIPTION Figure 1 is a block diagram of the invention of mobile phones.

Figure 2 is a schematic flow chart of a mobile phone automatic time correction method.

[DETAILED DESCRIPTION] Hereinafter, in conjunction with Figure 1 and Figure 2 the present invention will be described in detail, based on the mobile phone as an example in the following description, one of ordinary skill in the art will appreciate, electronic embodiment of the electronic apparatus of the present invention is not limited to a mobile phone, having a wireless communication function such as smart phones and personal digital assistants (PDA) can be applied to the present invention.

See Figure 1, the embodiment of the present invention, a mobile phone 1 includes: a signal receiving / transmitting unit 10 for transmitting and receiving wireless communication signals; time signal sampling unit 11, and the signal receiving / transmitting unit 10 is coupled to the received signal in the time signal samples; a memory 12 for storing a system program of the mobile telephone, the time correction period, the standard time source contacts and the mobile phone 1 of the first setting time; a display unit 14 for displaying the system time of the mobile phone 1; central processor 13, and each of the unit is coupled to the control over the operation of the different units.

See Figure 2, the mobile phone 1 of the present invention, the automatic time correction method comprising the steps of:

Setting the mobile phone of the initial time, the time correction cycle, and the standard time source contact and time of the request, and such data is stored in a memory of the mobile phone 12, wherein the time correction period can be set to one week or one month, The standard time for the sound source can exercise stations, a query such as 114 Chinese mainland China Taiwan 104 repeater stations or station (step 100); mobile phone a central processor 13 determines whether the need for time correction, that is, from the initial set time Since, if after a set time correction cycle time, as otherwise continue to determine (step 101); For the time correction, that is, from the initial set time has been set time correction cycle time, the move The central processor 13 performs an automatic telephone contact function, reads the standard time source contacts from the memory 12, and automatically links, signal receiving / transmitting unit 10 transmit a request to the time the standard time source (step 102); standard time sent by the source of the mobile phone 1 requests the time information to the mobile phone 1 (step 103); time signal sampling unit 11 of the mobile phone 1 and the sampling time for

the signal stored to the memory 12 (step 104); a central processor 13 This time is set to the system time of the mobile phone 1 and displayed on (step 105) the display unit 14.

Preferably, when the standard time for the sound source exercise station, and the mobile phone 1 is equipped with a voice generating unit and a voice recognition unit, step 100 includes a pre-set time in the mobile phone 1 inquiry request, such as may be inquired time sound signal, step 102 includes the following steps: When a mobile phone call sound exercise stations, a mobile phone made by voice generating unit time inquiry request, and the corresponding step 103 includes the following steps: Time sound exercise station in turn request sent signal to the mobile telephone 1, the signal through the mobile phone voice generating unit 1 to issue, and the speech recognition unit of the mobile phone 1 and the sampling time for the signal stored to the memory 12.

Preferably, the standard time when the source is a mobile telephone service provider network, step 100 comprises a pre-set time in the mobile phone 1 inquiry request, such as SMS for inquiry time, step 102 includes the following steps: the mobile phone 1 read from the memory 12 times the standard source of contact information, and automatically links the signal receiver / transmitter unit 10 will ask for time to transmit messages to the mobile phone service provider network in, while the corresponding step 103 includes the following steps: mobile phone service providers network in order to send a text message to the mobile phone standard time a mobile phone signal sampling unit 11 hours a time signal sampling and storage to memory 12.

Compared with the prior art, the present invention is the use of a mobile phone outside the regular standard time source mobile phone system time is corrected, thereby periodically time error promptly eliminated so that even if the mobile phone is generally of a clock circuit using a quartz oscillator nor will cause inconvenience to the user, so the need to adopt a more expensive quartz oscillator or other fine-tuning capacitor, etc., it will not increase the cost of mobile phones, and nor will it interfere with the formation of the miniaturization of mobile phones.

CLASSIFICATIONS

International Classification	G04R20/00, H04M1/21, H04M1/00

LEGAL EVENTS

Date	Code	Event	Description
Nov 26, 2008	C02	Deemed withdrawal of patent application after publication (patent law 2001)	
Sep 6, 2006	C10	Request of examination as to substance	
Jul 12, 2006	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04M 17/00 (2006.01)
H04Q 7/22 (2006.01)
H04L 12/14 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510070958.9

[43] 公开日 2006 年 11 月 22 日

[11] 公开号 CN 1867024A

[22] 申请日 2005.5.19
[21] 申请号 200510070958.9
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 申 海 孙 谦

[74] 专利代理机构 北京同达信恒知识产权代理有限公司
代理人 郭润湘

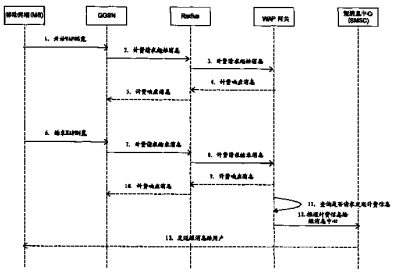
权利要求书 3 页 说明书 9 页 附图 2 页

[54] 发明名称

一种计费信息发送方法

[57] 摘要

本发明公开了一种计费信息发送方法，应用于无线应用协议(WAP)业务，该方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。本发明方法能实现由 WAP 网关将用户使用 WAP 业务的计费信息即时发送给用户终端，方便用户控制和使用 WAP 业务。



1、一种计费信息发送方法，应用于无线应用协议（WAP）业务，该方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。

2、如权利要求 1 所述的方法，其特征在于，在 WAP 网关中预先设置计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后 WAP 网关根据设置的计费信息发送方式发送计费信息给移动终端。

3、如权利要求 2 所述的方法，其特征在于，所述 WAP 网关中预先设置的计费信息发送方式与移动终端对应，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

4、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为短消息发送；WAP 网关通过 WAP 推送方式发送移动终端使用 WAP 业务的计费信息给短消息中心；短消息中心以短消息方式将所述计费信息下发给移动终端。

5、如权利要求 4 所述的方法，其特征在于，所述计费信息发送方式中还包括设定的时间间隔，在移动终端使用 WAP 业务过程中，WAP 网关按所述设定的时间间隔发送所述计费信息给短消息中心。

6、如权利要求 4 所述的方法，其特征在于，所述计费信息发送方式中还包括设定的余额阈值、流量阈值或费用阈值，在移动终端使用 WAP 业务过程中，当 WAP 网关检测到预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，WAP 网关发送计费信息给短消息中心。

7、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关为该

移动终端产生一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址以及超链接的显示文字插入到移动终端当前请求浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除所述临时 WAP 网页。

8、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成 WAP 网页返回给移动终端。

9、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：设定一个用于发送计费信息的固定超链接地址，当 WAP 网关检测到移动终端请求该固定超链接地址时将该移动终端的计费信息以 WAP 网页方式发送给移动终端。

10、如权利要求 9 所述的方法，其特征在于，所述固定超链接地址预置在所述移动终端中。

11、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 IP 数据包发送，WAP 网关接收到移动终端的计费信息请求或根据设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。

12、如权利要求 11 所述的方法，其特征在于，在移动终端 WAP 浏览器界面的固定位置显示所述计费信息。

13、如权利要求 1 所述的方法，其特征在于，当移动终端为预付费终端，还包括 WAP 网关在该移动终端请求 WAP 业务时，查询其预付费余额的步骤；若预付费余额不足，则 WAP 网关通知该移动终端，并拒绝其使用请求的 WAP 业务，否则移动终端正常使用 WAP 业务。

14、如权利要求 1 所述的方法，其特征在于，所述 WAP 业务为 WAP 浏览

类业务或 WAP 流媒体业务。

15、如权利要求 1 所述的方法，其特征在于，所述计费信息为移动终端本次使用 WAP 业务流量、累计使用 WAP 业务流量、本次使用 WAP 业务费用、累计使用 WAP 业务费用、本次业务使用时长、本次业务费率和预付费余额其中之一或任意多个的组合信息。

16、如权利要求 15 所述的方法，其特征在于，若 WAP 网关发送的计费信息包括累计使用 WAP 业务流量、累计使用 WAP 业务费用、本次业务费率或预付费余额中至少其中之一时，还包括 WAP 网关向数据业务管理平台发送请求消息，获取上述计费信息的步骤。

17、如权利要求 16 所述的方法，其特征在于，若数据业务管理平台没有保存相应请求的计费信息，则由数据业务管理平台到智能网的业务控制点（SCP）上获取。

一种计费信息发送方法

技术领域

本发明涉及无线通信领域，尤其涉及无线应用协议（Wireless Application Protocol，WAP）业务的计费信息发送方法。

背景技术

WAP技术目前已成为移动通信网络中终端访问无线信息服务的全球主要标准，也是实现现有移动数据及增值业务的技术基础。WAP浏览类业务是最普通和常用的移动数据业务，用户通过终端的浏览器查看从服务器收到的WAP网页信息，作为移动数据业务的一种基础业务，WAP浏览类业务正被越来越多的移动用户所使用并接受。另外基于WAP的移动流媒体业务，也将成为3G通信网络中的主流应用。开放移动联盟（Open Mobile Alliance，OMA）在WAP业务具体计费实现上并没有做出限定，而现有技术中也还没有一种将WAP业务计费信息即时传送给移动终端的方法。移动终端的计费信息只能在话费月结时由计费系统如BOSS对从WAP网关采集来的话单进行统计批价，然后打印出来提供给用户，而且通常还没有费用的明细记录。由于WAP网关很多情况都是按流量进行计费，这样对于预付费和后付费用户，都存在一个同样的问题：用户在使用WAP业务中或进行一次WAP业务后，不知道产生了多少流量，也不知道本月累计使用了多少流量，使得用户无法及时掌握或控制WAP业务的使用情况；特别是对于预付费用户，当预付费用用完时，在用户无法事先获知的情况下WAP网关会强行中断业务，给用户使用WAP业务造成困扰。

发明内容

本发明提供一种计费信息发送方法，用以解决现有技术中存在的 WAP 业

务不能即时提供计费信息的问题。

本发明方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。

根据本发明的上述方法，在 WAP 网关中预先设置计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后 WAP 网关根据设置的计费信息发送方式发送计费信息给移动终端。

所述 WAP 网关中预先设置的计费信息发送方式与移动终端对应，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

所述计费信息发送方式为短消息发送；WAP 网关通过 WAP 推送方式发送移动终端使用 WAP 业务的计费信息给短消息中心；短消息中心以短消息方式将所述计费信息下发给移动终端。

所述计费信息发送方式中还包括设定的时间间隔，在移动终端使用 WAP 业务过程中，WAP 网关按所述设定的时间间隔发送所述计费信息给短消息中心。

所述计费信息发送方式中还包括设定的余额阈值、流量阈值或费用阈值，在移动终端使用 WAP 业务过程中，当 WAP 网关检测到预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，WAP 网关发送计费信息给短消息中心。

所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关为该移动终端产生一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址以及超链接的显示文字插入到移动终端当前请求浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除所述临时 WAP 网页。

所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP

业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成 WAP 网页返回给移动终端。

所述计费信息发送方式为 WAP 网页；具体包括：设定一个用于发送计费信息的固定超链接地址，当 WAP 网关检测到移动终端请求该固定超链接地址时将该移动终端的计费信息以 WAP 网页方式发送给移动终端。

所述固定超链接地址预置在所述移动终端中。

所述计费信息发送方式为 IP 数据包发送，WAP 网关接收到移动终端的计费信息请求或根据设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。

在移动终端 WAP 浏览器界面的固定位置显示所述计费信息。

当移动终端为预付费终端，还包括 WAP 网关在该移动终端请求 WAP 业务时，查询其预付费余额的步骤；若预付费余额不足，则 WAP 网关通知该移动终端，并拒绝其使用请求的 WAP 业务，否则移动终端正常使用 WAP 业务。

所述 WAP 业务为 WAP 浏览类业务或 WAP 流媒体业务。

所述计费信息为移动终端本次使用 WAP 业务流量、累计使用 WAP 业务流量、本次使用 WAP 业务费用、累计使用 WAP 业务费用、本次业务使用时长、本次业务费率和预付费余额其中之一或任意多个的组合信息。

若 WAP 网关发送的计费信息包括累计使用 WAP 业务流量、累计使用 WAP 业务费用、本次业务费率或预付费余额中至少其中之一时，还包括 WAP 网关向数据业务管理平台发送请求消息，获取上述计费信息的步骤。

若数据业务管理平台没有保存相应请求的计费信息，则由数据业务管理平台到智能网的业务控制点（SCP）上获取。

本发明有益效果如下：

（1）本发明通过利用 WAP 网关向终端发送计费信息，实现了用户在使用 WAP 业务过程中或刚刚使用 WAP 业务完成后的时间内能够即时获取计费信

息，方便用户控制和使用 WAP 业务。

（2）本发明提供了多种计费信息发送方式的实现方案，包括：短消息方式、WAP 网页方式和 IP 数据包方式，WAP 网关可以根据网络状况和能力选择其中至少一种计费信息发送的实现方案将计费信息即时发送给用户终端；而对于同时提供了多种计费信息发送方式的 WAP 网关，用户也可以灵活设置计费信息发送方式，充分满足用户的个性化需求和使用习惯。

（3）本发明可以对需要 WAP 业务计费信息即时发送的用户预先进行登记，系统只对登记的用户按默认或设置的计费信息发送方式发送计费信息，在充分满足用户需求的同时，减少系统负荷。

附图说明

图 1 为计费信息下发所涉及的系统结构示意图；

图 2 为本发明实施例中 WAP 浏览业务计费过程及通过短消息下发计费信息的信令流程图；

图 3 为本发明实施例中 WAP 流媒体业务计费过程及通过短消息下发计费信息的信令流程图。

具体实施方式

本发明方法是由 WAP 网关在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后发送计费信息给移动终端。而 WAP 网关发送计费信息的方式可以是短消息，WAP 网页等，具体实施中可以在 WAP 网关中实现一种或同时实现多种计费信息发送方式。

对于不同的移动终端，通过预先在 WAP 网关存储对应的计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

在实际应用中，可以将计费信息发送作为一个新的 WAP 业务功能，由用

户进行登记。对于登记使用该业务功能的用户，在使用 WAP 业务过程中或业务结束后，WAP 网关采用该移动终端对应的计费信息发送方式发送计费信息给该移动终端，如果 WAP 网关不允许用户设置自己的计费信息发送方式或者用户没有设置自己的计费信息发送方式则 WAP 网关采用系统默认的计费信息发送方式发送计费信息给移动终端；对于没有登记该业务功能的用户，则可以不发送计费信息。

具体实施方法包括：在 WAP 网关的用户信息数据库中添加表明用户希望使用 WAP 计费信息即时发送标识（为描述方便，称之为第一标识），当用户申请 WAP 计费信息即时发送这项业务功能时，给该移动用户的第一标识赋值为“1”；否则，赋值为“0”表示该用户不使用 WAP 业务计费信息即时发送业务功能。同时，需要添加计费信息发送方式标识（为描述方便，称之为第二标识）；在第二标识中可以用不同的值代表不同的发送方式，如：“0”表示以短消息方式发送，“1”表示以 WAP 网页方式发送，“2”表示以 IP 数据包方式发送等；同种方式还可以衍生出多种子类型，如按时间间隔周期性发送，超过设定的流量阈值或费用阈值时发送等。还可以将其中一种发送方式作为系统默认的发送方式，如第二标识为“0”的短消息方式发送方式。

当移动用户请求 WAP 业务时，WAP 网关查询存储的用户信息数据库，若检测到该移动用户已申请 WAP 计费信息即时发送业务功能，则将其计费信息按照设置的发送方式发送给移动终端。

发送的计费信息包括至少下列之一：本次或累计流量，本次或累计费用，业务使用时长，业务费率，预付费余额等。WAP 网关一般只有当前流量信息，累计流量以及费率等需要从数据业务管理平台（DSMP）和业务控制点（SCP）上获取，如图 1 所示，WAP 网关向 DSMP 发送请求，如果 DSMP 上没有相应信息，则 DSMP 向 SCP 请求信息，获取业务相关的费率、预付费余额以及终端累计费用信息等，然后发送给移动终端。一般情况下，WAP 网关不直接与 SCP 相连，而是通过 DSMP 连接 SCP 获取计费信息。

若移动终端对应的计费信息发送方式为短消息发送，则 WAP 网关通过 WAP 推送方式发送计费信息给短消息中心；短消息中心以短消息方式将计费信息下发给移动终端。

如图 2 所示，为 WAP 浏览业务计费过程及通过短消息下发计费信息的信令流程图，包括如下流程：

1、移动用户通过移动终端发起 WAP 浏览；

2、网关 GPRS 支持节点（GGSN）为移动终端（MS）分配了 IP 地址后向远程身份验证拨入用户服务（RADIUS）服务器发送计费请求起始消息，在该消息中包含分配给 MS 的 IP 地址和手机号码；

3、RADIUS 服务器向 WAP 网关转发计费请求起始消息；

4、WAP 网关收到计费请求起始消息后，向 RADIUS 服务器发送计费响应消息；

5、RADIUS 服务器收到计费响应消息后转发给 GGSN，若 GGSN 未收到计费响应消息，应向 RADIUS 服务器重新发送计费请求起始消息；

6、移动用户结束此次 WAP 浏览；

7、GGSN 向 RADIUS 服务器发送计费请求结束消息；

8、RADIUS 服务器向 WAP 网关转发计费请求结束消息；

9、WAP 网关收到计费请求结束消息后，向 RADIUS 服务器发送计费响应消息；

10、RADIUS 服务器收到计费响应消息后转发给 GGSN，若 GGSN 未收到计费响应消息，应重新发送计费请求结束消息；

11、WAP 网关发送计费响应后，判断该移动用户的第一标识，如果第一标识为“0”，则结束；如果第一标识为“1”，且第二标识为通过短消息方式发送计费信息，则执行步骤 12；

12、WAP 网关通过推送代理网关（Push Proxy GateWay，PPG）向短消息中心（SMSC）推送用户本次使用流量（费用）以及累计流量（费用）等信息；

13、SMSC 以短消息方式将接收的计费信息发送到移动终端上。

图 3 为 WAP 流媒体业务计费过程及通过短消息下发计费信息的信令流程图。WAP 网关收到 MS 发出的访问请求后，对访问请求的统一定位资源（URL）进行解析，判断为流媒体业务后将相关业务的提供商标识信息（SPID）、业务标识信息（ServiceID）以及用户的 IP 地址等与计费相关的信息上报给 DSMP 进行业务鉴权批价。流媒体业务计费同时支持预付费用户和后付费用户。对于预付费用户，DSMP 通过与 SCP 的交互完成实时扣费。具体信令交互流程如图 3 所示，包括:

1、MS 向 WAP 网关发起流媒体业务访问请求。

2、WAP 网关收到访问请求后，判断是否对用户请求进行转发，如果满足转发条件，则继续处理；否则，拒绝此次访问请求。

在该步骤中，是否对用户的业务请求进行前转或拒绝，是根据系统数据库中的一个“转发控制表”来执行的，该表存储有不可访问某项业务的 MS 的 IP 地址或终端号码，比如，在用户欠费或余额不足的情况下，将对其禁用某些类型的业务请求；当 MS 请求业务时，WAP 网关将查找“转发控制表”，如果发送业务请求的 MS 包含在“转发控制表”中，则确定所请求此项业务是否为不可访问业务，如果是，则对此 MS 禁用该项业务，并将用户的欠费信息发送给 MS；如果发送业务请求的 MS 不在转发控制表中，则说明此 MS 是合法的，WAP 网关则将该请求透传给业务提供商（SP），并进行内容计费或流量计费，在业务使用过程中或使用后将计费信息发给 MS。为了防止用户在已经充值的情况下，仍然无法使用某项业务，转发控制表中的用户信息是实时更新的。

3、WAP 网关将业务请求转发给相应的业务提供商或内容提供商（SP/CP）。

4、SP/CP 返回访问请求应答消息给 WAP 网关。

5、WAP 网关把请求应答消息下发给终端 MS。

6、WAP 网关记录或查询用户在线信息，并判断用户类型（根据 MSISDN 号段或 IMSI 号段区分用户类型，如预付费用户、后付费用户），如果是后付费

用户，业务使用结束后直接跳转到第 11 步；如果是预付费用户，根据请求的 URL 采集 SPID、ServiceID 以及用户 IP 地址等计费相关信息。

7、WAP 网关将采集到的计费相关信息上报 DSMP，进行鉴权批价。

8、DSMP 到 SCP 申请费用预扣。

9、SCP 向 DSMP 返回费用预扣应答消息。

10、DSMP 向 WAP 网关返回鉴权批价应答消息。

11、MS 向 WAP 网关发出断连请求。

12、WAP 网关把断连请求转发给 SP/CP。

13、SP/CP 向 WAP 网关返回断连请求应答消息。

14、WAP 网关把断连请求应答消息下发给终端 MS。

15、WAP 网关生成话单记录（Call Detail Record ，CDR），包括业务开始时间，结束时间，终端号码，业务类型等。

16、WAP 网关将 CDR 话单中的计费信息通过 WAP PUSH 短消息发给 MS。

以上用 WAP 浏览业务和流媒体业务的计费过程为例，对本发明采用短消息方式发送 WAP 业务计费信息进行了详细描述。其中，短消息发送方式可以是在移动终端使用 WAP 业务过程中，由 WAP 网关按设定的时间间隔发送；或在移动终端使用 WAP 业务过程中，当预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，在 WAP 浏览业务的第 5 步与第 6 步之间或在 WAP 流媒体业务的第 10 步与第 11 步之间，由 WAP 网关发送计费信息给短消息中心。另外对于流媒体业务与浏览业务同时使用的情形，如 WAP 浏览时打开了一个流媒体，这样 WAP 网关同时将两个业务的计费信息分别或合并在一起发送给 MS。

对于计费信息的发送，除了采用短消息方式发送外，还可以采用 WAP 网页方式发送，包括下列具体方法：

方法一：在移动终端使用 WAP 业务过程中，WAP 网关为该移动终端产生

一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址插入到移动终端当前浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除产生的临时 WAP 网页。

方法二：在移动终端使用 WAP 业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成包含计费信息的 WAP 网页由 WAP 网关返回给移动终端。

方法三：将移动终端使用 WAP 业务的计费信息存储到一个固定超链接地址的 WAP 网页中，当移动终端访问该固定超链接地址时，WAP 网关获取相应的计费信息并更新到上述 WAP 网页然后返回给移动终端。为用户使用方便，可以将上述固定超链接地址预先存储到移动终端中，用户可以随时通过访问该超链接地址获取计费信息。

计费信息发送方式还可以为 IP 数据包发送，可以设置为当 WAP 网关接收到移动终端的计费信息请求时，将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，或 WAP 网关按照设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。同时改进 WAP 浏览器，使之在终端浏览器界面的固定位置显示 WAP 网关发送的计费信息（流量或费用信息）。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

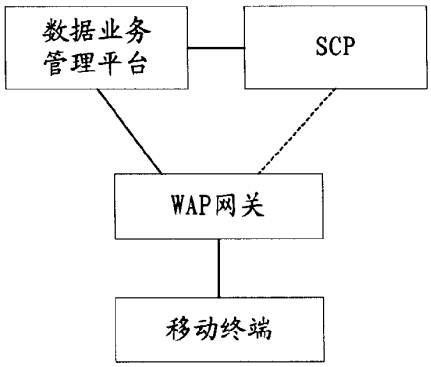

数据业务
管理平台
SCP
WAP网关
移动终端

图 1

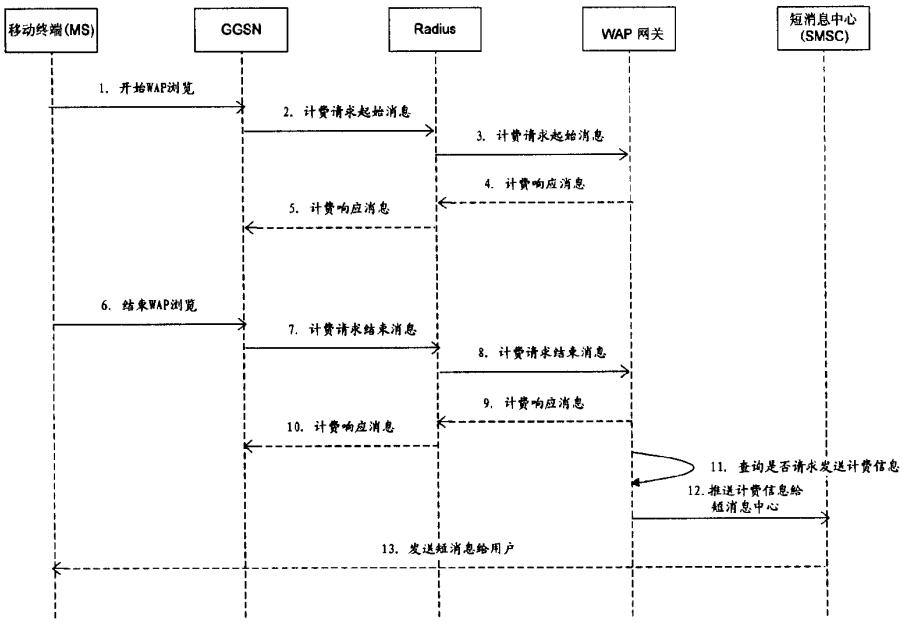

移动终端(MS)
GGSN
Radius
WAP 网关
短消息中心
(SMSC)
1. 开始WAP浏览
2. 计费请求起始消息
3. 计费请求起始消息
4. 计费响应消息
5. 计费响应消息
6. 结束WAP浏览
7. 计费请求结束消息
8. 计费请求结束消息
9. 计费响应消息
10. 计费响应消息
11. 查询是否请求发送计费信息
12. 推送计费信息给
短消息中心
13. 发送短消息给用户

图 2

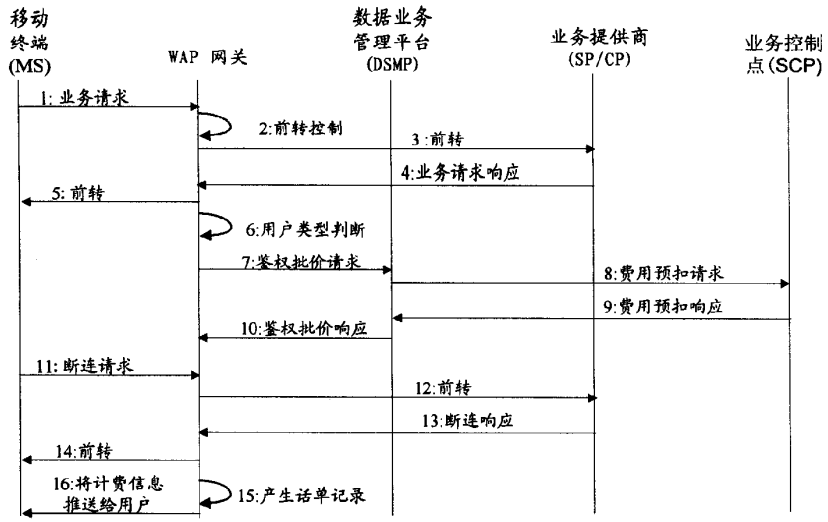

移动
终端
(MS)
WAP 网关
数据业务
管理平台
(DSMP)
业务提供商
(SP/CP)
业务控制
点(SCP)
1: 业务请求
2:前转控制
3 :前转
4:业务请求响应
5: 前转
6:用户类型判断
7:鉴权批价请求
8:费用预扣请求
9:费用预扣响应
10:鉴权批价响应
11: 断连请求
12:前转
13:断连响应
14:前转
16:将计费信息
推送给用户
15:产生话单记录

图 3

Sign in

Patents Application Grant English Chinese

Find prior art Discuss this application View PDF Download PDF

Charging information transmitting method

CN 1867024 A

Publication number	CN1867024 A
Publication type	Application
Application number	CN 200510070958
Publication date	22 Nov 2006
Filing date	19 May 2005
Priority date	19 May 2005
Also published as	CN1867024B
Inventors	申商, 孙豫
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (6), Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention relates to a charge information sending method, used in wireless application protocol (WAP) service, which comprises: the mobile terminal via WAP gateway uses WAP service; the WAP gateway charges the mobile terminal and sends the charge information to the mobile terminal. The invention can make the WAP gateway instantly send the charge information of consumed WAP service to the user terminal, to support the control and application of WAP service.

DESCRIPTION translated from Chinese

An information transmission method accounting

FIELD

The present invention relates to the field of wireless communications, and more particularly to a wireless application protocol (Wireless ApplicationProtocol, WAP) service charging information transmission method.

BACKGROUND

WAP technology has become a major global standard for mobile communications network terminal access wireless information services, as well as the technical foundation of existing mobile data and value-added services. WAP browser is the most common class of business and popular mobile data services, the user terminal via a browser to view WAP pages of information received from the server, as a basis for business mobile data services, WAP browsing class of business is being more and more Mobile users are using and accepted. Also WAP-based mobile streaming media business, will become the mainstream of 3G communication network applications. Open Mobile Alliance (Open Mobile Alliance, OMA) on WAP service specific implementation does not make a limited charging, while the prior art has not yet a WAP service billing information to a method for real time transmission to the mobile terminal. Billing information of the mobile terminal only when such calls monthly billing system by BOSS collected from the WAP gateway to the words of a single statistical rating, then print it out to users, but usually no expense detail records. Many cases are due to a WAP gateway billing by traffic, so for prepaid and postpaid users, there is a similar problem: the user in the use of WAP services, or conduct a WAP service, I do not know how much traffic generated, but also I do not know how much traffic this month cumulative use, so users can not grasp or control the use of WAP services; especially for prepaid subscribers, prepaid expenses when exhausted, in case the user can not be informed in advance of the WAP gateway will be forced to interrupt business users to use WAP services to cause trouble.

SUMMARY

The present invention provides a method for transmitting charging information to solve the prior art are not readily available WAP service charging information problems.

CLAIMS (17) translated from Chinese

A charging information transmission method, applied to a wireless application protocol (WAP) service, the method comprising: a mobile terminal using WAP services via the WAP gateway, WAP gateway of the mobile terminal for billing, WAP gateway sends accounting information to the mobile terminal.

2. The method according to claim 1, characterized in that the WAP gateway is preset in the charging information transmission method, in a mobile terminal using the WAP services used during or after the WAP gateway WAP service charging information according to the transmission setting Billing information is sent to the mobile terminal.

3. The method according to claim 2, characterized in that the charging information transmission method with the mobile terminal of the WAP gateway preset correspondence, using WAP service in a mobile terminal during or after completion of the WAP gateway WAP services using accounting information corresponding to the mobile terminal sending to send accounting information to the mobile terminal.

4. A method as claimed in claim 2 or claim 3, characterized in that the charging information transmission method for transmitting a short message, WAP gateway sends the mobile terminal using the WAP service charging information via WAP push mode to the short message center; SMS short message center to the next billing information to the mobile terminal.

5. The method according to claim 4, characterized in that the charging information transmission mode further includes setting the time interval, the mobile terminal using WAP in the course of business, WAP gateway according to the set time intervals sending the accounting information to the short message center.

6. The method of claim 4 when the WAP gateway detection claim, characterized in that the charging information transmission mode further includes setting a threshold value of the balance, the flow rate threshold or cost threshold, the mobile terminal using WAP in the course of business, When the prepaid balance of the mobile terminal is less than a set threshold balance value, the mobile terminal uses the mobile terminal traffic threshold or WAP traffic exceeds the costs of the use of WAP services cost more than the set threshold value, WAP

The method of the present invention includes: a mobile terminal via WAP gateway using WAP services, WAP gateway for mobile terminals for billing, WAP gateway sends billing information to the mobile terminal.

The above-described method according to the invention, the WAP gateway preset charging information transmission method, the business process using WAP or WAP gateway used to send accounting information to the accounting information based on the transmission method set by the mobile terminal after the WAP service in a mobile terminal .

Billing information transmitting manner with the WAP gateway of the mobile terminal set in advance corresponding to, in a mobile terminal using the WAP services used during or after completion of WAP gateway WAP services using the mobile terminal corresponding to the charging information sending to send accounting information to the mobile terminal.

The charging information transmission method for sending short messages; WAP gateway sends the mobile terminal using the WAP service billing information via WAP push mode to the short message center; short message center to a mobile short message will be sent to the billing information under terminal.

Information transmission mode further includes setting the charging time interval, using the WAP service in a mobile terminal during, WAP gateway according to the preset time interval to transmit the accounting information to the short message center.

The billing information transmitting mode further includes setting a threshold value of the balance, the flow rate threshold or cost threshold, the mobile terminal using WAP in the course of business, when the WAP gateway detects that the mobile terminal prepaid balance is less than the set threshold balance, moving When the end-use flow threshold or WAP mobile terminal traffic exceeds the cost of using WAP services exceeds the cost threshold, WAP gateway sends billing information to the short message center.

The charging information transmission method for WAP pages; including: the mobile terminal business processes using WAP, WAP gateway WAP page that contains the provisional billing information for the mobile terminal, and the temporary WAP page hyperlink address and display text hyperlinks inserted in the mobile terminal is currently viewed page request, the mobile terminal acquires the billing information by accessing the hyperlink address; and after the WAP service, deleting the temporary WAP page.

The charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP business process, WAP gateway will point to an immediate hyperlink accounting unit is inserted into the mobile terminal is currently viewed page request, the mobile terminal accesses when said hyperlink, immediate accounting unit receives charging information of the mobile terminal from the WAP gateway, and generates WAP pages returned to the mobile terminal.

The charging information transmission method as WAP pages; specifically includes: setting a fixed address hyperlink for transmitting the charging information, when the WAP gateway detects that the mobile terminal requests the fixed address of the mobile terminal hyperlink billing Information sent to the WAP pages to the mobile terminal.

Said fixed hyperlink address preset in the mobile terminal.

The charging information transmission method for transmitting IP packets, WAP gateway receives the charging information to the mobile terminal or a request intervals containing charging information according to the set time of the data packet transmitted to the mobile terminal corresponding to the IP protocol in accordance with the format of IP address, the mobile terminal displays the charging information.

gateway sends accounting information to the short message center.

7. The method according to claim 2 or claim 3, characterized in that the charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP business process, WAP gateway generates a count for the mobile terminal comprising Temporary fee WAP pages of information, and the temporary WAP page hyperlink address and hyperlink display text is inserted into the mobile terminal is currently viewed page request, the mobile terminal to obtain billing information by accessing the hyperlink address; and After the WAP service, delete the temporary WAP pages.

8. The method according to claim 2 or claim 3, characterized in that the charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP service process, WAP gateway will point to a real-time accounting unit hyperlink into the mobile terminal is currently viewed web page request, the mobile terminal to access the hyperlink, the accounting unit immediately obtain charge information of the mobile terminal from the WAP gateway, and generates WAP pages returned to the mobile terminal.

When the WAP gateway detection setting a fixed hyperlink address for sending billing information: including; 9. The method of claim 2 or claim 3, wherein the charging information transmission method for WAP pages to the mobile terminal requests the address of the hyperlink fixed charge information to the mobile terminal WAP page sent to the mobile terminal.

10. The method according to claim 9, characterized in that the fixed hyperlink address preset in the mobile terminal.

11. The method according to claim 2 or claim 3, characterized in that the charging information transmission method for transmitting IP packets, WAP gateway receives the charging information to the mobile terminal according to a request or set time interval will contain packet transmission according to the charging information to the mobile terminal IP protocol format corresponding to the IP address, the mobile terminal displays the charging information.

12. The method according to claim 11, characterized in that the charging information is displayed in a fixed position of the mobile terminal WAP browser interface.

13. The method of claim 1, wherein, when the mobile terminal is a prepaid terminal, further comprising the WAP gateway when the mobile terminal requests the WAP service, its pre-paid balance inquiry step; if insufficient pre-paid balance, the WAP gateway informs the mobile terminal, and reject the use of WAP service request, otherwise normal use of WAP mobile terminal business.

14. A method as claimed in claim 1, characterized in that the WAP service for WAP browsing WAP class of business or streaming media services.

15. A method as claimed in claim 1, characterized in that the billing information for mobile terminal using WAP traffic in this, the cumulative use of WAP traffic, this time using WAP operating expenses, total operating expenses using WAP, this When using a long time business, this business combination and prepaid tariff information which one or any number of balance.

16. The right to at least one of the times when business rates or prepaid balance method of claim 15, wherein if the WAP gateway sends billing information, including cumulative use WAP traffic, total

In the fixed position of the mobile terminal WAP browser interface displays the charging information.

When the mobile terminal for prepaid terminals, including WAP gateway when the mobile terminal requests WAP services, check their prepaid balance steps; pre-paid balance if less, the WAP gateway informs the mobile terminal, and reject the use of the requested WAP business, otherwise normal use of WAP mobile terminal business.

The WAP service for WAP Browser WAP class of business or streaming media services.

operating expenses using WAP, further comprising a WAP gateway to the data service management platform sends a request message, the charge information acquisition step.

17. The method of claim 16, wherein, if the data service management platform does not save the corresponding charging information requested by the data service management platform to a service control point (SCP) of the intelligent network on the acquisition.

The charging information for the mobile terminal using WAP traffic in this, the cumulative use of WAP traffic, this time using WAP operating expenses, total operating expenses using WAP, use a long time in this business, this business rates and pre-paid balance among One or a combination of any number of information.

If the WAP gateway sends billing information, including cumulative use WAP traffic, the cumulative cost of using WAP services, at least one of the times when business rates or pre-paid balance, which also includes a WAP gateway to the data service management platform sends a request message to get said step of charging information.

If the data is not saved billing service management platform information corresponding request by the data service management platform to the service control point (SCP) on the acquisition of the intelligent network.

Beneficial effects of the present invention is as follows: (1) The present invention utilizing WAP gateway sends billing information to the terminals, the user in the course of business using WAP or just use the time after the completion of WAP services can instantly obtain billing information, user-friendly control and use WAP services.

(2) The present invention provides a variety of billing information transmission method implementations, including: short message, WAP page mode and IP packet mode, WAP gateway can select at least one of the charging information is sent according to the network status and the ability realization of the program will immediately send the charging information to the user terminal; and for a variety of billing information while providing a way to send a WAP gateway, users can flexibly set billing information transmission mode, fully meet the user's individual needs and habits .

(3) The present invention may require the user to send instant WAP service billing information pre-registration, the system only to registered users by default or set of accounting information send send billing information, while fully meet user demand, reduce system load.

Brief Description

Figure 1 is a schematic structural view of the system under the charging information issued involved; Fig. 2 embodiment of the present invention, WAP browse service billing process and the short message sent by a flowchart of charging information at a signaling; Figure 3 embodiment of the present invention example WAP streaming service billing process and issued the flow chart via SMS billing information signaling.

DETAILED DESCRIPTION

The method of the present invention is a mobile terminal using the WAP gateway WAP in the course of business or accounting information sent to the mobile terminal after the end of the use of WAP services. The WAP gateway sends billing information can be a way SMS, WAP pages, the specific implementation can be achieved in a WAP gateway or billing information is sent simultaneously to achieve a variety ways.

For different mobile terminal via the WAP gateway is stored in advance in the charging information corresponding to the transmission method, in a mobile terminal during use or after use WAP services complete WAP gateway WAP services using the mobile terminal corresponding to the charging information sending to send accounting information to the mobile terminal.

In practice, the charging information may be sent as a new WAP service function registration by the user. For registered users to use the business functions, after or during the use of the WAP service end of the business, WAP gateway uses the mobile terminal corresponding billing information send billing information is sent to the mobile terminal, if the WAP gateway does not allow users to set their own billing information is sent way or you do not set your own way billing information is sent using the default WAP gateway sends billing information send billing information to the mobile terminal; for there is no registration of the business functions of the user, you can not send billing information.

DETAILED DESCRIPTION The method comprises: a WAP gateway in the user information database indicates that the user wishes to add in a WAP charging information sent immediately identified (for convenience of description, referred to the first identification), when the user applies the charging information immediately send the WAP service When the function assigned to the first identification of the mobile subscriber is "1"; otherwise, the value "0" indicates that the user

does not immediately send a service function using the WAP service billing information. Meanwhile, the need to add the accounting information identifies the transmission mode (for convenience of description, referred to the second identification); in the second identification can be different values represent different transmission methods, such as: "0" indicates that a short message sent "1" means to send WAP pages, "2" to send IP packets, etc; the same way many seeds can also be derived types, such as by sending periodic intervals, the flow exceeds the set threshold value or cost of When the threshold is sent and the like. Wherein a further short message transmission mode as the default transmission mode, such as the second identifier is "0" may be input mode.

When the mobile user requests a WAP service, the WAP gateway queries the user information database stored, if it is detected that the mobile user has applied charging information sent immediately WAP service function, it is the accounting information sent to the mobile terminal according to the transmission mode set.

Billing information sent includes at least one of the following: The total flow or that this or cumulative cost, long-time business use, business rates, and other pre-paid balance. WAP gateway generally only current traffic information, as well as cumulative flow rate, etc. need to obtain from the data service management platform (DSMP) and a service control point (SCP), as shown in Figure 1, WAP gateway sends a request to DSMP, if on no DSMP appropriate information, then DSMP to SCP request information, access to business-related rates, pre-paid balance and terminal cumulative cost information, and then sent to the mobile terminal. Generally, WAP gateway not directly connected with the SCP, but is connected SCP receives charging information DSMP.

If the mobile terminal corresponding to the charging information transmission method for sending short messages, the WAP gateway sends billing information via WAP push mode to the short message center; short message center to short message will be sent to the mobile terminal next billing information.

2, the billing process for the WAP browsing service by sending the next charging information and a signaling message flow diagram, comprises the following processes: 1, the mobile terminal through the mobile user initiates a WAP browser; 2, Gateway GPRS Support Node (After GGSN) for the mobile terminal (MS) is assigned an IP address to the Remote Authentication Dial-In User Service (RADIUS) server sends an accounting request start message containing the IP address assigned to the MS, and phone number in the message; 3, RADIUS server forwards the request to start charging WAP gateway message; 4, WAP gateway billing request after receiving the initial message, send a response message to the RADIUS accounting server; 5, RADIUS server receives the forwarded after charging response message to the GGSN If the GGSN charging response message is not received, the RADIUS server should start charging request to resend the message; 6, the end of the WAP mobile users browse; 7, GGSN sends an accounting request to the RADIUS server end of the message; 8, RADIUS WAP billing gateway server forwards the request to the end of the message; 9, WAP gateway charging request received after the end of the message, send a response message to the RADIUS accounting server; 10, RADIUS server receives forwarded to the GGSN after charging response message, if the GGSN charging response message is not received, the end should resend the charging request message; 11, WAP gateway after sending charging response, determines the first identification of the mobile user, if the first identifier is "0", the end; if the first one identified as "1", and the second is identified as sending billing information via short message, proceed to Step 12; 12, WAP Push Proxy Gateway gateway (Push Proxy GateWay, PPG) to the Short Message Service Center (SMSC) to push users The use of flow (expense) and total flow (expense) and other information;

13, SMSC to send billing information received short message to the mobile terminal.

Figure 3 WAP streaming service billing process and issued the flow chart via SMS billing information signaling. After the WAP gateway receives an access request issued by MS, unified resource location (URL) access request is parsed to determine the identification information for the provider of streaming media services-related business will (SPID), business identification information (ServiceID) and user The IP address and billing-related information reported to the grant price DSMP authorization to conduct business. Streaming service billing support prepaid and postpaid users users. For prepaid subscribers, DSMP through real-time interaction with the completion of the SCP deductions. Specific signaling interaction process shown in Figure 3, including: 1, MS initiates streaming service access request to the WAP gateway.

2, after the WAP gateway receives an access request to determine whether the request is forwarded to the user, if the forwarding condition, then continue processing; otherwise, reject the access request.

In this step, the front of the user's service request is transposed or rejected based on the system database in a "forwarding control table" to be executed, the table stores a business of MS is not accessible IP address or a station number , for example, in the user arrears or insufficient balance situation, which will be disable certain types of service requests; "Forward Control Table" When MS requests a service, WAP gateway will find, MS If you send a service request is contained in " forwarding control table ", it is determined whether the requested service is inaccessible to this service, if yes, the service is disabled for this MS, and the information is sent to the user arrears MS; if the MS is not transmitting a service request forwarding control table, the description for this MS is legitimate, WAP gateway through the request is passed to the service provider (SP), and content-based billing or traffic accounting, business use during or after the use of accounting information sent to MS. To prevent the user has to recharge the case is still unable to use certain services,

forwarding control table user information is updated in real time.

3, WAP gateway service request will be forwarded to the appropriate service provider or content provider (SP / CP).

4, SP / CP returns an access request response message to the WAP gateway.

5, WAP gateway to request a response message to the terminal MS under.

6, WAP gateway records or query the user online information, and determine the type of user (based on MSISDN or IMSI number section number section all types of users, such as pre-paid subscribers, post-paid subscribers), if it is post-paid users to jump directly after the end of the business use Go to Step 11; if it is a pre-paid subscribers, collecting SPID, ServiceID as well as the user's IP address and other billing related information according to the requested URL.

7, WAP gateway will be collected charging related information reporting DSMP, authenticate the grant price.

8, DSMP to SCP application fee withholding.

9, SCP DSMP return costs to withhold a response message.

10, DSMP grant price return authorization response message to the WAP gateway.

11, MS issued a disconnection request to the WAP gateway.

12, WAP gateway forwards the request to put off even the SP / CP.

13, SP / CP returns to the WAP gateway disconnection request response message.

14, WAP gateway to the disconnection request response message to the terminal under MS.

15, WAP gateway CDR record generation (Call Detail Record, CDR), including business start time, end time, terminal number, type of service.

16, WAP gateway bill in the CDR billing information to the MS via WAP PUSH short message.

WAP browser with more services and streaming services billing process, for example, the present invention uses the short message sent WAP service billing information described in detail. Wherein, the short message transmission mode in the mobile terminal may be a business process using the WAP, the WAP gateway send at set time intervals; or in the mobile terminal using the WAP service process, when the prepaid balance of the mobile terminal is less than the set balance threshold, the mobile terminal using flow threshold or mobile terminal WAP traffic exceeds the use of WAP service fee exceeds the cost threshold between Step 5 WAP browsing services with step 6 or WAP streaming media business section 10 steps between step 11 and sent by the WAP gateway billing information to the short message center. In addition to the case of streaming services and browse business use, such as the WAP browser to open a streaming media, such WAP gateway billing information while the two businesses separately or combined to the MS.

For sending billing information, in addition to the short message sent, but also can be sent using WAP pages, including the following specific methods: Method One: In the mobile terminal business process using WAP, WAP gateway generates a count for the mobile terminal contains Temporary fee WAP pages of information, and the temporary WAP page hyperlink address into the mobile terminal while browsing the mobile terminal to obtain billing information by accessing the hyperlink address; and after the WAP service, delete produce Temporary WAP pages.

Method 2: In the mobile terminal business process using WAP, WAP gateway will instantly hyperlink pointing to a billing unit is inserted into the mobile terminal is currently viewed web page request, the mobile terminal to access the hyperlink, instant charging unit from WAP gateway acquires accounting information of the mobile terminal, and generates charging information WAP page containing the return by the WAP gateway to the mobile terminal.

Method three: the mobile terminal using the WAP service billing information is stored to a fixed address hyperlink WAP pages, when the mobile terminal to access the fixed hyperlink addresses, WAP gateway obtains the corresponding charging information and updates to said WAP page then returned to the mobile terminal. The user easy to use, can be a hyperlink to the fixed address previously stored in the mobile terminal, the user can obtain billing information at any time by visiting the hyperlink address.

Accounting information packet transmission method can also transmit IP packets, may be provided to the WAP gateway when the mobile terminal receives the request for charging information, the charging information contains the mobile terminal transmits the corresponding IP address according to the IP protocol format , or a WAP gateway according to the set time interval will contain data packets transmitted to the accounting information corresponding to the IP address of the mobile terminal according to IP protocol format, the mobile terminal displays the charging information. While improving the WAP browser that displays the charging information (traffic or cost information) WAP gateway sends the location of the terminal in a fixed browser interface.

Obviously, those skilled in the art may make various modifications of the present invention and modifications without departing from the spirit and scope of the invention. Thus, if such modifications and variations of the present invention and the claims of the invention belongs to the technical scope of equivalents, the present invention is also intended to include these changes and modifications included.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100450130C	21 Dec 2005	7 Jan 2009	中兴通讯股份有限公司	System and method for realizing intermediately informing user telephone fee
CN101286858B	12 Apr 2007	8 Dec 2010	中兴通讯股份有限公司	Method and system for charging of WAP gateway for mobile terminal
CN101287161B	14 May 2008	20 Apr 2011	华为软件技术有限公司	Service request forwarding method, gateway for wireless application protocol and communication system
CN101583095B	3 Jun 2009	8 May 2013	中兴通讯股份有限公司	Telephone charge prewarning method and prewarning system
CN101674561B	15 Jan 2009	4 Jul 2012	华为技术有限公司	Subscriber arrearage treatment method, device and system
WO2010028556A1 *	10 Jul 2009	18 Mar 2010	Huawei Technologies Co., Ltd.	Method for processing user debt, mobile management entity and network system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04Q7/22, H04L12/14, H04M17/00

LEGAL EVENTS

Date	Code	Event	Description
6 Oct 2010	C14	Granted	
17 Jan 2007	C10	Request of examination as to substance	
22 Nov 2006	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101815275 A
(43)申请公布日 2010.08.25

(21)申请号 201010143134.0

(22)申请日 2010.04.09

(71)申请人 刘泱
地址 100190 北京市海淀区知春路 63 号卫星大厦 6 层 604 单元

(72)发明人 梁秋实 袁彬

(74)专利代理机构 北京联创佳为专利事务所（普通合伙） 11362
代理人 郭防

(51)Int.Cl.
H04W 4/24(2009.01)
H04W 88/02(2009.01)

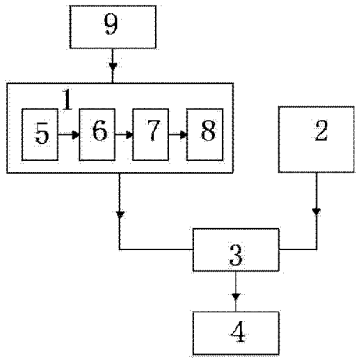
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

一种手机话费计算装置

(57)摘要

本发明公开了一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器(9)和手机；还包括设置在手机上的同步用户的话费计费规则到手机的网络同步模块(1)，记录用户通话详情的监控模块(2)，使用网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价的批价模块(3)和将批价后的账单存储在手机上的存储模块(4)。本发明计算话费时的实时性和准确性高，并且可直接在手机上查询，话费详单数据量小，无需密码，更加方便快捷，同时存储的账单也便于用户对话费的核对。



CN 101815275 A

1. 一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器(9)和手机；还包括设置在手机上的

网络同步模块(1)，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器(9)相连；

监控模块(2)，用于记录用户通话详情；

批价模块(3)，用于将网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价；

存储模块(4)，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块(2)和网络同步模块(1)与批价模块(3)相连，批价模块(3)与存储模块(4)相连。

2. 根据权利要求1所述的手机话费计算装置，其特征在于：所述网络同步模块(1)包括获取手机的运营商、归属地和品牌信息的用户信息模块(5)，根据获取的用户信息从业务支撑服务器(9)下载运营商该品牌下所有的套餐列表的列表下载模块(6)、用于用户选择所用套餐的选择模块(7)和根据用户所选套餐从业务支撑服务器(9)获取该套餐计费规则的规则下载模块(8)。

3. 根据权利要求2所述的手机话费计算装置，其特征在于：所述用户信息模块(5)为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

4. 根据权利要求2所述的手机话费计算装置，其特征在于：所述用户信息模块(5)为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

5. 根据权利要求4所述的手机话费计算装置，其特征在于：所述短信中心号与运营商、省份的对应关系从业务支撑服务器(9)下载，或预先存储在手机上。

6. 根据权利要求2所述的手机话费计算装置，其特征在于：所述规则下载模块(8)下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS上网费用计费规则、月租费、套餐费和手机号段。

7. 根据权利要求1所述的手机话费计算装置，其特征在于：所述监控模块(2)在手机端监控用户的通话、发送短信、通过GPRS联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

8. 根据权利要求7所述的手机话费计算装置，其特征在于：所述通话详情包括用户的通话、发送短信和通过GPRS联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

9. 根据权利要求1、2或5所述的手机话费计算装置，其特征在于：所述业务支撑服务器(9)是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

一种手机话费计算装置

技术领域

[0001] 本发明涉及一种手机话费计算装置，特别是一种手机上使用的手机话费计算装置。

背景技术

[0002] 一个典型的电信运营商所使用的计费系统中，业务网元是电信运营商提供基础服务的系统，电信的核心服务包括通话、短信、GPRS(GeneralPacketRadioService)等，每个服务对应一组业务网元。CDR(calldetailrecord)是业务详情记录，记录业务网元向用户提供的每次服务的详情。CDR40不仅仅指通话详情记录，也包括短信或GPRS的使用详情记录。每条CDR中包含发话时间、结束时间、主叫、被叫、发话地点等信息。系统向业务网元查询CDR40，然后对CDR40批价，得到账单详情，并将账单详情存入账单数据库。

[0003] 而现有的话费计算系统存在下述问题：

首先，现有的话费计算系统是在各电信运营商内部运作，且因为一些技术原因容易出现话费错算、误算的情况，手机用户很难清楚的了解自己每笔话费的产生原因，进而无法确定自己话费的准确性、正确性。

[0004] 其次，因为话单的数量巨大，一些电信运营商并不对全部用户提供话费详单查询服务。即便某些电信运营商对于部分用户开放了详单查询的业务，也存在使用不便(比如要输入服务密码、或者到移动营业厅现场办理)、实时性不强(比如只能查上月的话费详单、或几天前的话费详单)等问题。

[0005] 再次，即便用户拿到了话费详单，也会因为各运营商、各种套餐的计算规则各异，如存在优惠时段、赠送通话分钟数等特殊规则，导致用户对话费的核对非常困难。

发明内容

[0006] 本发明的目的在于，提供一种手机话费计算装置。它是一种便于用户查看和理解，具有高实时性、准确性的手机话费计算装置。

[0007] 本发明的技术方案：一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器和手机；还包括设置在手机上的

网络同步模块，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器相连；

监控模块，用于记录用户通话详情；

批价模块，用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价；

存储模块，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块和网络同步模块与批价模块相连，批价模块与存储模块相连。

[0008] 上述的手机话费计算装置中，所述网络同步模块包括获取手机的运营商、归属地

和品牌信息的用户信息模块，根据获取的用户信息从业务支撑服务器下载运营商该品牌下所有的套餐列表的列表下载模块、用于用户选择所用套餐的选择模块和根据用户所选套餐从业务支撑服务器获取该套餐计费规则的规则下载模块。

[0009] 前述的手机话费计算装置中，所述用户信息模块为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0010] 前述的手机话费计算装置中，所述用户信息模块为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

[0011] 前述的手机话费计算装置中，所述短信中心号与运营商、省份的对应关系从业务支撑服务器下载，或预先存储在手机上。

[0012] 前述的手机话费计算装置中，所述规则下载模块下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS 上网费用计费规则、月租费、套餐费和手机号段。

[0013] 前述的手机话费计算装置中，所述监控模块在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

[0014] 前述的手机话费计算装置中，所述通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0015] 前述的手机话费计算装置中，所述业务支撑服务器是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0016] 与现有技术相比，本发明由于使用了无线网络、业务支撑服务器和手机组成的基本构架，并在手机上结合了用于同步用户的话费计费规则到手机上的网络同步模块、用于记录用户通话详情的监控模块和用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价的批价模块。这种结合方式可以使计算话费时的实时性和准确性高，并且可直接在手机上查询，无需密码，更加方便快捷，同时存储的账单也便于用户对话费的核对。本发明所提供的手机话费计算装置，针对特定用户计算他自身的手机话费，话费详单数据量小，使用户可以很方便、快捷的查看、汇总自己以往的话费使用情况，并且可以在通话结束后立刻看到通话费用的变化。同时利用了电信运营商的话费计算规则，保证了话费计算的准确性，透明性。又因为计费规则存储在手机上，所以无需等待一次通话、联网结束即可实时计算当前通话、联网所产生的费用，更可以在拨出、接听一个电话之前预估本次通话每分钟的费用。现有的计费装置是在电信端计算，这套装置要对一个地市或一省的所有用户提供计费服务，其计算、存储的数据量相当庞大，因此也造成了计算的实时性较差，准确度不高，查询不便的问题。而本装置只针对特定用户计算，数据量、运算量只有电信计费装置的数百万至数千万分之一。对于正常使用的用户，每个月的数据存储只消耗数百 K，每天需要计费的电话、短信、上网等次数也只有数百次以内，完全可以做到实时准确的计算。

附图说明

[0017] 图 1 是本发明的结构示意图；

图 2 是本发明实施例的工作流程图；

图 3 是图 2 中步骤 S10 的工作流程图。

[0018] 附图中的标记：1- 网络同步模块，2- 监控模块，3- 批价模块，4- 存储模块，5- 用户信息模块，6- 列表下载模块，7- 选择模块，8- 规则下载模块，9- 业务支撑服务器。

具体实施方式

[0019] 下面结合附图和实施例对本发明作进一步的说明，但并不作为对本发明限制的依据。

实施例

[0020] 一种手机话费计算装置，结构如图 1 所示，包括无线网络、业务支撑服务器 3 和手机；还包括设置在手机上的

网络同步模块 1，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器 9 相连；

监控模块 2，用于记录用户通话详情；

批价模块 3，用于将网络同步模块 1 上的话费计费规则对监控模块 2 记录的用户通话详情进行批价；

存储模块 4，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块 2 和网络同步模块 1 与批价模块 3 相连，批价模块 3 与存储模块 4 相连。

[0021] 网络同步模块 1 包括获取手机的运营商、归属地和品牌信息的用户信息模块 5，根据获取的用户信息从业务支撑服务器 9 下载运营商该品牌下所有的套餐列表的列表下载模块 6、用于用户选择所用套餐的选择模块 7 和根据用户所选套餐从业务支撑服务器 9 获取该套餐计费规则的规则下载模块 8。

[0022] 用户信息模块 5 为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0023] 用户信息模块 5 也为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

[0024] 短信中心号与运营商、省份的对应关系从业务支撑服务器 9 下载，或预先存储在手机上。

[0025] 规则下载模块 8 下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS 上网费用计费规则、月租费、套餐费和手机号段。

[0026] 监控模块 2 在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

[0027] 通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0028] 业务支撑服务器 9 是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0029] 本发明的工作流程(如图 2)：

步骤 S10，通过网络同步模块 1 同步该用户的话费计费规则到手机；

步骤 S20，在手机端通过监控模块 2 监控用户的通话、发送短信、通过 GPRS 联网的行为，

并将此行为存为详细日志；

步骤 S30，在批价模块 3 上，使用该用户的话费计费规则对详细日志进行批价；

步骤 S50，用存储模块 4 将批价后的账单存储在手机上。并通过手机显示设备（可为手机显示屏）展现给用户。

[0030] 其中步骤 S10 还包括以下步骤（如图 3）：

步骤 S101，通过用户信息模块 5，用户选择所用手机的运营商、归属地和品牌；

步骤 S102，通过列表下载模块 6，手机从支撑服务器获取该运营商该品牌下所有的套餐列表；

步骤 S103，通过选择模块 7，用户从列表中选择自己采用的套餐；

步骤 S104，通过规则下载模块 8，手机从支撑服务器获取该套餐的计费规则。

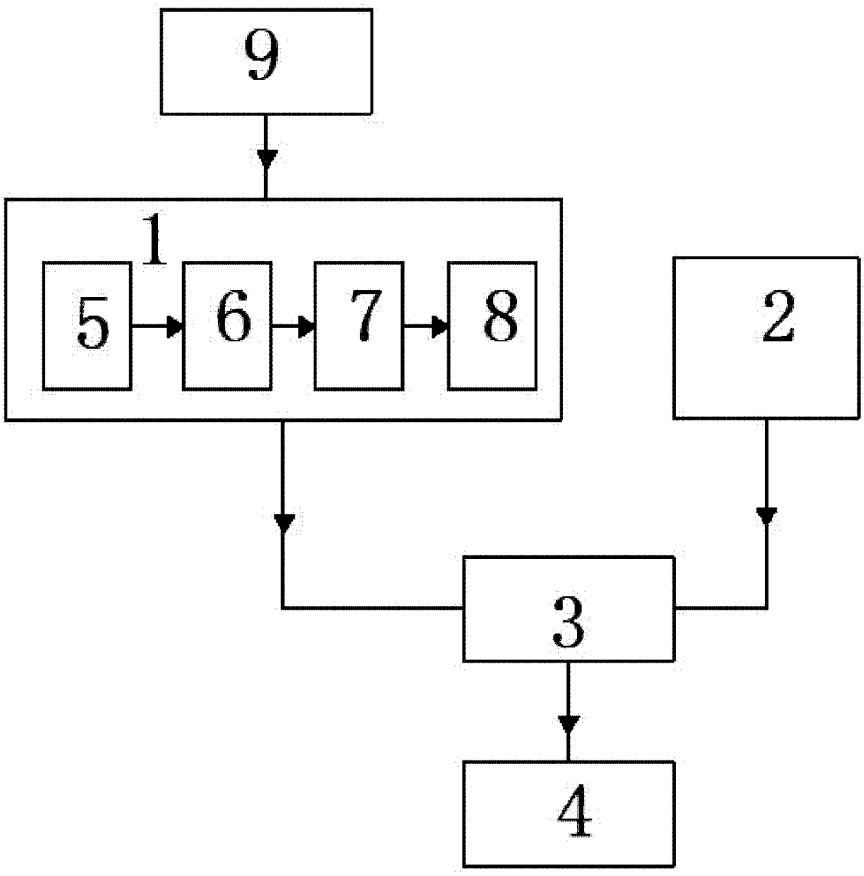


图 1

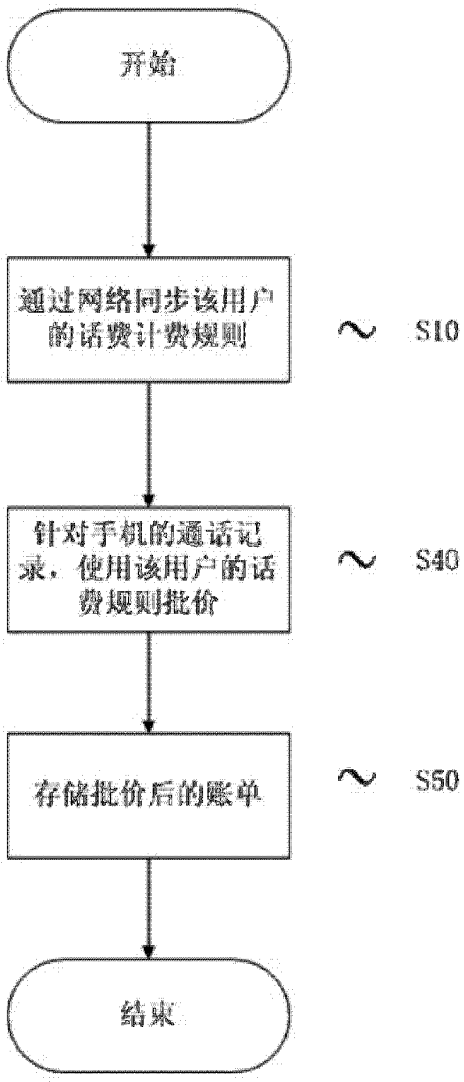

开始
通过网络同步该用户的话费计费规则
S10
针对手机的通话记录，使用该用户的话费规则批价
S40
存储批价后的账单
S50
结束

图 2

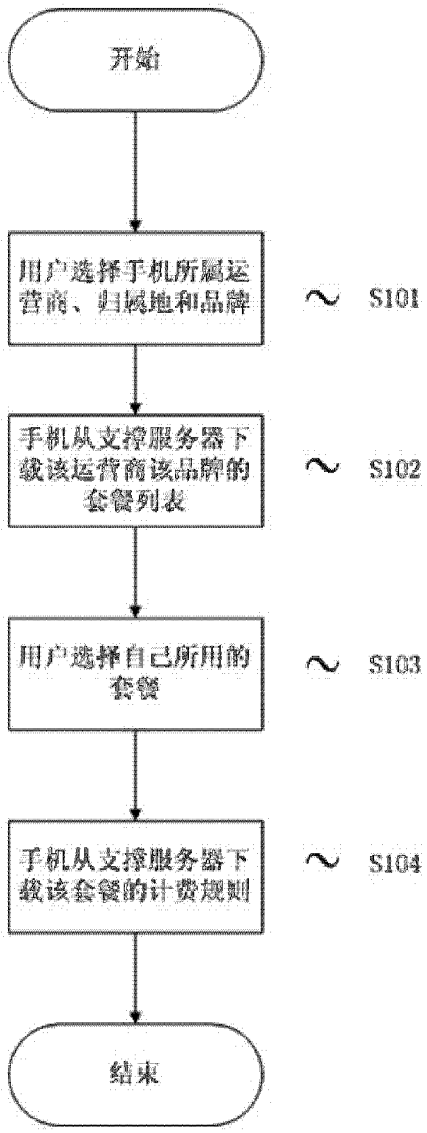

开始
用户选择手机所属运营商、归属地和品牌
S101
手机从支撑服务器下载该运营商该品牌的套餐列表
S102
用户选择自己所用的套餐
S103
手机从支撑服务器下载该套餐的计费规则
S104
结束

图 3

Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Mobile phone charge calculating device

CN 101815275 A

Publication number	CN101815275 A
Publication type	Application
Application number	CN 201010143134
Publication date	Aug 25, 2010
Filing date	Apr 9, 2010
Priority date	Apr 9, 2010
Inventors	樊秋实, 袁彬
Applicant	刘涉
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (2), Classifications (2), Legal Events (5)

External Links: SIPO, Espacenet

ABSTRACT

The invention discloses a mobile phone charge calculating device, which is characterized by comprising a wireless network, a service support server (9), a mobile phone, a network synchronization module (1), a monitoring module (2), a pricing module (3) and a storage module (4), wherein the network synchronization module (1) is arranged on the mobile phone and is used for synchronizing a charge billing rule of a user to the mobile phone; the monitoring module (2) is used for recording user conversation details; the pricing module (3) is used for pricing the user conversation details recorded by the monitoring module (2) by using the charge billing rule on the network synchronization module (1); and the storage module (4) is used for storing a bill after pricing in the mobile phone. The calculating device has high real-time performance and accuracy during charge calculation, can query the charge on the mobile phone directly, has a small charge detail record data volume, needs no password and is more convenient and efficient, and simultaneously the stored bill is convenient for a user to check the charge.

DESCRIPTION translated from Chinese

One kind of phone calls computing device

Art

[0001] The present invention relates to a phone bill computing devices, especially cell phone calls on a computing device to use the phone.

BACKGROUND

[0002] A typical billing system used by telecom operators, the business NE telecommunications operators to provide basic services systems, telecommunications core services include calls, SMS, GPRS (GeneralPacketRadioService), etc., each service corresponds to a Group business NE. ⑶R (calldetailrecord) is the business details of the recording, the details of each service provided to the user NE business records. CDR40 not only refers to the call detail records, including SMS or GPRS usage detail records. Each CDR contains the utterance time, end time, caller, callee, caller location and other information. Systems to business NE query CDR40, then CDR40 grant price, get bill details and billing details stored in the billing database.

[0003] and the existing computing system calls the following problems:

First, the existing computing system calls in the inner workings of the telecom operators, and prone to technical reasons because some calls wrong calculation, miscalculation of the situation, the mobile phone user is difficult to clearly understand the causes of their own each bill, and thus can not be determine their own phone bill accuracy, correctness.

[0004] Second, because of the huge number of single words, some carriers do not bill for all users with details of a single query service. Even some telecom operators for some users open the details of a single query of business, there are also inconvenient to use (for example, to enter the service password, or to apply for Business Hall site), real-time is not strong (such as last month's bill can only check single detail, or details of a single bill a few days ago) and other

CLAIMS (9) translated from Chinese

1. A phone bill computing device, comprising: a wireless network, business support server (9) and mobile phones; also includes network settings on the phone synchronization module (1), is used to synchronize the user's calls to a cell phone charging rules connected through a wireless network and business support server (9); monitoring module (2) for recording call details of the user; grant price module (3) for network synchronization module calls accounting rules (1), for monitoring Module User Call Details (2) batch record price; memory module (4) for the phone, and connected storage bills after the grant price and the phone's display equipment; monitoring module (2) and network synchronization module (1) the approved price module (3) is connected, (4) is connected to the grant price module (3) and memory modules.

2. The phone calls computing device of claim 1, wherein, wherein: said network synchronization module (1) including access to mobile phone operators, attribution and brand information subscriber information module (5), according to the obtained user information from the business support server (9) Downloads operators under the brand list download module lists all the packages (6) for the user to select the choice with our subscription module (7) and based on user selected business support package from the server (9) to get the package charging rules rules download module (8).

3. 3. Phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

4. The phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) through the phone's SMS center number to determine the user's operators and the home provinces, through the mobile phone base station information to the current assist in determining the

issues.

[0005] Once again, even if the user got the details of a single bill, also because the calculation rules for each operator, a variety of different packages, such as the existence of preferential period, giving the number of calls and other special rules minute, causing the user to check the phone bill is very difficult .

SUMMARY

The purpose of [0006] The present invention is to provide a phone bill computing device. It is a user-friendly viewing and understanding, with a high real-time accuracy of phone calls computing device.

[0007] aspect of the present invention: a phone bill computing device, comprising: a wireless network, business support servers and mobile phones; also includes setting on the phone

Network synchronization module for synchronizing user charging rules to the phone calls connected through a wireless network and business support server;

Monitoring module for recording user call details;

Grant price module for network synchronization module calls on the accounting rules for the monitoring module records the user calls the details were approved price;

Storage module for on the phone, and connected storage bills after the grant price and the phone's display device; connected monitoring module and network synchronization module and the grant price of the module, the module is connected to the grant price and the storage module.

[0008] The computing device of phone calls, the network synchronization module includes access to mobile phone operators, attribution and subscriber information module brand of information, access to information based on user downloads carriers under the brand all the support from the business server Package list List Download module for the user to select the package selection module and access rules of the charging rules package downloaded from the service module supporting server based on user-selected packages.

[0009] The aforementioned phone bill computing device, wherein the user information module for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0010] The foregoing phone calls computing device, the mobile phone subscriber information module for SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0011] The foregoing phone calls computing device, the message center number correspondence between operators, provinces and downloaded from the service support server or stored on the phone.

[0012] The foregoing phone calls computing device, the rules of the download module download package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, Package fee and phone number section.

[0013] The aforementioned phone bill computing device, wherein the monitoring module to monitor the end user in the mobile phone calls, send text messages through GPRS network acts as the call details, and this behavior is saved as a detailed log, or directly call phone call records As the call details.

[0014] The foregoing calculation means phone calls, the call details including the user's calls, send text messages and through the GPRS network behavior utterance time, end time, the called party, the caller, the caller location and traffic.

[0015] The foregoing phone calls computing device, the storage server is a business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0016] Compared with the prior art, the basic framework of the present invention is the use of a wireless network, composed of business support servers and mobile phones, combined with a bill charging rules for synchronizing user on the phone to the network synchronization module on your phone record the call details of the user for the monitoring module and charging rules calls for network synchronization module for monitoring module records the user's call details were awarded the grant price price module. This combination can make calls when calculating real-time and high

location of the user module.

5. 5. phone calls computing device according to claim 4, wherein, characterized in that: the SMS center number correspondence between operators, provinces and from business support server (9) download, or stored on the phone.

6. 6. phone calls computing device according to claim 2, wherein, wherein: said rules download module (8) Download the package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, GRPS Charging Rules Internet access charges, monthly fees, course fees and phone number section.

7. 7. The phone calls computing device according to claim 1, characterized in that: the monitoring module (2) monitor the user's end of the phone call, send SMS, via GPRS network acts as the call details, and keep this behavior for detailed logging, or directly call phone call records as a call for more information.

8. 8. phone calls computing device according to claim 7, wherein, wherein: said call details including the user's calls, send SMS and GPRS network behavior by utterance time, ending time, the called party, the caller, the caller Location and traffic.

9. 9. phone calls, 2 or computing device according to claim 5, characterized in that: the business support server (9) is a storage package list, the corresponding charging rule packages and SMS center number and operators, provinces server relationship.

accuracy, and can query directly on the phone without a password, faster and more convenient, but also easy for users to store bills for calls reconciliation. Phone calls computing device of the present invention provides, calculated for a particular user's phone bill of his own, a small amount of data calls single detail, so that users can easily and quickly view, summarizing his past calls usage, and can end in a call After seeing changes in the cost of calls immediately. While taking advantage of the service provider's bill calculation rules to ensure that the bill calculation accuracy, transparency. And because the accounting rules are stored on the phone, so no need to wait for a call, the networking end the current call to real-time computing, networking costs arising, more can be set aside, before answering a phone call estimate this cost per minute . Existing billing system is to calculate the telecommunications side, this device is to provide billing services for all users by one city or a province, which is calculated, the amount of data storage is quite large, and therefore resulted in the more real-time computing poor accuracy is not high, the query inconvenient questions. And this is only for a specific user computing device, the amount of data, computation device only telecommunications billing millions to thousands of parts per million. For normal use, the monthly data storage consumes only several hundred K, daily need billing telephone, text messaging, Internet and other times only within hundreds of times, can be done in real-time and accurate count Da Bian.

Brief Description

[0017] Figure 1 is a schematic structural view of the present invention; FIG. 2 is a flowchart of an embodiment of the present invention; FIG. 3 is a flowchart of step SIO of Figure 2.

[0018] The drawings mark: 1- network synchronization module, 2-monitoring module, 3 grant price module, 4 storage modules, user information module 5-, 6- List Download module, 7-selection module, 8 Rules download module, 9-business support server.

Specific embodiments

[0019] accompanying drawings and the following embodiment of the present invention will be further illustrated by, but not as a basis for limiting the present invention.

Example

[0020] A computing device phone calls, the structure shown in Figure 1, including Wi-Fi, business support server 3 and mobile phones; also includes setting on the phone

Network synchronization module 1, calls for synchronizing user charging rules to the phone, connected through a wireless network and business support server 9;

Monitoring Module 2, is used to record the call details of the user;

Module 3 approved price for network synchronization module Call Details user charging rule calls for a monitoring module 2 on the batch record price;

Storage Module 4 for the bill after the grant price of storage on the phone, and the phone is connected to a display device; monitoring module 2 and network synchronization module 1 module 3 is connected with the grant price, grant price of module 3 is connected with the storage module 4.

[0021] network synchronization module 1 includes access to mobile phone operators, attribution and brand information user information module 5, download carriers under the brand list all the packages to download the module from the list of six business support server 9 based on user access to information for the user to select the package selection module download module with 7 and rules based on user-selected packages to get the package from the service support server charging rules 9 8.

[0022] The user information module 5 for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0023] The user information module 5 also via mobile phone SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0024] SMS center number corresponds to the relationship operators, provinces and downloaded from the service support server 9, or stored on the phone.

[0025] Rule 8 download download module packages billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, package costs and phone number section.

[0026] 2 at the end of the phone monitoring module to monitor the user's call, send SMS, via GPRS network acts as the call details, and keep a detailed log of this behavior, or directly call phone call records as a call for more information.

[0027] Call details include the user's calls, send text messages and through the GPRS network behavior utterance time,

end time, the called party, the caller, the caller location and traffic.

[0028] 9 is a storage server business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0029] The workflow of the invention (Figure 2):

Step S10, the synchronous network synchronization module 1 through the user's calls to the phone charging rules; step S20, the mobile terminal 2 through the monitoring module to monitor users' calls, send text messages through GPRS network behavior, and this behavior is saved for details logs;

Step S30, the grant price Module 3, using the user's calls for a detailed log accounting rules grant price; step S50, with a storage module 4 will grant price after the bill is stored on the phone. And through mobile display devices (for mobile phone display) presented to the user.

[0030] wherein step further comprises the step SIO (Figure 3):

Step S101, the user information module 5, the user selects the mobile phone operators, attribution and brand; step S102, 6, cell phones get packages list of all under the carrier of the brand from the supporting server list download module; step S103, 7, users choose their own package by selecting the modules used from the list; step S104, the adoption of the rules download module 8, cell phone charging rules to get the package from the support server.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN102711076B *	May 24, 2012	Feb 11, 2015	武汉诚迈科技有限公司	一种实时预测手机通话余额的方法
WO2012171369A1 *	Mar 15, 2012	Dec 20, 2012	Zte Corporation	Method and system for calculating call charge of terminal

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04W88/02

LEGAL EVENTS

Date	Code	Event	Description
Oct 30, 2013	C12	Rejection of an application for a patent	
Jun 1, 2011	C41	Transfer of the right of patent application or the patent right	
Jun 1, 2011	ASS	Succession or assignment of patent right	**Effective date:** 20110421 **Free format text:** FORMER OWNER: LIU YANG **Owner name:** BEIJING WALI NETWORK TECHNOLOGY CO., LTD.
Jun 1, 2011	COR	Bibliographic change or correction in the description	**Free format text:** CORRECT: ADDRESS; FROM: 100190 UNIT 604, 6/F, SATELLITE BUILDING, NO. 63, ZHICHUN ROAD, HAIDIAN DISTRICT, BEIJING TO: 100114 ROOM 2533, BUILDING 3, NO. 3, XIJING ROAD, BADACHU HIGH-TECH. PARK, SHIJINGSHAN DISTRICT, BEIJING
Aug 25, 2010	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710123501.9

[43] 公开日 2008 年 12 月 31 日

[11] 公开号 CN 101335666A

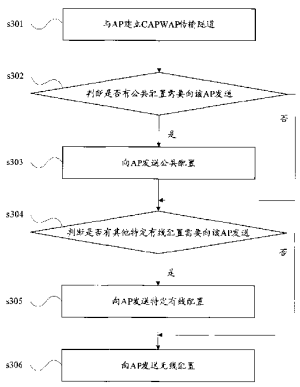
[22] 申请日 2007.6.29
[21] 申请号 200710123501.9
[71] 申请人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号华为杭州生产基地
[72] 发明人 史 扬 张志飞
[74] 专利代理机构 北京挺立专利事务所
代理人 龚家骅
权利要求书 3 页 说明书 13 页 附图 4 页

[54] 发明名称

一种配置发送的方法、接入控制设备和接入点

[57] 摘要

本发明公开了一种配置发送方法，包括如下步骤：接入点接入时，获取需要向所述接入点发送的至少一个配置文件，该配置文件中包括供接入点进行接入的配置信息；向接入点发送该配置文件。 本发明还提供了一种接入控制设备和接入点。 通过使用本发明，实现了 CAPWAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。



1、一种配置发送方法，其特征在于，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

2、如权利要求 1 所述配置发送方法，其特征在于，所述配置文件为：

包括公共配置信息的公共配置文件、包括特定有线配置信息的有线配置文件中的至少一种。

3、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件的步骤具体为：

将所述配置文件通过至少一个配置数据请求 CFG Data Request 消息向接入点发送；

接收到所述接入点响应的配置数据响应 CFG Data Response 消息时，若所述配置文件的发送未完成，继续发送下一 CFG Data Request 消息直至所述发送完成。

4、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件的步骤具体为：

将所述配置文件预先存储在接入点能够连接的网络设备上；

通知所述接入点所述网络设备的地址，以供所述接入点获取所述配置文件。

5、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件后还包括：

根据无线接入点控制与配置协议，在向所述接入点发送的协议消息中填加无线配置信息；

向所述接入点发送所述包括无线配置信息的协议消息。

6、一种配置发送方法，其特征在于，包括如下步骤：

获取接入控制设备发送的至少一个配置文件，所述配置文件中包括接入所述接入控制设备所需的配置信息；

根据所述配置文件中的配置信息，更新本地的配置。

7、如权利要求 6 所述配置发送方法，其特征在于，所述获取接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通过至少一个 CFG Data Request 消息发送的所述配置文件；

接收所述 CFG Data Request 消息完毕时，向所述接入控制设备响应 CFG Data Response 消息；

所述配置文件的发送未完成时，继续接收下一 CFG Data Request 消息并响应 CFG Data Response 消息直至所述发送完成。

8、如权利要求 6 所述配置发送方法，其特征在于，所述获取接收接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通知的存储有配置文件的网络设备的地址；

根据所述网络设备的地址，获取所述配置文件。

9、如权利要求 6 所述配置发送方法，其特征在于，在所述根据配置文件中的配置信息，更新本地的配置的步骤后，还包括步骤：

接收所述接入控制设备发送的包括无线配置信息的协议消息；

根据无线接入点控制与配置协议以及所述无线配置信息更新本地的无线配置。

10、一种配置发送方法，其特征在于，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

11、如权利要求 10 所述配置发送方法，其特征在于，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

12、一种接入控制设备，其特征在于，包括：

配置获取模块，用于接入点接入时，获取需要向所述接入点发送的至少一个配置文件；

配置发送模块，用于将所述配置获取模块获取的配置文件，向所述接入点发送。

13、如权利要求 12 所述接入控制设备，其特征在于，还包括:

配置存储模块，用于存储向接入点发送的配置文件，并在需要时向所述配置发送模块发送，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

14、如权利要求 12 所述接入控制设备，其特征在于，还包括:

接收模块，用于当所述配置发送模块通过CFG Data Request消息发送配置文件时，接收接入点响应的CFG Data Response消息并通知所述配置存储模块，以继续所述配置文件的发送直至完成。

15、一种接入点，其特征在于，包括:

终端获取模块，用于获取接入控制设备发送的至少一个配置文件;

终端配置模块，用于根据所述终端获取模块接收到的配置文件，更新本地的配置。

16、如权利要求 15 所述接入点，其特征在于，所述终端配置模块进一步包括:

解析子模块，用于解析所述配置文件并获得可执行的配置命令;

处理子模块，用于根据所述解析子模块获得的配置命令更新本地的配置。

17、如权利要求 15 所述接入点，其特征在于，还包括:

终端发送模块，用于接收来自接入控制设备的用来发送配置文件的 CFG Data Request 消息，并用于当所述终端获取模块完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向所述接收接入控制设备响应 CFG Data Response 消息。

一种配置发送的方法、接入控制设备和接入点

技术领域

本发明涉及通信技术领域，尤其涉及一种配置发送的方法、接入控制设备和接入点。

背景技术

802.11 WLAN（Wireless Local Area Network，无线局域网）网络提供了一种局域网的无线连接服务。AP（Access Point，接入点）是无线局域网的一个重要组成设备，是一个无线收发设备，用于将从有线网络（例如 Internet）接收到的数据转换成无线信号发送，将接收到的无线信号转换成数据并转发到有线网络。

802.11 WLAN 网络目前已经广泛地应用于企业等用户。这些用户的 AP 设备数量多、安全敏感、对 Qos（Quality of Service，服务质量）有严格要求，需要有效地管理手段来保证网络可管理性，降低用户的操作管理成本。

针对企业用户的需求，IETF 组织成立了专门的 WG（Work Group，工作组）制定 CAPWAP（Configuration and Provisioning for Wireless Access Points，无效接入点控制与配置）协议草案，预计在很快将成为正式的标准。传统意义的 AP 如目前家庭普遍使用的 AP 设备，用于完成 802.11 协议定义的完整功能。CAPWAP WG 提出了 Fit AP 的概念，Fit AP 主要完成实时性功能如消息确认、发送 Beacon 帧等，而对 AP 的管理、用户认证等功能需要通过 AC（Access Controller，接入控制设备）协同完成。

CAPWAP 协议定义了 AP 和 AC 之间将建立控制和数据隧道来完成网络的控制和转发。在向无线用户提供接入之前，AC 必须完成对 AP 的参数配置以完成控制平面的建立。现有技术中 AC 向 AP 发送配置的流程如图 1 所示，包括:

步骤 s101、AP 向网络中广播 Discover Request（发现请求）消息，寻找

网络中存在的 AC。

此步骤为 AP 寻找 AC 的阶段。AP 以广播方式发送 Discover Request 消息，寻找网络中可以使用的 AC。

步骤 s102、接收到该 Discover Request 消息的 AC 向该 AP 返回 Discover Response（发现响应）消息。

AC 接收到 AP 的 Discover Request 消息后，向该 AP 发送 Discover Response 消息作为响应。

步骤 s103、AP 向 AC 发送 Join Request（加入请求）消息。

AP 接收到 AC 发送的 Discover Response 消息后，与该 AC 建立 DLTS（Datagram Transport Layer Security，数据报传输层安全性）连接，并向 AC 发送向 AC 发送 Join Request 消息。

步骤 s104、AC 向 AP 发送 Join Response（加入响应）消息。

AC 接收到 AP 的 Join Request 消息后，向该 AP 发送 Join Response 消息作为响应，通知 AP 可以开始对其提供服务。

步骤 s105、AC 与 AP 之间建立 CAPWAP 隧道。

步骤 s106～s107、AP 与 AC 之间通过 Configuration status request（配置状态请求）和 Configuration status Response（配置状态响应）消息进行交互，实现 AC 对 AP 的配置下发。

步骤 s108～s109、AP 与 AC 之间通过 Configuration Update Request（配置更新请求）和 Configuration Update Response（配置更新响应）消息进行交互，实现 AC 对 AP 的配置更新。

上述步骤 s106～s109 中，Configuration status request、Configuration status Response、Configuration Update Request 和 Configuration Update Response 消息中通过携带 TLV（Type Length Value，类项长度值）来实现对 Radio，WLAN service，Qos 等配置。CAPWAP 协议中定义的 TLV 格式如图 2 所示，其中 Type 项（16bit）和 Length 项（16bit）分别标识了 Value 一项中携带的内容和长度。

现有技术中这个配置方法主要是面向无线属性的配置，没有对有线相关属性的配置。而 WLAN 网络并不是一个独立于有线网络的另一个网络，特别

是当 AP 也进行本地数据转发，如即 CAWPAP 定义的 Local Bridge（本地桥接）模式），AP 需要知道整个网络中的 ACL（Access Control List，访问控制列表）、Qos 等策略。

如果对于有线相关的配置下发仍然通过扩展新的 TLV 方式来实现，必然增加很大工作量，而且 CAPWAP 要进行大量的 TLV 扩展。有线和无线配置紧密耦合的方式必然影响 CAPWAP 协议的扩展性。另外，在 TLV 的扩展上，特定的 TLV 扩展对应了特定的软件版本。而在配置时要求 AC 和 AP 同时支持相同版本的 TLV，如果 AC 和 AP 版本不配套将影响 TLV 配置的下发。因此在对 TLV 的扩展不是进行有线配置下发的有效方法。

发明内容

本发明要解决的问题是提供一种配置发送方法、接入控制设备和接入点，以实现 CAPWAP 协议下 AC 根据不同 AP 的需求向 AP 发送不同的有线和无线配置。

为达到上述目的，本发明实施例的技术方案提供一种配置发送方法，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

其中，所述配置文件为：

包括公共配置信息的公共配置文件、包括特定有线配置信息的有线配置文件中的至少一种。

其中，所述向接入点发送配置文件的步骤具体为：

将所述配置文件通过至少一个配置数据请求 CFG Data Request 消息向接入点发送；

接收到所述接入点响应的配置数据响应 CFG Data Response 消息时，若所述配置文件的发送未完成，继续发送下一 CFG Data Request 消息直至所述发送完成。

其中，所述向接入点发送配置文件的步骤具体为：

将所述配置文件预先存储在接入点能够连接的网络设备上；

通知所述接入点所述网络设备的地址，以供所述接入点获取所述配置文件。

其中，所述向接入点发送配置文件后还包括：

根据无线接入点控制与配置协议，在向所述接入点发送的协议消息中填加无线配置信息；

向所述接入点发送所述包括无线配置信息的协议消息。

本发明实施例的技术方案还提供一种在接入控制设备上执行的计算机程序，包括若干指令用以执行上述配置发送方法。

本发明实施例的技术方案还提供一种存储介质，存储上述在接入控制设备上执行的计算机程序。

本发明实施例的技术方案还提供一种计算机设备，包括用以执行上述配置发送方法的软件及与软件配合的硬件。

本发明实施例的技术方案还提供一种配置发送方法，包括如下步骤：

获取接入控制设备发送的至少一个配置文件，所述配置文件中包括接入所述接入控制设备所需的配置信息；

根据所述配置文件中的配置信息，更新本地的配置。

其中，所述获取接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通过至少一个 CFG Data Request 消息发送的所述配置文件；

接收所述 CFG Data Request 消息完毕时，向所述接入控制设备响应 CFG Data Response 消息；

所述配置文件的发送未完成时，继续接收下一 CFG Data Request 消息并响应 CFG Data Response 消息直至所述发送完成。

其中，所述获取接收接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通知的存储有配置文件的网络设备的地址；

根据所述网络设备的地址，获取所述配置文件。

其中，在所述根据配置文件中的配置信息，更新本地的配置的步骤后，还包括步骤:

接收所述接入控制设备发送的包括无线配置信息的协议消息;

根据无线接入点控制与配置协议以及所述无线配置信息更新本地的无线配置。

本发明实施例的技术方案还提供一种在接入点上执行的计算机程序，包括若干指令用以执行上述配置发送方法。

本发明实施例的技术方案还提供一种存储介质，存储上述在接入点上执行的计算机程序。

本发明实施例的技术方案还提供一种计算机设备，包括用以执行上述配置发送方法的软件及与软件配合的硬件。

本发明实施例的技术方案还提供一种配置发送方法，包括如下步骤:

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息;

向所述接入点发送所述配置文件。

其中，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

本发明实施例的技术方案还提供一种接入控制设备，包括:

配置获取模块，用于接入点接入时，获取需要向所述接入点发送的至少一个配置文件;

配置发送模块，用于将所述配置获取模块获取的配置文件，向所述接入点发送。

其中，还包括:

配置存储模块，用于存储向接入点发送的配置文件，并在需要时向所述配置发送模块发送，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

其中，还包括:

接收模块，用于当所述配置发送模块通过CFG Data Request消息发送配置

文件时，接收接入点响应的CFG Data Response消息并通知所述配置存储模块，以继续所述配置文件的发送直至完成。

本发明实施例的技术方案还提供一种接入点，包括：

终端获取模块，用于获取接入控制设备发送的至少一个配置文件；

终端配置模块，用于根据所述终端获取模块接收到的配置文件，更新本地的配置。

其中，所述终端配置模块进一步包括：

解析子模块，用于解析所述配置文件并获得可执行的配置命令；

处理子模块，用于根据所述解析子模块获得的配置命令更新本地的配置。

其中，还包括：

终端发送模块，用于接收来自接入控制设备的用来发送配置文件的 CFG Data Request 消息，并用于当所述终端获取模块完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向所述接收接入控制设备响应 CFG Data Response 消息。

本发明实施例的技术方案还提供一种网络，包括前述的接入控制设备以及前述的接入点。

与现有技术相比，本发明具有以下优点：

实现了 CAWPAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。

附图说明

图 1 是现有技术中 AC 向 AP 发送配置的流程图；

图 2 是现有技术中 CAPWAP 协议中定义的 TLV 格式示意图；

图 3 是本发明的实施例中配置发送方法的流程图；

图 4 是本发明的实施例中 CAPWAP 协议控制消息的格式示意图；

图 5 是本发明的实施例中 AC 与 AP 间配置发送的信令流程图；

图 6 是本发明的实施例中接入控制设备的结构示意图；

图 7 是本发明的实施例中接入点的结构示意图。

具体实施方式

以下结合附图和实施例，对本发明的实施方式做进一步说明。

本发明中的实施例中，将AC向AP发送配置的过程分为了三个部分:

第一部分为向AP发送公共配置。该公共配置为所有的AP在配置时都会使用的相同配置，主要包括有线配置，也可能包括部分无线配置。对于这部分配置可以存储在一个公共配置文件中。

第二部分为向AP发送有线配置。

对于特定的AP，除了公共配置外，可能还存在其他特别的有线配置。该有线配置可以根据AC对不同AP的控制策略在配置内容上有所不同，因此需要保存为不同的配置文件。或因不同厂商的AP支持的配置命令格式不同，而需要保存为不同的配置文件。AC可以将使用同一配置格式及配置策略的配置保存在独立的配置文件中，并在需要时独立下发，从而管理支持不同配置方式的AP。

第三部分为向AP发送无线配置。

该部分即当前的CAPWAP协议过程，具体的，AC可以通过与AP的消息交互，如通过在Configuration Status Request/Configuration Status Response，Configuration Update Request/Configuration Update Response中携带相关的无线配置的TLV，实现无线配置的发送。

以上三个配置发送过程对于特定的AP不一定全部存在，如对于某些AP可能不需要进行公共配置的发送，对于另外的某些AP可能不需要进行特定有线配置的发送。

本发明的实施例中一种配置发送的方法以AC对AP依次进行公共配置、有线配置、无线配置的发送为例，其中公共配置和有线配置的发送位于AC与AP的Join过程后、通过Configuration Status Request/Configuration Status Response消息交互进行无线配置下发前。如图3所示，该配置发送包括以下步骤:

步骤s301、AC与AP建立CAPWAP隧道。

步骤s302、AC判断是否有公共配置需要向AP发送，需要发送时进行步骤s303，否则进行步骤s304。

对于被管理的AP，像ACL，Qos等策略配置（一般称为全局配置），与该AC相连接的所有AP一般会共用相同的配置。这些配置，可以保存在一个公共配置文件中，如appublic.cfg，并在AP与AC建立CAPWAP隧道后，作为第一个配置下发给AP。

在该公共配置文件的格式上，可以采用文本文件txt的格式。在该文件中包括对不同的项的具体设置。例如在文件中，对于每一需要进行配置的公共配置中的内容，通过Type和Value项进行表示。其中Type项表示Value一项中所携带的内容的标识，Value项表示具体的配置内容。例如，假设在预先设置的公共配置编制规则中ACL的标识为4096，则需要在公共配置中进行ACL的设置时，将Type项设置为4096，并在Value项中携带需要向AP发送的ACL内容。AP在接收到该公共配置文件后，可以根据Type项的值得知该配置是对ACL的配置，并根据Value项的值对ACL进行配置。当然也可直接通过字符串对不同的配置内容进行标识，并通过Value项的值携带具体的配置。

步骤s303、AC向AP发送该公共配置。

在该公共配置的发送方式上，可以采取以下方式:

方式一: AC可以将appublic.cfg通过多个CFG Data request（配置数据请求）消息发送给AP。

每次AP收到消息后，向AC发送CFG Data response（配置数据响应）消息确认收到了配置。完成配置文件传输后，AP执行配置文件更新本地配置。

该CFG Data request消息和CFG Data response消息的格式可以参考现有CAPWAP协议中的控制消息的格式。现有CAPWAP协议中的控制消息的格式如图4所示，包括Message Type（消息类型）项、Sequence Number（顺序号）项、Message Element Length（消息信元长度）项、Flags（标识）项以及Message Element（消息信元）项。其中，通过Message Type项标识了控制消息的类型与功能，Sequence Number项用于对接收到的Request消息和返回的Response消息进行对应，Message Element Length项为Message Element项的长度，Flags项

为0，Message Element项为控制消息的相关具体内容。对于Message Type项，现有的CAPWAP协议中已经对一些控制消息进行了定义，如1代表Discovery Request消息，2代表Discovery Response消息等，因此通过扩展该Message Type项并使用新的标识，可以对CFG Data Request和CFG Data Response消息进行定义。

进行消息类型的定义后，AC可以根据和AP预先约定的发送方式，将公共配置向AP发送，例如AC约定每次向AP发送1000bit的内容，则AC将公共配置文件中前1000bit的内容添加在CFG Data Request消息中向AP发送，并在消息的末尾设置标识位。AP接收该CFG Data Request消息完毕后，向AC发送CFG Data Response消息作为响应。接收到该消息后，AC继续向通过CFG Data Request消息向AP发送公共配置，直至所有的公共配置发送完成。

方式二：AC可以通知AP通过其他协议，如tftp（Trivial File Transfer Protocol，普通文件传输协议）协议或ftp（File Transfer Protocol，文件传输协议）协议来获得公共配置。具体的，AC可以通知AP存储有该公共配置文件的tftp或ftp服务器的地址，以及可能需要的登录密码，由AP登录该tftp或ftp服务器，下载配置文件后，执行该配置文件更新本地配置。

步骤s304、AC判断是否有其他特定有线配置需要向该AP发送，需要发送时进行步骤s305，否则进行步骤s306。

除了公共配置外，对于特定的AP还可能还有其他特定有线配置。这些配置并不属于公共配置，可以保存在一个独立的配置文件，该配置文件名称可以对应AP的标示，如AP + AP序列号.cfg。

这些独立的配置文件可以保证系统的兼容性，例如当网络中出现不同厂商的AP，而这些AP支持不同的配置方式（配置文件格式）。系统可以把这些AP的配置保存在各自独立的配置文件中。通过这些不同AP配置的独立下发，可以实现AC同时管理来不同厂商的AP。

步骤s305、AC向AP发送该有线配置。

在该有线配置的发送方式上，可以参考步骤s303中AC在发送公共配置时所采取的不同发送方式。AP在接收到该有线配置文件后，执行该配置文件更

新本地配置。至此，AP完成了公共配置和有线配置的流程。

步骤s306、AC向AP发送无线配置。

该步骤中，通过当前CAPWAP协议中已经定义的与无线相关配置对应的TLV，AC与AP交互Configuration status request、Configuration status Response、Configuration Update Request或Configuration Update Response等消息实现对Radio、WLAN service、Qos等与无线相关的配置。AP收到配置后，更新本地无线配置。至此，AC向AP发送配置的流程结束。

上述实施例中AC对AP依次进行公共配置、有线配置、无线配置的信令流程图如图5所示，

步骤 s501、AP 向网络中广播 Discover Request 消息，寻找网络中存在的 AC。

步骤 s502、接收到该 Discover Request 消息的 AC 向该 AP 返回 Discover Response 消息。

步骤 s503、AP 向 AC 发送 Join Request 消息。

步骤 s504、AC 向 AP 发送 Join Response 消息。

步骤 s505、AC 与 AP 之间建立 CAPWAP 隧道。

步骤 s506～s507、AC 与 AP 之间通过 CFG Data Request 和 CFG Data Response 消息进行交互，实现公共配置和特定有线配置的下发。

步骤 s508～s509、AP 与 AC 之间通过 Configuration status request 和 Configuration status Response 消息进行交互，实现 AC 对 AP 的无线配置下发。

步骤 s510～s511、AP 与 AC 之间通过 Configuration Update Request 和 Configuration Update Response 消息进行交互，实现 AC 对 AP 的无线配置更新。

在上述实施例中，以AC对AP依次进行公共配置、有线配置、无线配置的下发为例，描述了本发明中一种发送配置的方法。该配置发送的顺序主要是基于一般情况下发送配置的顺序，即先公共配置后特定配置、先有线配置后无线配置。但是，在发送配置时所采用的顺序不限于以上顺序。另外，在不同的配置发送步骤，还需要考虑不同配置间的关系。以上述实施例为例，AC需要考虑对于某些AP只发送其特定的有线配置即可，而不需要下公共配置。

另外，在公共配置与特定的有线配置存在冲突时，应该通过设定优先级关系或修改配置文件以达到避免配置冲突的问题。

通过使用上述实施例中提供的配置发送方法，实现了CAWPAP能够灵活支持新的配置下发需求，特别是ACL，Qos等有线相关的配置需求，保证CAPWAP协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展TLV带来的繁琐的工作。

本发明的另一实施例中，提供了一种接入控制设备，如图6所示，包括:

配置存储模块10，用于存储需要向AP发送的配置文件。该配置文件具体为：包括公共配置信息的公共配置文件，以及包括特定有线配置的有线配置文件。其中，公共配置文件一般只有一个，其中主要包括有线配置，也可能同时包括无线设置。而有线配置文件可能很多，其文件个数由所需要的不特定有线配置的数量而定，不同的特定有线配置存储在不同的有线配置文件中。在具体的实现中，该存储模块10可能为AC上的存储实体，也可能为AC之外的tftp或ftp服务器等存储实体。

配置获取模块20，用于对不同的AP的状态，获取需要向该AP发送的公共配置和/或有线配置。并将需要向该AP发送的公共配置和/或特定有线配置通知配置发送模块30。

配置发送模块30，用于在接收到配置获取模块20发送的需要向AP发送的公共配置或特定的有线配置时，向AP发送该公共配置或特定的有线配置。发送方式从配置存储模块10中获取需要发送的内容并通过CFG Data Request消息发送；或在配置存储模块10为外部tftp或ftp服务器等存储实体时，通知AP该存储该公共配置或特定有线配置的服务器的地址。

接收模块 40，用于当配置发送模块 30 通过 CFG Data Request 消息发送有线配置时，接收接入点响应的 CFG Data Response 消息。并通知配置发送模块30，以继续公共配置或特定有线配置的发送直至完成。

本发明的另一实施例中，还提供了一种接入点，如图7所示，包括:

终端获取模块 50，用于接收接入控制设备发送的配置文件。获取方法可以为接收接入控制设备发送的 CFG Data Request 消息，或从接收接入控制设

备通知的网络设备通过 tftp 或 ftp 协议获取。

终端配置模块 60，用于根据终端获取模块 50 接收到的配置文件，更新本地的配置。该模块进一步包括解析子模块 61，用于解析配置文件并获得可执行的配置命令；以及处理子模块 62，用于根据解析子模块 61 获得的配置命令更新本地的配置。

终端发送模块 70，用于终端获取模块 50 完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向接收接入控制设备响应 CFG Data Response 消息。

通过使用以上实施例所提供的接入控制设备和接入点，实现了 CAWPAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。

以上方式中，仍然是通过在 Configuration Status Request/Configuration Status Response，Configuration Update Request/Configuration Update Response 中携带相关的无线配置的 TLV，实现无线配置的发送。这样做可以和现有的 CAPWAP 协议相兼容，然而，无线配置部分同样可以纳入到公共配置和特定配置中来，无线配置不再特殊化处理，可以统一到一个公共配置及各个特有配置中，而各个特有配置也不在局限为特定有线配置。本发明通过将各种配置纳入到一个或者多个配置文件中然后下发给 AP，AP 接收以后解析这些文件获取其中的配置命令完成配置工作。其通过一次开发就可以解决以后所有新增配置的问题，因为无论新增什么配置，只需要把它纳入到配置文件中即可，AP 就可以通过解析文件获得配置。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实

施例所述的方法。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

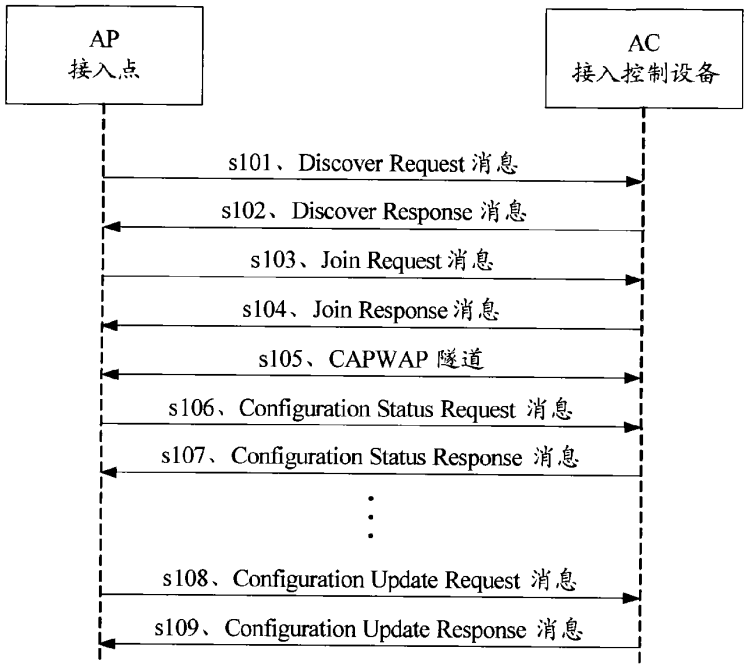

AP
接入点
AC
接入控制设备
s101、Discover Request 消息
s102、Discover Response 消息
s103、Join Request 消息
s104、Join Response 消息
s105、CAPWAP 隧道
s106、Configuration Status Request 消息
s107、Configuration Status Response 消息
s108、Configuration Update Request 消息
s109、Configuration Update Response 消息

图 1

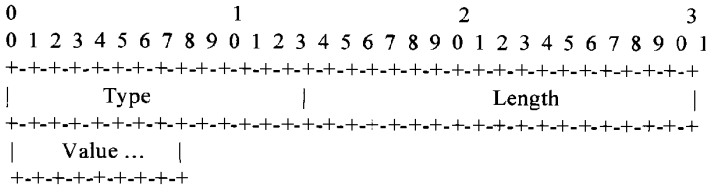

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Value ...

图 2

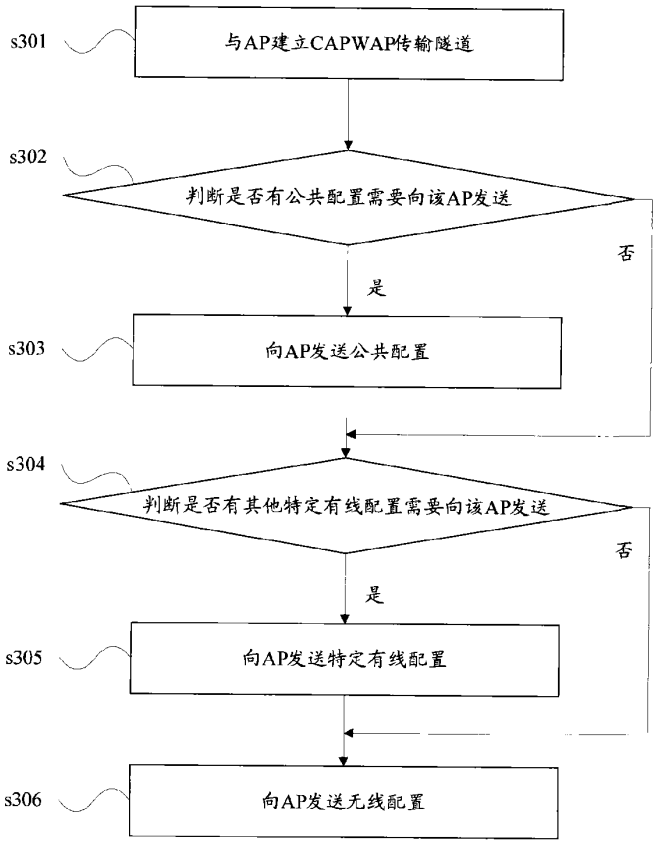

s301
与AP建立CAPWAP传输隧道
s302
判断是否有公共配置需要向该AP发送
否
是
s303
向AP发送公共配置
s304
判断是否有其他特定有线配置需要向该AP发送
否
是
s305
向AP发送特定有线配置
s306
向AP发送无线配置

图 3

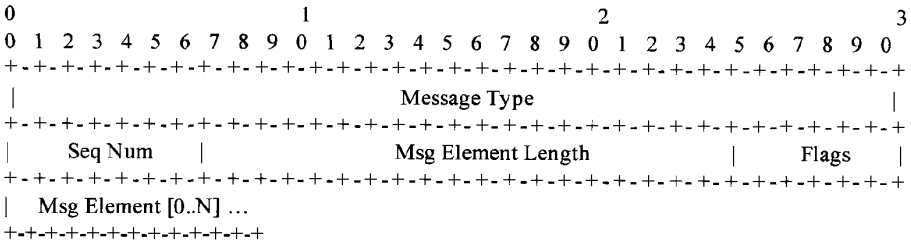

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Message Type
Seq Num
Msg Element Length
Flags
Msg Element [0..N] ...

图 4

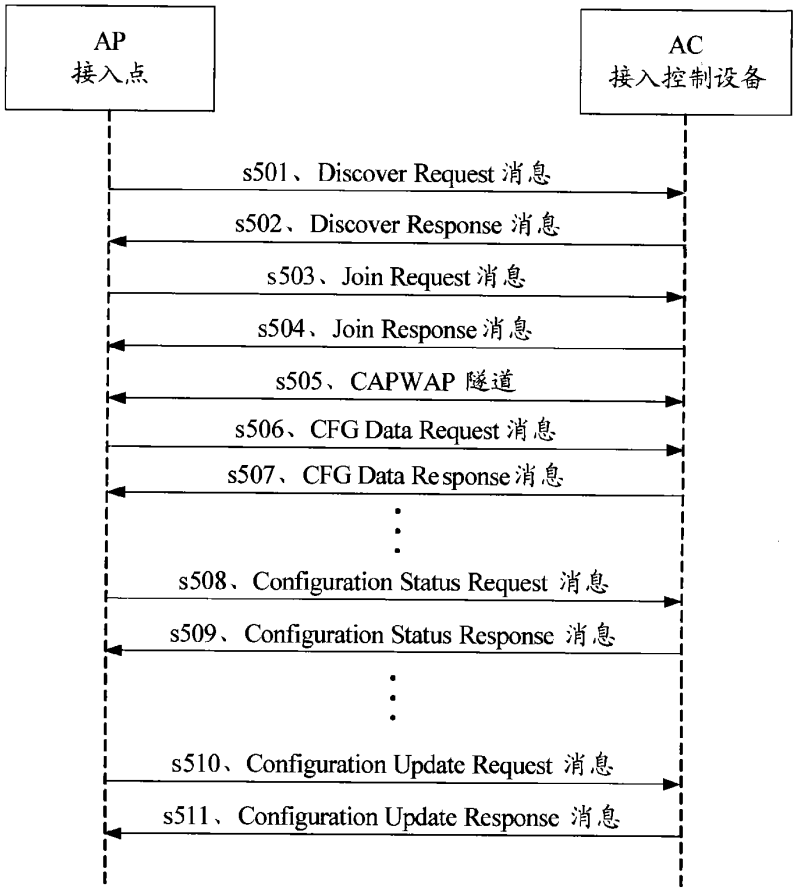

AP
接入点
AC
接入控制设备
s501、Discover Request 消息
s502、Discover Response 消息
s503、Join Request 消息
s504、Join Response 消息
s505、CAPWAP 隧道
s506、CFG Data Request 消息
s507、CFG Data Response 消息
s508、Configuration Status Request 消息
s509、Configuration Status Response 消息
s510、Configuration Update Request 消息
s511、Configuration Update Response 消息

图 5

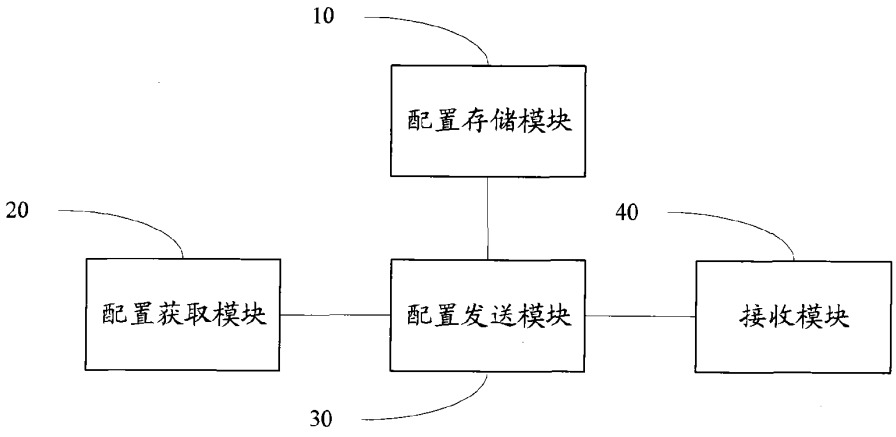

10
配置存储模块
20
40
配置获取模块
配置发送模块
接收模块
30

图 6

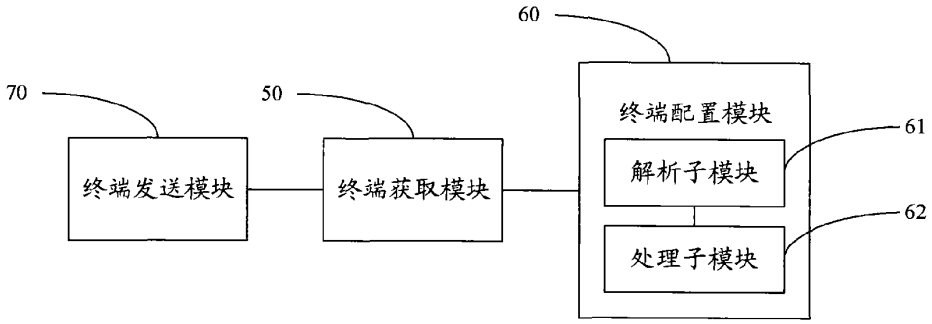

60
70
50
终端配置模块
61
终端发送模块
终端获取模块
解析子模块
62
处理子模块

图 7

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04M 1/247 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610157819.4

[43] 公开日 2007 年 11 月 28 日

[11] 公开号 CN 101080055A

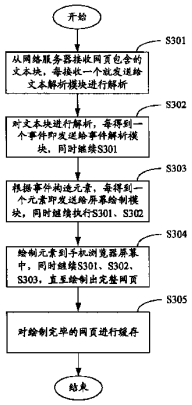
[22] 申请日 2006.12.21
[21] 申请号 200610157819.4
[71] 申请人 腾讯科技（深圳）有限公司
地址 518057 广东省深圳市高新科技园南区高新南一道飞亚达高科技大厦 5－10 层
[72] 发明人 纪 宇
[74] 专利代理机构 深圳市顺天达专利商标代理有限公司
代理人 郭伟刚 蔡晓红
权利要求书 4 页 说明书 12 页 附图 3 页

[54] 发明名称

一种基于手机浏览器快速浏览网页的方法、系统及设备

[57] 摘要

本发明涉及移动通信领域，提供了一种基于手机浏览器快速浏览网页的方法、系统及设备。 所述方法包括以下步骤：A. 所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给文本解析模块；B. 对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块，同时继续执行步骤 A；C. 根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤 A 和 B；D. 每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤 A、B、C，直至绘制出完整网页。 本发明提高了手机浏览器浏览网页时的显示效率。



1、一种基于手机浏览器快速浏览网页的系统，包括手机浏览器和网络服务器，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，其特征在于，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从所述网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块与所述网络收发模块相连，对所接收到的文本块进行解析并得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块与所述文本解析模块相连，根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

2、根据权利要求1所述的基于手机浏览器快速浏览网页的系统，其特征在于，所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制的网页。

3、一种手机浏览器，包括网络收发模块、文本解析模块、事件处理模块

和屏幕绘制模块，其特征在于，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块与所述网络收发模块相连，对所接收到的文本块进行解析并得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块与所述文本解析模块相连，根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

4、根据权利要求3所述的手机浏览器，其特征在于，所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制出的网页。

5、根据权利要求3或4所述的手机浏览器，其特征在于，所述手机浏览器设置有至少一个流量控制模式，用于限制所述手机浏览器在访问网页时所要下载文件的大小。

6、一种基于手机浏览器快速浏览网页的方法，其特征在于，所述方法包括以下步骤:

A.所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块；

B.所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时继续执行步骤A；

C.所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤A和B；

D.所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤A、B、C，直至绘制出完整网页。

7、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述步骤B中对文本块进行解析并得到对应事件的过程包括：

B1.从所述文本块中检测到一个文档开始标记，则产生一个开始文档树事件；

B2.继续检测到一个Tag开始标记，则产生一个开始元素事件；

B3.继续检测到一个Tag结束标记，则产生一个结束元素事件；

B4.当检测到一个文档结束标记，则产生一个结束文档树事件，并将所生成的事件发送给所述手机浏览器的事件处理模块进行处理。

8、根据权利要求7所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述步骤C中根据事件构造元素的过程包括：

C1.当收到所述开始文档树事件，则新建一个文档树，并设置当前游标为所述文档树的根节点；

C2.当收到所述开始元素事件，则生成一个新的元素，并将其设置为当前

游标节点的子节点;

C3.当收到所述结束元素事件，则计算当前游标元素的Rect，若所述游标元素的Rect与屏幕Rect存在交集，则产生绘制元素事件;

C4.当收到所述结束文档树事件，则结束当前线程，并将所生成的元素发送到所述手机浏览器的屏幕绘制模块进行绘制。

9、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述方法在步骤D之后进一步包括:

E.将所绘制出的网页的对象树存储到所述手机浏览器中，用于用户再次访问时的提取显示。

10、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述方法在步骤A之前进一步包括：对所述手机进行内存检测，若内存不足则释放缓存。

一种基于手机浏览器快速浏览网页的方法、系统及设备

技术领域

本发明涉及移动通信领域，更具体地说，涉及一种基于手机浏览器快速浏览网页的方法、系统及设备。

背景技术

随着因特网和移动通信技术的发展和融合，利用手机浏览器浏览网页已日益普及。

现有技术实现手机浏览器浏览网页所采取的方式是，首先下载完显示网页所需的全部文本及图片信息，然后在浏览器中统一显示。由于该现有技术的下载方式受限于网络速度，往往会导致网页显示得非常慢。

另一现有技术则采取将文本图片分步下载并显示的方式，也即：首先下载完文本文件，显示文本文件，然后下载图片，最后再显示完整的网页。该现有技术相对于前一技术，在网页显示效率方面有所提高，但仍不乐观。

因此需要一种新的方法，能够通过手机浏览器快速浏览网页。

发明内容

本发明的目的在于提供一种基于手机浏览器快速浏览网页的系统，旨在解决现有技术在利用手机浏览器浏览网页时显示效率低下的问题。

本发明的目的还在于提供一种基于手机浏览器快速浏览网页的设备，以更好地解决现有技术中存在的上述问题。

本发明的目的还在于提供一种基于手机浏览器快速浏览网页的方法，以更好地解决现有技术中存在的上述问题。

为了实现发明目的，所述基于手机浏览器快速浏览网页的系统包括手机浏览器和网络服务器，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括：

所述手机浏览器利用其网络收发模块从所述网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块；

所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块；

所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析；

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制的网页。

为了更好地实现发明目的，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，所述网络收发模块、文本解析模块、事

件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制出的网页。

所述手机浏览器设置有至少一个流量控制模式，用于限制所述手机浏览器在访问网页时所要下载文件的大小。

为了更好地实现发明目的，所述基于手机浏览器快速浏览网页的方法包括以下步骤:

A.所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

B.所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时继续执行步骤A;

C.所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤A和B;

D.所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤A、B、C，直至绘制出完整网页。

所述步骤B中对文本块进行解析并得到对应事件的过程包括:

B1.从所述文本块中检测到一个文档开始标记，则产生一个开始文档树事件;

B2.继续检测到一个Tag开始标记，则产生一个开始元素事件;

B3.继续检测到一个Tag结束标记，则产生一个结束元素事件;

B4.当检测到一个文档结束标记，则产生一个结束文档树事件，并将所生成的事件发送给所述手机浏览器的事件处理模块进行处理。

所述步骤C中根据事件构造元素的过程包括:

C1.当收到所述开始文档树事件，则新建一个文档树，并设置当前游标为所述文档树的根节点;

C2.当收到所述开始元素事件，则生成一个新的元素，并将其设置为当前游标节点的子节点;

C3.当收到所述结束元素事件，则计算当前游标元素的Rect，若所述游标元素的Rect与屏幕Rect存在交集，则产生绘制元素事件;

C4.当收到所述结束文档树事件，则结束当前线程，并将所生成的元素发送到所述手机浏览器的屏幕绘制模块进行绘制。

所述方法在步骤D之后进一步包括:

E.将所绘制出的网页的对象树存储到所述手机浏览器中，用于用户再次访问时的提取显示。

所述方法在步骤A之前进一步包括：对所述手机进行内存检测，若内存不足则释放缓存。

本发明通过将文本流转换成事件流，并利用手机浏览器中的各个模块以并行的方式对各事件进行解析、处理和绘制，从而提高了手机浏览器浏览网页时的显示效率；另外将所绘制的网页以对象树的形式进行缓存，进一步提高了网页的显示效率；此外还通过检查内存和进行流量控制，保证了浏览的安全性。

附图说明

图1是本发明中基于手机浏览器快速浏览网页的系统结构图;

图2是本发明中基于手机浏览器快速浏览网页的实现示意图;

图3是本发明中基于手机浏览器快速浏览网页的方法流程图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

在本发明中，手机浏览器利用其网络收发模块从网络服务器接收网页包含的文本块，且每接收到一个文本块就将其发送给手机浏览器中的文本解析模块；文本解析模块对所接收到的文本块进行解析，得到与文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收

文本块；事件处理模块根据文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析；屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素，直至绘制出完整网页。这种并行处理的方式极大地提高了手机浏览器浏览网页时的显示效率。

图1示出了本发明中基于手机浏览器快速浏览网页的系统结构，包括手机浏览器100和网络服务器200。

其中网络服务器200用于存储网络数据，并当用户通过手机浏览器100发送网页访问请求时，将该网页所包含的网络数据以文本块的形式返回给手机浏览器100。

手机浏览器100包括网络收发模块101、文本解析模块102、事件处理模块103、屏幕绘制模块104和缓存管理模块105，其中：

（1）网络收发模块101与网络服务器200之间进行通信，当用户期望浏览一个网页时，其根据用户的操作发送网页访问请求给网络服务器200，并接收返回的文本块形式的网页数据，然后将网页数据的这些文本块转发至文本解析模块102中进行处理。

（2）文本解析模块102与网络收发模块101和事件处理模块103相连，用于对网络收发模块101转发的文本块进行解析，得到相应的事件。本发明中并不是在网络收发模块101接收完网页的所有数据之后才将其发送到文本解析模块102中进行解析，而是在网络收发模块101接受完第一文本块之后就将其发送给

文本解析模块102，文本解析模块102立刻解析该第一文本块，得到与其对应的第一事件。在文本解析模块102对第一文本块进行解析的同时，网络收发模块101继续接收其他文本块。

（3）事件处理模块103与文本解析模块102、屏幕绘制模块104相连，用于对文本解析模块102解析得到的事件进行进一步处理，构造出与事件对应的元素。本发明中也并不是在文本解析模块102解析完所有的文本块之后才开始进行事件处理，而是在文本解析模块102解析得到第一事件之后就将该第一事件发送给事件处理模块103，事件处理模块103立刻处理该第一事件，构造其对应的第一元素。在事件处理模块103构造第一元素的同时，网络收发模块101继续接收其他文本块，且文本解析模块102继续对接收到的其他文本块进行解析。

（4）屏幕绘制模块104与事件处理模块103和缓存管理模块105相连，用于将事件处理模块103构造得到的元素绘制到手机浏览器100的屏幕上，直至最终绘制出完整的网页。本发明中也并不是在事件处理模块103构造出所有元素之后才开始进行绘制，而是在事件处理模块103构造出第一元素之后就将该第一元素发送给屏幕绘制模块104，屏幕绘制模块104立刻对该第一元素进行判断，若该第一元素的Rect值与屏幕Rect存在交集，则将该第一元素绘制到手机浏览器100的屏幕上。在屏幕绘制模块104绘制第一元素的同时，网络收发模块101继续接收其他文本块，且文本解析模块102继续对接收到的其他文本块进行解析，以及事件处理模块103继续构造其他元素。按照以上的并行处理方式，最终可快速地绘制出完整网页。

关于网络收发模块101、文本解析模块102、事件处理模块103、屏幕绘制模块104相互协作并行处理的具体过程，可参考附图2。

（5）缓存管理模块105与屏幕绘制模块104相连，用于缓存屏幕绘制模块

104所绘制出的网页的对象树，当用户再次访问该网页时则可根据该缓存管理模块105中的网页的对象树进行显示，进一步加快了网页显示的效率。

图2是本发明中基于手机浏览器100快速浏览网页的实现示意图。由该图可知，本发明中接收、解析、构造元素、绘制这四个步骤并不是单纯的串行处理：

各个模块内部所执行的操作是串行的，例如，网络收发模块101按时间顺序以串行方式接收各个文本块，文本解析模块102按时间顺序以串行方式对各个文本块进行解析并得到相应的事件，事件处理模块103按时间顺序以串行方式根据各个事件构造对应的元素，屏幕绘制模块104按时间顺序以串行方式将各元素绘制到手机浏览器100屏幕中的相应位置。

但是在整体上，各个模块对不同文本块的处理过程却是并行的，在本发明的其中一个实施例中，以图2进行说明如下：网络收发模块101接收到第一文本块并发送给文本解析模块102；当文本解析模块102对该第一文本块进行解析以得到第一事件的同时，网络收发模块101在接收第二文本块；当事件处理模块103根据第一事件构造第一元素的同时，网络收发模块101有可能正在接收第三文本块，且文本解析模块102则在对第二文本块进行解析；当屏幕绘制模块104将第一元素绘制到屏幕上的同时，网络收发模块101有可能正在接收第四文本块，且文本解析模块102则在对第三文本块进行解析，以及事件处理模块103正在根据第二事件构造第二元素。

利用以上的并行处理方式，可极大地提高网页显示的速度。例如，现有技术中显示一张网页时，需10秒钟读取完该网页包含的全部网络数据，3秒钟进行解析，3秒钟根据解析得到的事件构造出所有元素，5秒钟完成显示，则显示出来需要21秒。而在本发明中，若手机屏幕是128*128像素，用户访问的网页

经过排版后128像素宽、1024像素高，网络收发模块101只需要2秒钟左右可以读取128像素宽、128像素高的内容，其将此内容传递给文本解析模块102，文本解析模块102利用1秒钟完成解析，事件处理模块103用1秒钟构造元素，屏幕绘制模块104只需2秒钟完成绘制并显示，这样便只需要6秒钟就可以显示完占满用户手机屏幕的内容，在用户阅读内容的同时，继续作后续内容的收取、解析、构造和绘制显示。

图3示出了本发明中基于手机浏览器100快速浏览网页的方法流程。

在执行所有步骤之前，当用户期望浏览一个网页时，则通过手机浏览器100发送网页访问请求，该网页访问请求通过手机浏览器100中的网络收发模块101发送至网络服务器200。

在步骤S301中，网络收发模块101接收网络服务器200返回的上述网页包含的HTTP数据，这些数据以文本块的形式传送给网络收发模块101，网络收发模块101再将所接收到的文本块转发至文本解析模块102中。本发明中网络收发模块101并不是接收完网页的全部数据之后才将其发送，而是每接收到一个文本块则将其发送给文本解析模块102进行处理，同时网络收发模块101继续接收该网页的其他文本块。步骤S301的具体过程包括：若网络收发模块101收取到一个新的网页文档，则产生一个新文档（new Document）事件，自身继续收取文档。本发明中，网络收发模块101收取到一个文本块，则产生一个新文本块（new Document Block）事件，并将其立即发送给文本解析模块102进行解析。收取完所有文本块，则产生一个结束文档（end Document）事件，结束自己的线程。

在步骤S302中，文本解析模块102每次接收到网络收发模块101发送过来的文本块之后，则立刻对其进行解析，得到与该文本块对应的事件，且每解析得

到一个事件即发送至事件处理模块103中，同时继续执行步骤S301接收其他文本块。步骤S302中解析的具体过程包括：（1）对所接收到的文本块进行检测，当检测到一个文档开始标记（如<html>）时，则产生一个开始文档树事件；（2）继续检测到一个Tag开始标记（如<body>）时，则产生一个开始元素事件；（3）继续检测到一个Tag结束标记（如</body>）时，则产生一个结束元素事件；（4）当检测到一个文档结束标记（如</html>）时，则产生一个结束文档树事件。完成上述解析，则得到文本块对应的事件，并将该事件发送给手机浏览器100的事件处理模块103进行处理。在本发明的一个实施例中，若由于网络传输等因素造成网络收发模块101所接到到的是非完整性文档，如一个文档有5K字节，网络中断导致网络收发模块101仅收取了3K，则当文本解析模块102在对其进行解析时也将产生结束文档树事件，并通知事件处理模块103解析结束。

在步骤S303中，事件处理模块103根据文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块104中，同时继续执行步骤S301接收其他文本块，以及继续执行步骤S302对所接收到的文本块进行解析。步骤S303中根据事件构造元素的具体过程包括：（1）当事件处理模块103收到文本解析模块102发送的开始文档树事件，则新建一个文档树，并设置当前游标为该文档树的根节点；（2）当事件处理模块103继续接收到文本解析模块102发送的开始元素事件，则生成一个新的元素，并将其设置为当前游标节点的子节点；（3）当事件处理模块103继续接收到文本解析模块102发送的结束元素事件，则对游标元素进行排版，计算出游标元素的Rect，并同时更新此结点的父结点、爷爷结点直至根节点的Rect，如该游标元素的Rect与屏幕Rect（SR）存在交集，则产生一个绘制元素事件，同时调整游标，将游标节点的父结点设置为当前游标节点；（4）当事件处理模块103继续接收到文本解析模块102发送的结束文

档树事件，则结束当前线程，并将所生成的元素发送到手机浏览器100的屏幕绘制模块104中进行绘制。

在步骤S304中，屏幕绘制模块104每接收到事件处理模块103发送的一个绘制元素事件及相应的元素，就将该元素绘制到手机浏览器100屏幕上的对应位置，同时继续执行步骤S301、S302、S303，直至绘制出完整网页。关于对每一个元素进行绘制的具体过程，可参考现有技术。

如上所述，以上步骤S301、S302、S303、S304的执行过程，并不是一个简单的串行过程，在整体上是一个并行处理的过程，在一个步骤执行的同时其他步骤对应的线程也在运行，这样可在最短的时间内绘制出网页并显示给用户。

此外，在步骤S305中，当屏幕绘制模块104绘制出完整网页后，则将该网页的对象树存入缓存管理模块105中，这样当用户再次访问该网页时，则可直接提取该对象树显示出网页，进一步提高了效率。

本发明在实现快速浏览网页的同时，还考虑到安全浏览问题。由于手机在访问内容较多的互联网网页时，很可能会因为网页太大或者手机内存资源受限而造成手机浏览器100程序死机。为了解决这个问题，本发明提供了两种方法：

（1）引入内存检测（Check Memory）机制：在每个需要花费大量内存空间的函数入口都执行该内存检测机制，且在每一次申请内存时，都检查是否申请成功。如果内存检测的返回结果是“出错”（false），说明手机空余内存不足，或者申请内存失败，此种情况下应首先释放缓存，设置已经释放的标志，再回调到失败的函数本身。如果已经释放缓存仍然在内存检测时返回false，则产生内存不足错误，并且提示用户。

（2）在手机浏览器100中引入流量控制，典型的例如，可允许用户在手机浏览器100中设置三种流量控制模式：系统控制，限定单张网页最大流量，以及不下载图片。当用户选择“系统控制”时，每次下载网页或图片前，比较已下载文件和即将下载文件的大小总和与系统预设的允许大小值，如果大于系统预设的允许大小值，则不下载；当用户选择“限制单张网页最大流量”时，每次下载网页或图片前，比较已下载文件和即将下载文件的大小总和与用户设定的单张网页最大流量，大于用户设定值，则不下载；当用户选择“不下载图片”时，则不下载所有图片。

应当作出说明的是，本发明典型的应用但是并不限于在手机浏览器中浏览网页的情形，基于其他相关或类似的电子设备浏览网页时，也可以采用本发明的上述方法。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

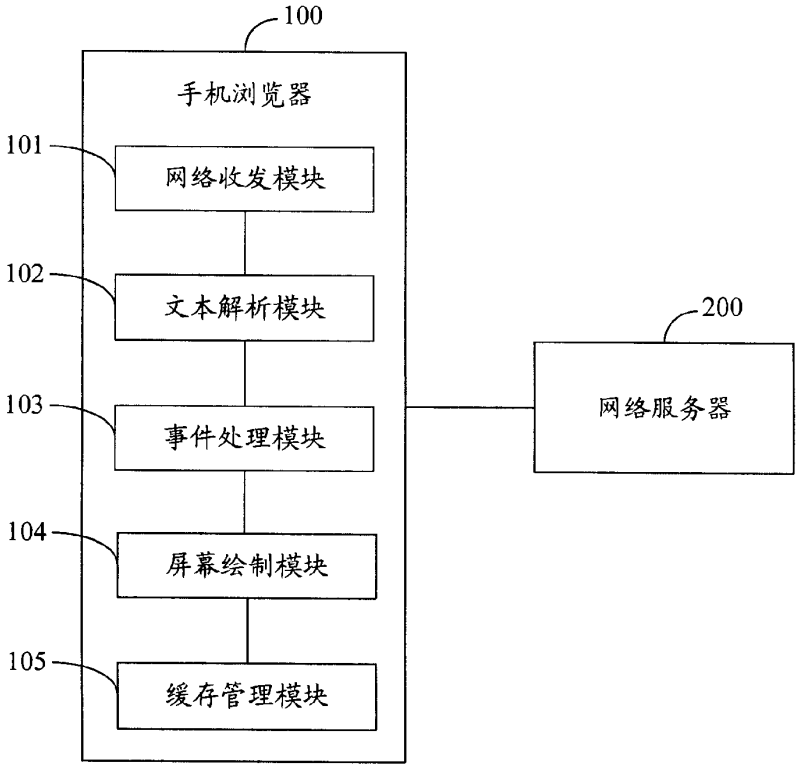

100
手机浏览器
101
网络收发模块
102
文本解析模块
103
事件处理模块
104
屏幕绘制模块
105
缓存管理模块
200
网络服务器

图 1

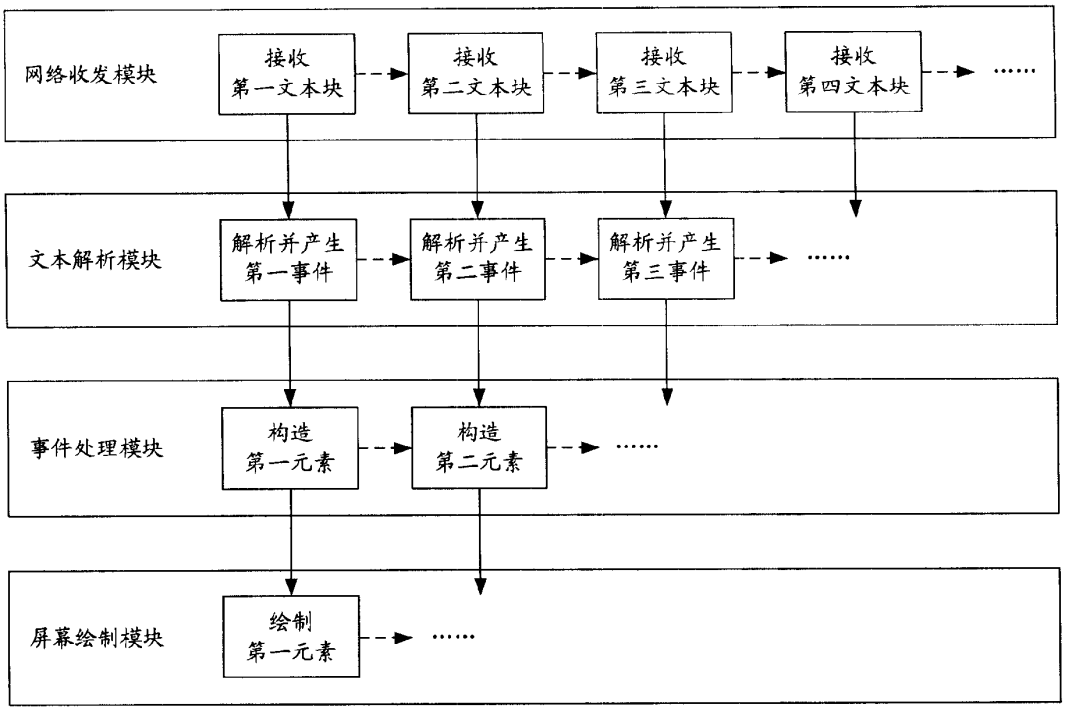

网络收发模块
接收
第一文本块
接收
第二文本块
接收
第三文本块
接收
第四文本块
……
文本解析模块
解析并产生
第一事件
解析并产生
第二事件
解析并产生
第三事件
……
事件处理模块
构造
第一元素
构造
第二元素
……
屏幕绘制模块
绘制
第一元素
……

图 2

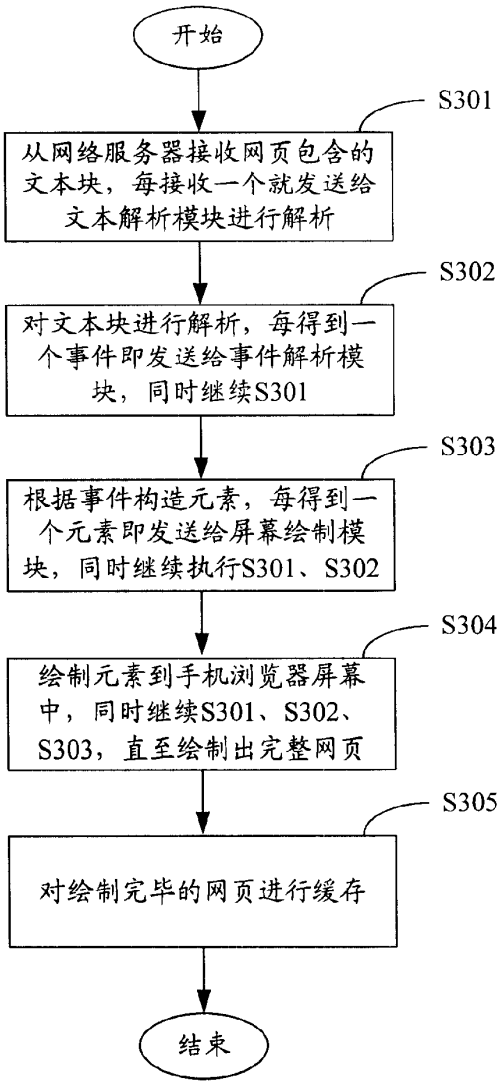

开始
S301
从网络服务器接收网页包含的文本块，每接收一个就发送给文本解析模块进行解析
S302
对文本块进行解析，每得到一个事件即发送给事件解析模块，同时继续S301
S303
根据事件构造元素，每得到一个元素即发送给屏幕绘制模块，同时继续执行S301、S302
S304
绘制元素到手机浏览器屏幕中，同时继续S301、S302、S303，直至绘制出完整网页
S305
对绘制完毕的网页进行缓存
结束

图 3

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/14
H04M 17/00

[12] 发明专利申请公开说明书

[21] 申请号 03137490.5

[43] 公开日 2005 年 1 月 19 日

[11] 公开号 CN 1567818A

[22] 申请日 2003.6.25 [21] 申请号 03137490.5

[71] 申请人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 张 庆 于 泽 严雪松

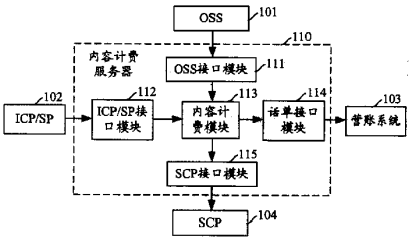
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 宋志强 王 琦

权利要求书 3 页 说明书 13 页 附图 1 页

[54] 发明名称 一种数据业务的内容计费方法及其计费系统

[57] 摘要

本发明公开了一种数据业务的内容计费方法，该方法将计费规则定制为计费规则部件，当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/业务提供商(ICP/SP)获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。本发明同时公开了一种业务的内容计费系统，该系统由专用的内容计费服务器来实现，其包含运营支撑系统(OSS)接口模块、ICP/SP 接口模块、内容计费模块、付费接口模块。本发明的这种内容计费方法及其计费系统，具有独立性、灵活性、可扩展性、开放性和分布性的特点，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。



ISSN1008-4274

1、一种数据业务的内容计费方法，其特征在于，该方法包括以下步骤：

1）按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；

2）预先保存签约数据业务用户的用户信息；

3）当用户执行数据业务时，根据该数据业务、步骤2）所述的用户信息和互联网内容提供商/业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。

2、如权利要求1所述的内容计费方法，其特征在于，所述的步骤1）进一步包括：为每个计费规则部件设置一个计费因子，通过对计费因子的组合实现多种计费规则的组合计费。

3、如权利要求1所述的内容计费方法，其特征在于，所述的用户信息至少包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

4、如权利要求3所述的内容计费方法，其特征在于，所述的步骤3）包括以下步骤：

31）根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

32）判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

5、如权利要求4所述的内容计费方法，其特征在于：当对移动数据业务进行计费时，所述的预付费处理设备为业务控制节点（SCP）。

6、如权利要求4所述的内容计费方法，其特征在于：该方法进一步包括，

步骤3）获得的计费结果由营帐系统根据用户需要生成用户帐单。

7、一种数据业务的内容计费系统，其特征在于，该系统包含内容计费服务器，该内容计费服务器至少包含：

运营支撑系统（OSS）接口模块，将OSS与内容计费模块相连，从OSS中获取签约数据业务用户的用户信息，发送给内容计费模块；

互联网内容提供商/业务提供商（ICP/SP）接口模块，将ICP/SP与内容计费模块相连， ICP/SP将内容计费记录信息发送给内容计费模块；

内容计费模块，根据数据业务类型、数据业务用户的用户信息、内容计费记录对数据业务进行计费，并根据付费类型生成计费结果；

付费接口模块，与内容计费模块相连，根据付费类型将计费结果发送给相应的付费处理设备。

8、如权利要求7所述的内容计费系统，其特征在于，所述的付费接口模块包含：

预付费接口模块，将预付费处理设备与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给预付费处理设备。

话单接口模块，将内容计费模块与营帐系统相连；将内容计费模块产生的后付费用户的计费结果发送给营帐系统。

9、如权利要求8所述的内容计费系统，其特征在于，所述的预付费接口模块为：业务控制节点（SCP）接口模块，将SCP与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给SCP。

10、如权利要求7所述的内容计费系统，其特征在于，所述的内容计费模块至少包含：

计费引擎，与OSS和ICP/SP分别相连，从OSS中获取签约数据业务用户的用户信息，接收ICP/SP发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件；

批价部件，保存不同数据业务类型的基本费率，根据数据业务类型、数据

业务用户的用户信息、内容计费记录从计费规则部件中取出相应的计费规则，对数据业务进行计费，并根据付费类型生成计费结果；

计费规则部件，根据不同数据业务类型存储不同的计费规则。

11、如权利要求 7 所述的内容计费系统，其特征在于，所述的用户信息至少包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

12、如权利要求 8 所述的内容计费系统，其特征在于，所述的话单接口模块为话单接口机，其与内容计费模块通过以文件格式传输信息。

13、如权利要求 9 所述的内容计费系统，其特征在于：所述的内容计费服务器与 OSS 为实时的同步消息接口，或以文件形式进行数据传输；内容计费服务器与 ICP/SP、内容计费服务器与 SCP 之间均按照运营商接口规范进行连接。

14、如权利要求 13 所述的内容计费系统，其特征在于，所述内容计费服务器与 ICP/SP 采用消息或文件方式进行交互；内容计费服务器与 SCP 之间采用扩展移动点到点协议（EMPP）协议消息进行交互。

15、如权利要求 8 所述的内容计费系统，其特征在于：话单接口模块与营帐系统以文件传输协议（FTP）或文件传输访问和管理（FTAM）传输信息，在用户需要时营帐系统通过话单接口模块到内容计费服务器取计费结果。

16、如权利要求 7 所述的内容计费系统，其特征在于，所述的内容计费服务器包含一个以上服务器；计费引擎与计费规则部件分布在不同的服务器主机上。

一种数据业务的内容计费方法及其计费系统

技术领域

本发明涉及数据业务的计费技术，特别涉及一种数据业务的内容计费方法及其计费系统。

背景技术

目前，根据通用移动通信系统（UMTS）论坛报告9的分析，3G数据业务分成内容连接类和移动性类两大类，内容连接类可以划分成：移动Internet接入和企业Intranet/Extranet接入；移动性类可以划分成：客户化信息、娱乐；多媒体消息业务；基于位置的业务；另外还有增强话音共6类业务。

这6类业务代表了3G业务的主要需求。今天以话音为主宰的移动通信领域，将来一定会是一个以数据业务为中心的环境。在任何时间任何地点能够接入Internet的内容将明确成为3G的重要任务。

3G计费是3G解决方案的一个重要组成部分。虽然3G业务是多种多样的，前景是诱人的，但如果没有相应的计费解决方案，不建立相应的价值链体系，即运行商无法运营，那么一切都是空谈。

目前传统的计费系统都是针对语音业务来设计的，一般根据呼叫持续的时间、主被叫的距离等因素进行计费。即传统计费与呼叫时长及主被叫位置相关，而与消费的业务内容无关。

目前的3G计费系统，仍然以语音业务的计费为主，其计费策略普遍采用硬编码的方式，即计费公式在代码中写死，一旦计费费率表确定，其计费算法也就相应固定。

硬编码方式的主要缺点在于代码重用性、灵活性差，如果增加新的需求则需要更改大量代码，代码间耦合性大，修改涉及面广，不易维护，也不利于计

费系统的稳定性。针对3G业务对计费灵活性的要求，此种实现方式显然不能满足。

另外一种方法是使用脚本的方式固化计费策略，使用脚本语言实现计费公式。使用脚本语言虽然可以非常灵活的增加新的计费策略，修改计费公式时也不必修改代码，但由于计费公式一般比较复杂，使用脚本实现有很大的困难、可读性很差。除此之外，对脚本语言的解释对系统性能也会产生一定的影响。

现有 3G 计费系统是由移动通信系统原有的设备整合来实现的，即计费功能融合在 SSP 或 SCP 中，由 SSP/SCP 完成对用户的计费功能。

传统的话音业务计费是和用户消费的内容无关的，只与时长（用户的通话时间）、距离（本地通话或长途）有关，因此不必上报业务信息或内容属性等，同时不关心用户消费业务的流量、次数，只需要在 SSP/SCP 侧统计用户的通话时间，由 SSP/SCP 完成对用户的计费功能后，由营帐系统根据计费结果，生成用户帐单，在用户需要时提交给用户。

3G 最吸引人的地方在于“永远在线”的服务，即只要打开手机就可以享受到丰富多采的业务内容，因此仅限于语音业务的传统计费系统明显不能满足多样化业务所带来的多样化内容计费的需求。因此传统的话音计费不能满足内容计费的需要。

且由于现有技术的计费系统通过移动通信系统原有的设备整合来实现，占用了移动通信系统的资源，计费过程繁琐，灵活性差，不能适应日益发展的丰富多采的数据业务的计费需要。

发明内容

有鉴于此，本发明的目的在于提供一种数据业务的内容计费方法，实现根据业务内容进行计费，满足数据业务中灵活多样的计费要求。

本发明的另一个目的在于提供一种数据业务的内容计费系统，节省移动通信系统资源，实现根据业务内容进行计费，满足数据业务中灵活多样的计

费要求。

根据上述目的的一个方面，本发明提供了一种数据业务的内容计费方法，该方法包括以下步骤：

1）按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；

2）预先保存签约数据业务用户的用户信息；

3）当用户执行数据业务时，根据该数据业务、步骤2）所述的用户信息和互联网内容提供商/业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。

其中，所述的步骤1）可以进一步包括：为每个计费规则部件设置一个计费因子，通过对计费因子的组合实现多种计费规则的组合计费。

所述的用户信息至少可以包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

所述的步骤3）可以包括以下步骤：

31）根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

32）判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

当对移动数据业务进行计费时，所述的预付费处理设备可以为业务控制节点（SCP）。

根据上述目的的另一个方面，本发明提供了一种内容计费系统，该系统包含专用的内容计费服务器，该内容计费服务器至少包含：

运营支撑系统（OSS）接口模块，将OSS与内容计费模块相连，从OSS中

获取签约数据业务用户的用户信息，发送给内容计费模块；

互联网内容提供商/业务提供商（ICP/SP）接口模块，将 ICP/SP 与内容计费模块相连， ICP/SP 将内容计费记录信息发送给内容计费模块；

内容计费模块，根据数据业务类型、数据业务用户的用户信息、内容计费记录对数据业务进行计费，并根据付费类型生成计费结果；

付费接口模块，与内容计费模块相连，根据付费类型将计费结果发送给相应的付费处理设备。该付费接口模块可以包含：

预付费接口模块，将预付费处理设备与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给预付费处理设备。

话单接口模块，将内容计费模块与营帐系统相连；将内容计费模块产生的后付费用户的计费结果发送给营帐系统。

其中，所述的预付费接口模块可以为：业务控制节点（SCP）接口模块，将 SCP 与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给 SCP。

所述的内容计费模块至少可以包含：

计费引擎，与 OSS 和 ICP/SP 分别相连，从 OSS 中获取签约数据业务用户的用户信息，接收 ICP/SP 发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件；

批价部件，保存不同数据业务类型的基本费率，根据数据业务类型、数据业务用户的用户信息、内容计费记录从计费规则部件中取出相应的计费规则，对数据业务进行计费，并根据付费类型生成计费结果；

计费规则部件，根据不同数据业务类型存储不同的计费规则。

所述的用户信息至少可以包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

所述的话单接口模块可以为话单接口机，其与内容计费模块通过以文件格

式传输信息。

所述的内容计费服务器与 OSS 可以为实时的同步消息接口，或以文件形式进行数据传输；内容计费服务器与 ICP/SP、内容计费服务器与 SCP 之间均可以按照运营商接口规范进行连接。

所述内容计费服务器与 ICP/SP 可以采用消息或文件方式进行交互；内容计费服务器与 SCP 之间可以采用扩展移动点到点协议（EMPP）协议消息进行交互。

话单接口模块与营帐系统可以以文件传输协议（FTP）或文件传输访问和管理（FTAM）传输信息，在用户需要时营帐系统通过话单接口模块到内容计费服务器取计费结果。

所述的内容计费服务器可以包含一个以上服务器；计费引擎与计费规则部件分布在不同的服务器主机上。

由本发明的技术方案可见，本发明的这种内容计费系统及其计费方法，将计费规则定制为计费规则部件，当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/ 业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。

附图说明

图 1 为本发明一个较佳实施例的内容计费实现框图；

图 2 为图 1 所示实施例中内容计费模块的实现框图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

本发明的这种数据业务的内容计费方法，是为了满足 3G 业务的特点，采用根据业务内容进行计费的方式。并根据计费需求的灵活多变，定制不同

的计费规则。也就是说，本发明能够根据计费规则定制不同的计费公式，对计费策略、折扣策略等实现灵活组合、易于扩充。

本发明的这种数据业务的内容计费方法，首先按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；同时预先保存签约数据业务用户的用户信息，该用户信息可以包括：用户开户信息、付费类型、用户属性、欠费记录等。

其中，在定制计费规则部件时，参考了下列因素：

A、不同 ICP/SP 可能有不同的计费策略；

B、不同业务可能有不同的资费策略，如游戏，不同游戏可能的收费不同；

C、支持按时长计费，如游戏，时间长短收费不同；

D、支持基于内容的流量计费，如下载图片，按照流量计费，但是费率根据不同的图片有所区别；

E、支持按使用次数计费（包括按条、按页面、按次计费），如下载图片、MP3、铃声等；

F、支持按时间段或日期采用不同的计费策略；如某些日期免费促销、每天的某些时间段访问给予一定折扣等；

G、支持平价计费、支持签约费（月租）+按使用次数或时长或流量等计费策略；

H、支持用户个性化的计费，不同用户可以根据自身情况选择不同的资费或计费策略；

I、支持随使用量不同（时长、流量、次数）采用不同的计费策略，其类似于跳档；

J、广告业务，支持用户访问ICP的广告送费服务，又可以分为赠送使用费和赠送使用量两种；

K、支持接入不同的数据网络采用不同的计费策略，考虑QoS等因素；

L、支持在不同区域或地区运用不同的计费策略，有可能在各“热点地区”

向用户收费不同。比如，可以相对于“办公区”的概念，对“生活区”收取更低的费用；

M、支持封顶费用。

除此之外，折扣是SP和网络运营商吸引用户的非常重要的手段，无论是传统的语音业务，还是面向3G的移动数据业务，折扣的地位都是举足轻重的。折扣方式多种多样，目前普遍使用的折扣方式主要有以下几种：

a、时间段折扣——保留现有的日常、星期、节假日折扣方式。这种方式也可以扩展到按流量计费的计费模式中。

b、累计折扣——包括时长累计折扣、流量累计折扣、条目累计折扣、金额累计折扣等4种折扣方式。

c、一次累计折扣——按照一次使用总量、一次使用总金额折扣

d、用户折扣——对某种集团用户进行统一的折扣。可在所有折扣基础上累乘。

e、业务折扣——对某种业务进行统一折扣。

本发明在具体实施中根据上述因素，定制了多个计费规则部件。一种业务的计费可以通过批价部件和一个或多个计费规则部件来实现。计费规则部件可以进行组合计费，同时为一种组合设置一个计费因子，在实际计费过程中用批价部件中的基本费率和计费因子实现多种附加计费规则的组合计费。

在实际应用中，数据业务的计费策略可以用批价部件中保存的基本费率信息+附加计费规则部件的计费因子信息”来描述。

例如：对应于互联网内容提供商的短信业务，那么其基本费率信息可以如表一所示，表一为一种短信业务简单的费率表。

费率 ID	计费模式	计费单位	费率值
1	1（按次计费）	1（次）	10（分）

表一

表一的含义就是对按次计费的业务，每次收 10 分钱。

不同的用户附加的计费因子可能不同，如果要求用户同时享受累积折扣、时间折扣，计费因子信息可以如表二所示，表二为一种短信业务计费因子表。

计费因子 ID	折扣标识	折扣索引	折扣部件
0	3（代表累积折扣）	0	累积折扣
0	5（代表时间折扣）	1	时间折扣

表二

表二对应了两种折扣，相当于将两种折扣组合成了一个计费因子。

上述两个表都是基本信息，实际应用中的表结构不仅限于此。

对应于累积折扣，如表三所示，表三为累积折扣表。

折扣 ID	折扣下限	折扣类型	折扣值
0（对应于计费因子表中的“折扣索引”字段）	30	0（表示百分比折扣）	80

表三

表三的含义就是当用户累积使用业务达到 30 次后，可以享受 8 折优惠

同样的，如表四所示，表四为时间折扣表。

折扣索引	起始时间	结束时间	折扣类型	折扣值
1	22:00:00	23:59:59	0(表示百分比折扣)	50

表四

表四的含义就是在 22：00~23：59 分使用业务的用户，都可以享受 5 折优

惠。

将基本费率信息与计费因子信息相结合，就得到了一种计费策略，这样的一个计费策略就可以和一个业务相绑定。参见表五，表五为短信业务的一种计费策略。

业务 ID	费率索引	计费因子索引
8888	1	0

表五

其中 ID 为 8888 的业务代表短信业务，其计费策略就是：按次计费业务，每次收费 10 分，同时如果用户累积使用 30 次以上，可以享受 8 折优惠，如果在 22：00~23：59 之间享受业务，又可以享受 5 折优惠。

如果一个用户已经使用该业务 30 次，又在 22：30 使用该业务，那么该用户的实际收取金额=1（次）*10（分）*0.8*0.5=4（分）

如果需求产生变动，要求除支持以上两种折扣之外，再增加一种用户折扣，那么计费因子描述表只需进行修改，修改后的计费因子描述表参见表六。

计费因子 ID	折扣标识	折扣索引	折扣部件
0	3	0	累积折扣
0	5	1	时间折扣
0	6	2	用户折扣

表六

这样，启动用户折扣部件，就可以轻而易举的实现动态增加一种折扣类型了，完全不需要做代码的修改，真正达到了动态灵活配置计费规则的目的。其中 6 代表用户折扣。

例如：一个个人移动用户签约了互联网内容提供商的短信业务，当该用户接收短信时，互联网内容提供商向内容计费服务器发送内容计费记录，其中包含了该用户执行的是短信业务、发送短信的条数、发送的时间等信息。内容计费服务器收到该内容计费记录后，取出 OSS 预先存储在内容计费服务器中的该

用户的个人信息，包括该用户的开户信息、付费类型（例如本用户为预付费用户）、该用户属性为个人用户、该用户没有欠费记录、用户已付费情况等信息。内容计费服务器根据该用户执行的是短信业务、发送短信的时间、发送短信的数目已超出预定额度，以及该用户为个人用户、且没有欠费记录，判断该用户应该享有表六所述的三种折扣，因此使用表六中ID号为0的计费因子进行计费，然后内容计费服务器将该计费结果发送给SCP，SCP在该用户的帐户上扣除相应的费用。

当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/ 业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。其中内容计费记录信息可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

其中内容计费可以由以下步骤来实现：

步骤 A、根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

步骤 B、判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，对于移动数据业务是业务控制节点（SCP），预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

步骤C、营帐系统根据用户需要取出计费结果，生成用户帐单。

参见图1，图1为本发明一个较佳实施例的内容计费实现框图。本实施例是对移动数据业务进行计费。其中内容计费系统由专用的内容计费服务器110来实现，该内容计费服务器110与OSS 101、ICP/SP 102、SCP 104和营帐系统分别相连。内容计费服务器110与OSS 101为实时的同步消息接口，或以文件形式进行数据传输 ，ICP/SP 102、SCP 104之间均按照运营商接口规范进行连接。其中，内容计费服务器110与ICP/SP102采用消息或文件方式进行交互；内容计费服务

器110与SCP 104之间采用EMPP协议消息进行交互。本实施例的接口均按照运营商接口规范设计，有利于与外部其他设备的对接。

本实施例中的内容计费服务器 110 包含了：

运营支撑系统（OSS）接口模块 111，将 OSS 101 与内容计费模块 113 相连，从 OSS 101 中获取签约移动数据业务用户的用户信息，发送给内容计费模块 113；

互联网内容提供商/ 业务提供商（ICP/SP）接口模块 112，将 ICP/SP102 与内容计费模块相连 113，ICP/SP 102 将内容计费记录信息发送给内容计费模块 110。

内容计费模块 113 是内容计费的主要功能模块，参见图 2，图 2 为图 1 所示实施例中内容计费模块的实现框图。内容计费模块 113 包含：计费引擎 201，其通过 OSS 接口模块 111、ICP/SP 接口模块与 OSS101 及 ICP/SP102 分别相连）从 OSS 101 中获取签约移动数据业务用户的用户信息，接收 ICP/SP 102 发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件 202。

批价部件 202，存储了不同移动数据业务类型的基本费率，根据移动数据业务类型、移动数据业务用户的用户信息、内容计费记录从相应的一个或多个计费规则部件 203 中取出相应的计费规则，对移动数据业务进行计费，并根据付费类型生成计费结果。

本实施例的内容计费服务器110预先定制了多个计费规则部件203，其根据不同移动数据业务类型分别存储不同的计费规则。计费规则部件203可以根据移动数据业务的变化，随时进行增加、删除和修改。可见，本实施例的内容计费系统以组件的方式实现，增加新需求即相当于增加新组件，对原有代码没有影响。同时各组件可以对外提供开放性接口，易于扩展。

总之，内容计费模块 113，根据移动数据业务类型、移动数据业务用户的用户信息、内容计费记录对移动数据业务进行计费，并根据付费类型生成计费结果。

业务控制节点（SCP）接口模块 115，将 SCP 104 与内容计费模块 113 相连，将内容计费模块 113 产生的预付费用户的计费结果发送给业务控制节点 104；

话单接口模块 114，将内容计费模块 113 与营帐系统 103 相连；将内容计费模块 113 产生的后付费用户的计费结果发送给营帐系统 103。

本实施例中的业务控制节点（SCP）接口模块 115 和话单接口模块 114 构成了付费接口模块，根据数据业务的付费类型将计费结果发送给相应的计费处理设备——业务控制节点 104 或营帐系统 103。

话单接口模块 114 与营帐系统以 FTP 或 FTAM 传输信息，在用户需要时营帐系统通过话单接口模块 114 到内容计费服务器 110 取计费结果。话单接口模块 114 可以由一个独立的话单接口机来实现，其与内容计费模块 113 通过以文件格式传输信息。

在本实施例的内容计费服务器 110 计费过程中，用户信息和内容计费记录信息是计费中的重要信息，该用户信息具体可以包括：用户开户信息、付费类型、用户属性、欠费记录；内容计费记录信息具体可以包括：移动数据业务类型、该移动数据业务执行的时间、执行该移动数据业务的数据流量、该移动数据业务执行的次数。

另外，本实施例的内容计费服务器110可以由多个服务器来实现；其中，计费引擎201可以由专用的服务器来实现，批价部件202和计费规则部件203分布在其他的专用的服务器主机上。这样计费引擎201与计费规则部件203分布在不同主机上，能够确保内容计费系统的性能。

本实施例的内容计费系统，使用专用的服务器来实现，不依赖于其他设备，与其他设备的交互采用消息机制或 API 函数调用机制，使内容计费模块具有较高的独立性，可以进行独立的测试，减少了开发与测试的工作量，易于维护。

同时，本实施例可以动态增加或修改计费规则部件的组合，无需修改代码或重启计费系统，具有很大的灵活性，最大限度的满足了计费需求的灵活

多变的特性。

由上述的实施例可见，本发明的这种数据业务的内容计费方法及其计费系统，具有独立性、灵活性、可扩展性、开放性和分布性的特点，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。

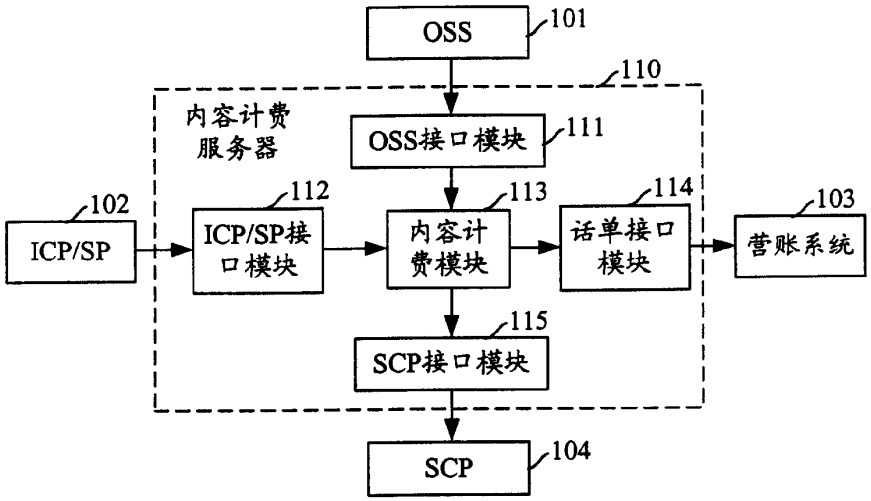

OSS
101
110
内容计费
服务器
OSS接口模块
111
102
ICP/SP
112
ICP/SP接
口模块
113
内容计
费模块
114
话单接口
模块
103
营账系统
115
SCP接口模块
SCP
104

图 1

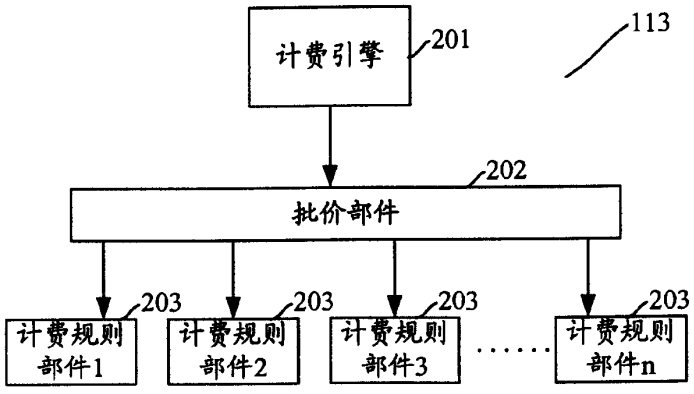

计费引擎
201
113
202
批价部件
203
计费规则
部件1
203
计费规则
部件2
203
计费规则
部件3
203
计费规则
部件n

图 2

Search Images Maps Gmail Drive Calendar Translate Docs More »

Google Patents Application Grant English Chinese Advanced Patent Search

Find prior art Discuss this application View PDF Download PDF

A content charging method of data service and charging system thereof

CN 1567818 A

Publication number	CN1567818 A
Publication type	Application
Application number	CN 03137490
Publication date	19 Jan 2005
Filing date	25 Jun 2003
Priority date	25 Jun 2003
Also published as	CN100550747C, CN101159566A, CN101159566B
Inventors	张庆, 于泽, 严雪松
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (9), Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention discloses a data service content charging method, customizing the charging rules as charging rule parts, as user executes data service, according to data service, user information and the content charging record obtained by Internet content provider/service provider (ICP/SP), using the corresponding charging rule part to making content charging. At the same time, it discloses a service content charging system, implemented by special content charging server and containing operation supporting system (OSS), ICP/SP interface module, content charging module, and payment interface module. It has the characters of independency, flexibility, extendability, openness and distributivity, realizes the charge according to data service content and meets the flexible and various charging requirements in data service.

DESCRIPTION translated from Chinese

A data service content charging method and charging system

Technical Field

The present invention relates to a data service charging technology, and more particularly to a data content service charging method and charging system.

Background

Currently, according to Universal Mobile Telecommunications System (UMTS) Forum Report 9 analysis, 3G data connection business into content categories and mobility class two categories, content connection type can be divided into: mobile Internet access and corporate Intranet / Extranet access; Mobility category can be divided into: customer information, entertainment; multimedia message service; location-based services; in addition to a total of six class enhanced voice services.

This 6 class of business represents a major demand for 3G services. Today, voice-dominated field of mobile communications, the future will be a data-centric business environment. Content at any time and any place to access the Internet will clearly be an important task of 3G.

3G billing is an important part of the 3G solutions. While 3G services are varied, prospects are tempting, but if there is no corresponding accounting solutions that do not establish the corresponding value chain system, which operators can not operate, then all talk.

Current traditional billing systems are designed for voice traffic, generally based on call duration, distance and other factors calling and called for billing. Namely the traditional billing and call duration and the Lord called location-related, regardless of the business content consumption.

The current 3G billing system, still based billing of voice services, its accounting policy commonly used hard-coded way, that the accounting formula in the code writing dead, once the billing rate tables to determine which accounting method correspondingly fixed.

CLAIMS (16) translated from Chinese

A method of data service billing content, characterized in that the method comprises the following steps: 1) according to the different types of data traffic of different charging rules, the one or more custom charging rules member; 2) pre-stored signed data service user's user information; 3) When the user performs data services, according to the data service, step 2) content of the user information and Internet content providers / service provider (ICP / SP) billing record information obtained using the corresponding charging rule components, content billing.

2. The content charging method according to claim 1, wherein said step a) further comprises: providing a charging member charging rules for each factor, by a combination of factors to achieve a variety of billing combination accounting rules for accounting.

3. The content billing method according to claim 1, wherein the user information includes at least: user account information, payment types, user attributes, arrears records; and the content billing record information including at least : data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

The content charging method according to claim 3, wherein said step 3) comprises the steps of: 31) in accordance with the type of data service, remove the corresponding charging rule corresponding charging rule member, then the data service based on the time for execution of data flow of the data service, the number of times the data service execution, an accounting rule for accounting; 32) to determine whether the type of user fees prepaid, if the prepaid The results will be sent to the prepaid billing processing equipment, processing equipment by prepaid billing deductions result from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

5. The content billing method according to claim 4, wherein: when

The main disadvantage is that the hard-coded code reuse, flexibility is poor, if the increase in new demand you need to change a lot of code, the code coupling between large, modification covers a wide, easy to maintain, is not conducive to the stability of the charging system. Billing flexibility for 3G services requirements, such implementations obviously can not meet.

Another way is to use a script curing accounting policy, using a scripting language for accounting formula. While using a scripting language can be very flexible to add new accounting policy, modify the accounting formula also having to modify the code, but is generally more complex due to the accounting formula, using scripts have great difficulty, poor readability. In addition, the interpretation of the scripting language for system performance will have some impact.

Billing systems existing 3G mobile communication system is composed of original equipment integration to achieve, namely accounting functions integrated in the SSP or SCP, the SSP / SCP complete user billing capabilities.

Traditional voice services and content user consumption billing is irrelevant, only the long (user talk time), distance (local or long-distance calls), and therefore do not have to report business information or content attributes, but users do not care about the consumer business traffic times, just in SSP / SCP side statistics users talk time, after the SSP / SCP complete user accounting function, the tent system based on accounting results generated user bill, presented to the user needs users.

3G the most attractive place is "always on" service, as long as open the phone you can enjoy the rich and varied business content, therefore limited to traditional voice services billing system obviously can not meet the diverse business brings diverse content billing requirements. Thus traditional voice billing does not meet the needs of content billing.

And because the prior art billing system via a mobile communication system to achieve the integration of existing equipment, takes up the resources of mobile communication systems, billing process cumbersome, inflexible, unable to meet the growing data business colorful count Fee required.

DISCLOSURE

In view of this, the present invention is to provide a data service content charging methods to achieve billing based on business content, data services to meet flexible billing requirements.

Another object of the present invention is to provide a data service content billing systems, saving mobile communication system resources, billing based on business content, data services to meet flexible billing requirements.

In accordance with one aspect of the above object, the present invention provides a data service billing content, the method comprising the steps of: 1) according to the different types of data traffic of different charging rules, one or more custom charging rules member; 2) the business user subscription data previously stored user information; 3) When the user performs data services, according to the data service, user information and Internet content provider in step 2) above / service provider (ICP / SP) obtained content billing record information, use the appropriate charging rule means content billing.

Wherein said step 1) may further comprise: providing a charging member charging rules for each factor, billing factor by charging a variety of combinations to achieve a combination of charging rules.

The user information may include at least: user account information, payment types, user attributes, arrears records; billing record information of the content may be at least include: the type of data service, the data service time for execution of the data service data traffic, the data service execution times.

Said step 3) may comprise the steps of: 31) in accordance with the type of data billing for mobile data services, prepaid processing equipment for the service control point (SCP).

Content billing method according to claim 6, wherein: the method further comprises, billing the result of step 3) obtained by the tent system according to the user needs to generate user billing.

A data service content billing system, wherein the system comprises content billing server, the content accounting server includes at least: Operations Support System (OSS) interface module, connect OSS and content billing module, Get the OSS in business user subscription data user information to the content billing module; Internet content provider / service provider (ICP / SP) interface module, connect ICP / SP and content billing module, ICP / SP will content billing record information to the billing module content; content billing module, based on the type of data services, data services, user's user information, content billing records billing data services, and generates accounting results based on the type of pay; Pay Interface module is connected to the content billing module, according to the type of charge will send the results to the appropriate billing payment processing equipment.

8. The content metering system according to claim 7, characterized in that said interface module comprises charge: prepaid interface module, the processing of prepaid billing module connected to the device with the content, the content of the billing module generates prepaid user accounting result to a prepaid processing equipment. If a single interface module, connect content billing module and tent systems; the content billing module generates after paying user accounting results to the camp system.

9. The content metering system according to claim 8, characterized in that the said prepaid module interfaces: service control point (SCP) interface module, the contents of the billing module connected to the SCP, the contents of the billing module generating prepaid subscribers accounting result to the SCP.

10. The content billing system according to claim 7, wherein the content of the billing module comprising at least: billing engine, connected respectively OSS and ICP / SP, get a business user subscription data from the OSS user information, content billing record information received ICP / SP transmitted, and user information and content billing record information to grant price components; grant price component, save the basic rate of different types of data traffic, according to the data type of business, data service user's user information, content billing record is removed from the charging rule corresponding charging rule parts, billing for data services, and generates accounting results based on the type of charge, charging rules parts, depending on the type of data service store different charging rules.

11. The content billing system according to claim 7, wherein the user information includes at least: user account information, payment types, user attributes, arrears records; content billing record information includes at least : data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

12. The content billing system according to claim 8, wherein said interface module for the bill if a single interface machine, its content billing module to transmit information by file format.

13. The content billing system according to claim 9, wherein: the content accounting server and OSS real-time synchronous message interface, or as files for data transmission; the content accounting server and ICP / SP , content billing server between SCP and are in

service, remove the corresponding charging rule corresponding charging rule component, then the data service based on the time for execution of the data flow of the data service, the number of times the data service execution, an accounting rule for accounting; 32) to determine whether the type of user fees prepaid, if prepaid will send the results to the prepaid billing processing equipment, processing equipment by prepaid plan fee deductions result from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

When billing for mobile data services, prepaid processing device may be the service control point (SCP).

According to another aspect of the above object, the present invention provides a content billing system, which includes a dedicated server content billing, content billing server that includes at least: Operations Support System (OSS) interface module, the OSS and content Billing module is connected, access the user's subscription data service user information from OSS, and sent to the billing module content; Internet content provider / service provider (ICP / SP) interface module, connect ICP / SP and content billing module , ICP / SP will send the contents of the billing record information to the billing module content; content billing module, based on the type of data services, data services, user's user information, content billing records data services billing, and paying according to the type of generation accounting result; pay interface module is connected to the content billing module, according to the type of charge will send the results to the appropriate billing payment processing equipment. The pay-interface module comprising: a prepaid interface module, a prepaid processing billing module connected devices and content, the content billing module generates prepaid subscribers accounting result to a prepaid processing equipment.

If a single interface module, connect content billing module and tent systems; the content billing module generates after paying user accounting results to the camp system.

Wherein the prepaid interface module can be: service control point (SCP) interface module, connect the SCP and content billing module, content billing module generates prepaid subscribers accounting result to the SCP.

The contents of the billing module can at least contain: billing engine, connected respectively OSS and ICP / SP, business users get subscription data user information from OSS, the content billing record information received ICP / SP to send, and user information and content billing record information to grant price components; grant price component, save the basic rate of different types of data traffic, according to the data service type, data service user's user information, content billing records from the accounting rule member Remove the appropriate accounting rules, data service billing, and generates accounting results based on the type of charge; charging rules parts, depending on the data stored in different types of business accounting rules.

The user information may include at least: user account information, payment types, user attributes, arrears records; billing record information of the content may be at least include: the type of data service, the data service time for execution of the data service data traffic, the data service execution times.

The CDRs CDR interface module can interface machine, with content billing module to transmit information to a file format.

The content of the accounting servers and OSS for real-time synchronous message interface, or as files for data transmission; can be carried out according to the operator interface specification between the content accounting server and ICP / SP, content billing server and SCP connection.

The content accounting server and ICP / SP can be used to interact with the message or file mode; the content may be used between the accounting server and SCP (EMPP) mobile PPP protocol message extension to interact.

If a single interface module and tent system can File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) transmit information when the user needs tent system via CDR interface module to fetch the content accounting server accounting results.

The content of the accounting server may contain one or more servers; billing and charging rules engine components distributed across different server host.

Seen from the aspect of the present invention, the content of the billing system and accounting methods of the present invention, the accounting rules for the charging rules customized parts, when the user performs data services, according to data services, user information and internet content provider content billing record information / service provider (ICP / SP) obtained using the corresponding charging rule parts, content billing, billing realized according to the data service content to meet the data services in flexible terms fee requirements.

accordance with the operator interface specification for the connection.

14. The content billing system as claimed in claim 13, characterized in that the content accounting server and ICP / SP messages or files using interactive manner; moving from point to point by the extended content billing server and SCP Protocol (EMPP) protocol message interaction.

15. The content billing system according to claim 8, wherein: if a single tent system interface module File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) transmit information when the user needs tent system By bill to content billing server interface modules take accounting results.

16. The content billing system according to claim 7, wherein the content of the accounting server contains more than one server; billing and charging rules engine components distributed across different server host.

Brief Description

Figure 1 is an example of content billing invention a preferred embodiment of realization diagram; Figure 2 is a block diagram of realization content billing module shown in FIG. 1 embodiment.

DETAILED DESCRIPTION

For the purposes of this invention, technical solutions and advantages more apparent, the following Examples and accompanying drawings, the present invention is described in further detail.

This data service content billing method of the present invention is to meet the characteristics of 3G services, the use of billing approach based on business content. And flexible billing based on the ever-changing needs, customize different charging rules. That is, the present invention can be customized according to different accounting rules billing formula, accounting policy, discount strategy flexible combination, easy expansion.

This data service content billing method of the present invention, the first data according to different accounting rules for different types of services, customized billing rule one or more parts; at the same time the business user subscription data previously stored user information, the user information including: user account information, payment types, user attributes, arrears records.

Among them, the custom component charging rules, the reference to the following factors: A, different ICP / SP may have different charging policies; B, different services may have different pricing strategies, such as different games, different games may charge; C, support long time and billing, such as casino games, duration and costs; D, support content-based traffic accounting, such as downloading pictures, according to traffic accounting, but the rates differ depending on the image; E, supported by using the number of billing (including Article, by page, pay-per), such as downloading pictures, MP3, ring tones; F, supported by time period or date using different accounting policies; as certain date free promotion, every day Some time access to give some discounts; G, support parity billing, support contract fee (monthly) + per use or duration or flow and other accounting policies; H, supports billing of individual users, different user You can choose according to their different tariff or billing strategy; I, the amount of support with the use of different (length, flow, frequency) using different accounting policies, which are similar to hop gear; J, advertising, allowing users to access the ICP advertising delivery fee service, and it can be divided Get royalty and Get amounts of the two to use; K, support access to different data networks using different accounting policies, and other factors to consider QoS; different L, support the use in different regions or areas billing policy, it is possible in the "hot spots" in different charge to the user. For example, with respect to the concept of "work area" on the "living area" to charge lower fees; M, support capping costs.

In addition, the discount is a very important means of SP and network operators to attract users, whether traditional voice services, or 3G for mobile data services, and discounts are pivotal position. Discount variety of ways, the current widespread use of rebates are the following: a, period discount - retaining the existing daily, week, holidays rebates. This approach can be extended to a metered charging mode.

b, the cumulative discount - including long cumulative discount, discount the cumulative flow, cumulative entry discount, the cumulative amount of discounts and other four kinds of rebates.

c, a cumulative discount - in accordance with the first use of the total, the total amount of time you use the discount d, user discounts - for certain user groups unified discount. All discounts can be tiring ride basis.

e, business discounts - for certain business unified discount.

In a specific embodiment of the present invention according to the above factors, a number of accounting rules customized components. Charging a business can be achieved by the grant price component and one or more charging rules components. Charging Rules components can be combined billing, and set a billing factor is a combination of the actual billing process using the grant price component of the base rate and billing factor to achieve a combination of a variety of additional charging rules count fee.

Basic Rate Information + billing factor information in practical applications, data services charging policies can be stored in approved price component parts of additional charging rules "to describe.

For example: corresponds to the short message service Internet content providers, its basic rate information as shown in Table I, Table I as a simple SMS tariff.

Image not available. View PDF

Table I Table it is the meaning of the pay-per-service, per charge 10 cents.

Different users additional accounting factor may be different, if the requirements of users while enjoying BONUS time discount factor accounting information as shown in Table II, Table II as a short message service charging factor table.

Image not available. View PDF

Table II Table II correspond to two discount, equivalent to two kinds of discount combined into a billing factor.

Both tables are basic information, practical application of the table structure is not limited to this.

Corresponding to the cumulative discount, as shown in Table III, Table 3 gives the BONUS table.

Image not available. View PDF

Table III Table III cumulative meaning that when users use the business 30 times, you can enjoy 20% discount Similarly, as shown in Table IV. Table IV is the time discount table.

Image not available. View PDF

Table 4 and Table IV meaning that at 22:00 ~ 23:59 minutes using business users, you can enjoy 50% discount.

The basic rate information and billing information combined factors, we get an accounting policy, such a billing policy can and bound to a business. Table V. Table V as an accounting policy SMS service.

Image not available. View PDF

Table V wherein the agent ID to SMS 8888, the accounting policy is: pay-per-service, a charge of 10 points, but if you use more than 30 times the cumulative, you can enjoy a 20% discount, if at 22:00 ~ 23: 59 between enjoying the business, you can enjoy a 50% discount.

If a user has used the service 30 times, and use the service at 22:30, then the user's actual charge amount = 1 (time) * 10 (points) * 0.8 * 0.5 = 4 (points) if demand fluctuates, Requirements In addition to supporting these two discount outside, and then add a user discount factor accounting description then just make changes, the revised accounting factor description in Table VI.

Image not available. View PDF

Table VI Thus, the launch customer discount member, you can easily add a dynamic type of discount, you do not need to modify the code completely, thereby achieving a dynamic and flexible accounting rules configuration purposes. Including six representatives user discounts.

For example: an individual mobile users subscribing to Internet content providers short message service, when the user receives messages, Internet content providers to send content billing records to the content accounting server, which contains the short message service is performed by the user, sending the number of text messages, send the time and other information. After the content accounting server receives the content billing records, remove OSS previously stored in the content accounting server in the user's personal information, including the user's account information, payment types (such as this user prepaid users), the user attributes for individual users, the user has no arrears records, and other information the user has paid. SMS content accounting server is performed based on the user, time to send text messages, send text messages number has exceeded a predetermined amount, and the user for individual users, and no arrears records to determine if the user should have the table of the six Three discount, so use Table 6 ID number is 0 billing factors accounting, billing and content billing server sends the results to the SCP, SCP deduct the cost on the user's account.

When the user performs data services, according to data services, content billing record information of the user information and Internet content providers / service provider (ICP / SP) obtained using the corresponding charging rule parts, content billing. Wherein the content billing record information may include: data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

Wherein the content billing can be achieved by the following steps: Step A, according to the data type of business, remove the corresponding charging rules in the corresponding parts in the accounting rules, according to the time the data service for execution of data flow of the data service the number of times the data service execution, an accounting rule for accounting; procedure B, determine whether the user charges prepaid type, if it is pre-paid billing results will be sent to the prepaid-processing equipment, for mobile data services is a service control point (SCP), prepaid billing processing apparatus according to the results of deductions from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

Procedure C, tent system takes the accounting results based on user needs, to generate user billing.

Referring to Figure 1, Figure 1 is a block diagram of an invention implement content billing preferred embodiment. In this embodiment, the mobile data service billing. Wherein the content billing system consists of a dedicated server 110 to implement content billing, content billing server 110 and OSS 101, ICP / SP 102, SCP 104 and tents are connected to the system. Content billing server 110 and OSS 101 is a real-time synchronous message interface, or as files for data

transmission, ICP / SP 102, between SCP 104 in accordance with the operator interface specification for the connection. Wherein the content accounting server 110 and ICP / SP102 messages or files using interactive mode; the content accounting server used between 110 and SCP 104 EMPP protocol messages to interact. Interface to the present embodiment in accordance with the operator interface specification design is conducive to docking and other external devices.

In this embodiment of the content billing server 110 includes: operations support systems (OSS) interface module 111, the OSS 101 is connected with the contents of the billing module 113 to obtain the user's mobile data service contract user information from OSS 101 and send it to content billing module 113; Internet content provider / service provider (ICP / SP) interface module 112, the ICP / SP102 and content billing module connected to 113, ICP / SP 102 content billing record information to the content billing module 110.

Content billing module 113 is the main function module content billing, see Figure 2, Figure 2 is a block diagram shown in Figure 1 to achieve the implementation of the contents of the accounting module. Content billing module 113 comprises: billing engine 201, which, ICP / SP interface module OSS101 and ICP / SP102 respectively connected via OSS interface module 111) to obtain the user's mobile data service contract user information from OSS 101, a receiving ICP / SP 102 content billing record information sent and the user information and content billing record information to grant price component 202.

Grant price component 202 stores a basic rate of different types of mobile data services, mobile data services based on the type of mobile data service user's user information, content billing records removed from the corresponding one or more of the appropriate accounting rules section 203 accounting rules, mobile data services billing, and generate results based on accounting charge type.

Content billing server 110 of the present embodiment a plurality of pre-charging rules customized member 203, which depending on the type of mobile data services are stored in different charging rules. Charging Rules section 203 may vary as mobile data services, at any time to add, delete and modify. Visible, content billing system of the present embodiment by way of implementation of the components, add the new requirement is equivalent to adding new components, there is no effect on the original code. At the same time the components can provide external open interfaces, easy to expand.

In short, content billing module 113, based on the type of mobile data services, mobile data service user's user information, content billing record for mobile data services billing, and generate results based on accounting charge type.

Service control point (SCP) interface module 115, the SCP 104 billing module 113 is connected with the content, content billing module 113 generates prepaid subscribers accounting result to the service control node 104; if a single interface module 114, the content billing module 113 is connected with the camp system 103; the contents of the billing module 113 generates after paying user accounting system 103 sends the results to the tent.

In this embodiment of the service control point (SCP) interface module 115, and then a single interface module 114 constitutes a charge interface module, based on the type of data services paid billing results will be sent to the appropriate accounting treatment equipment - service control node 104 or tent system 103.

If a single interface module 114 and tent systems to FTP or FTAM transfer information when the user needs tent system interface module 114 through the bill to take the accounting content billing server 110 results. If a single interface module 114 may be composed of a separate bill to implement the interface machine, with content billing module 113 to transmit information by file format.

In this embodiment, the content accounting server 110 billing process, user information and content billing record information is important billing information, the user information may include: user account information, payment types, user attributes, arrears record; content billing record information may include: a mobile data service type, time of the mobile data services for execution of the data flow of mobile data services, the number of times the mobile data service execution.

Further, the content accounting server 110 of the present embodiment may be implemented by a plurality of servers; wherein the billing engine 201 may be implemented by a dedicated server, rating and charging rules 202 parts 203 parts distributed in other dedicated server host. Such billing and charging rules engine 201 203 members distributed on different hosts, to ensure the performance of the contents of the billing system.

Examples of content billing system of this embodiment, the use of a dedicated server to achieve, is not dependent on other devices, messaging mechanism or API function calls to interact with other equipment used to make the contents of the billing module with high independence can be independent testing, reducing the effort required to develop and test, easy to maintain.

Also, the present embodiment can dynamically add or modify parts of combination accounting rules, without modifying the code or restart the billing system with great flexibility, and satisfy the changing needs Flexible billing features.

Seen from the above-described embodiment, the data traffic of the invention content billing method and billing system, independence, flexibility, scalability, openness and distribution characteristics, to achieve a data service based on content billing, data services to meet the flexible billing requirements.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100394737C	11 Jul 2005	11 Jun 2008	西安大唐电信有限公司	Method for accessing network server and supporting system
CN100596074C	9 Feb 2007	24 Mar 2010	华为技术有限公司	Charge mode providing method and charge control system
CN101582776B	15 May 2008	21 Nov 2012	浙江大学	Service charging method and service charging system
CN101800824A *	4 Mar 2010	11 Aug 2010	中兴通讯股份有限公司	Method and device for charging
CN102098650A *	21 Jan 2011	15 Jun 2011	中国联合网络通信集团有限公司	Content charging-based flow adaptive method and system
CN102098650B	21 Jan 2011	3 Jul 2013	中国联合网络通信集团有限公司	Content charging-based flow adaptation method and system
CN102255734A *	19 May 2010	23 Nov 2011	华为技术有限公司	Charging method of content business, apparatus and system thereof
WO2006116894A1 *	29 Apr 2005	9 Nov 2006	Utstarcom Telecom Co Ltd	A method of flexible setting the charging mode in ims system
WO2007051416A1 *	2 Nov 2006	10 May 2007	Huawei Tech Co Ltd	A charging method and system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04M17/00, H04L12/14

LEGAL EVENTS

Date	Code	Event	Description
14 Oct 2009	C14	Granted	
7 Dec 2005	C10	Request of examination as to substance	
19 Jan 2005	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Electronic Acknowledgement Receipt

EFS ID:	22688247
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	19-JUN-2015
Filing Date:	15-NOV-2013
Time Stamp:	16:37:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1.pdf	614366 95bbfac9c192382e86196bd7f91c14b0f5e74504	no	11

Warnings:	
Information:	

2	Foreign Reference	2060.pdf	1082588 d731de97188a46d46fa00f136f87db05a28d9044	no	10
Warnings:					
Information:					
3	Foreign Reference	2061.pdf	2061940 86232d632925d26176ca285a7928e3c5a3f21baa	no	21
Warnings:					
Information:					
4	Foreign Reference	2062.pdf	907410 8e1e1537e7aa0c658cd339f06c2b1b63ab448ad0	no	12
Warnings:					
Information:					
5	Foreign Reference	2063.pdf	2400276 5c7addfc40b293a3442a4c140083d3fc5d876114	no	21
Warnings:					
Information:					
6	Foreign Reference	2064.pdf	2345898 db3b0051c6d9ab3dfa64f05d6324394e5fc54486	no	20
Warnings:					
Information:					
7	Foreign Reference	2065.pdf	2381976 7796f26254f7db3b899626b2e7332663eaff0633	no	25
Warnings:					
Information:					
8	Non Patent Literature	3039_Dixon.pdf	1271520 5ff7631e8a8dfa2c00f75e44b77d86a2e9719407	no	12
Warnings:					
Information:					
9	Non Patent Literature	3040_Ahmed.pdf	698684 312cdbfa74f55adbbd7f0eee7032be26a77e3ad5	no	10
Warnings:					
Information:					
10	Non Patent Literature	3041_Kassar.pdf	840076 1b87a4e38876abbcb73a0c7a689d940a997ba013	no	14
Warnings:					
Information:					

11	Non Patent Literature	3042_Kaufmann.pdf	3412131 987a5e9e6c5cadcf6cd5982f4c181ac27b6dafe7	no	283
Warnings:					
Information:					
12	Non Patent Literature	3043_Sadeh.pdf	1095284 adc744cb7b194a97b6f3ac3e1b28a65e042a8d9f	no	16
Warnings:					
Information:					
		Total Files Size (in bytes):	19112149		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7809351	B1	2010-10-05	Panda et al.	
	2	8346210	B2	2013-01-01	Balsan et al.	
	3	8355696	B1	2013-01-15	Olding et al.	
	4	8488597		2013-07-16	Nie et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050250536	A1	2005-11-10	Deng et al.	
	2	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	20060035631	A1	2006-02-16	White et al.	
	4	20060206709	A1	2006-09-14	Labrou et al.	
	5	20070060200	A1	2007-03-15	Boris et al.	
	6	20090046707	A1	2009-02-19	Smires et al.	
	7	20100311402	A1	2010-12-09	Srinivasan et al.	
	8	20110277019	A1	2011-11-10	Pritchard Jr., John Russell	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-03-03
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/14 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710302140.4

[43] 公开日 2008 年 5 月 21 日

[11] 公开号 CN 101183958A

[22] 申请日 2007.12.14
[21] 申请号 200710302140.4
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 陈 靖 石迎生 袁潮灏

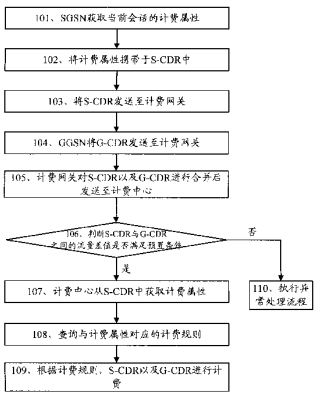
[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 逯长明
权利要求书 5 页 说明书 12 页 附图 2 页

[54] 发明名称

一种计费控制方法及计费中心以及相关设备

[57] 摘要

本发明公开了一种计费控制方法及计费中心以及相关设备，用于提高计费的精确性。本发明方法包括：通用分组无线服务支持节点 GSN 获取当前会话的计费属性；将所述计费属性携带于将所述计费属性携带于每一个 CDR 中，所述计费属性用于指示所述 CDR 的隧道相关信息；向计费中心发送所述 CDR；计费中心根据所述 CDR 中的信息获取所述 CDR 的计费属性；计费中心根据所述 CDR 以及其计费属性进行计费。本发明还提供计费中心以及相关设备。本发明可以有效地提高计费的精确性。



1、一种计费控制方法，其特征在于，包括:

通用分组无线服务支持节点 GSN 获取当前会话的计费属性;

将所述计费属性携带于每一个 GSN 计费数据记录 CDR 中，所述计费属性用于指示所述 CDR 的隧道相关信息;

向计费中心发送所述 CDR;

计费中心根据所述 CDR 中的信息获取所述 CDR 的计费属性;

计费中心根据所述 CDR 以及其计费属性进行计费。

2、根据权利要求 1 所述的方法，其特征在于，所述将所述计费属性携带于每一个 CDR 中的步骤包括:

在所述 CDR 中设置直接隧道标识用于指示所述 CDR 中所有的流量节点的属性均为单隧道。

3、根据权利要求 1 所述的方法，其特征在于，所述将所述计费属性携带于每一个 CDR 中的步骤包括:

在所述 CDR 中设置直接隧道标识;

若所述 CDR 中所有的流量节点的属性均为单隧道，则将所述直接隧道标识的数值设置为预置的数值。

4、根据权利要求 1 所述的方法，其特征在于，所述将所述计费属性携带于每一个 CDR 中的步骤包括:

在所述 CDR 中某个流量节点字段中设置直接隧道标识用于指示所述流量节点的属性均为单隧道。

5、根据权利要求 1 所述的方法，其特征在于，所述将所述计费属性携带于每一个 CDR 中的步骤包括:

在所述 CDR 中某个流量节点字段中设置直接隧道标识;

若所述流量节点的属性均为单隧道，则将所述直接隧道标识的数值设置为预置的数值。

6、根据权利要求 2 所述的方法，其特征在于，所述根据 CDR 中的信息

获取所述 CDR 的计费属性的步骤包括:

判断所述 CDR 中是否包含直接隧道标识，若包含，则确定所述 CDR 的中的所有流量节点的属性均为单隧道，若不包含，则确定所述 CDR 中所有的流量节点的属性均为双隧道。

7、根据权利要求 3 所述的方法，其特征在于，所述根据 CDR 中的信息获取所述 CDR 的计费属性的步骤包括:

判断所述 CDR 中包含的直接隧道标识的数值是否为预置数值，若是，则确定所述 CDR 的中的所有流量节点的属性均为单隧道，若不是，则确定所述 CDR 中所有的流量节点的属性均为双隧道。

8、根据权利要求 4 所述的方法，其特征在于，所述根据 CDR 中的信息获取所述 CDR 的计费属性的步骤包括:

判断所述 CDR 中的流量节点标识字段中是否包含直接隧道标识，若包含，则确定该流量节点标识对应的流量节点的属性为单隧道，若不包含，则确定该流量节点标识对应的流量节点的属性为双隧道。

9、根据权利要求 5 所述的方法，其特征在于，所述根据 CDR 中的信息获取所述 CDR 的计费属性的步骤包括:

判断所述 CDR 中的流量节点标识字段中包含的直接隧道标识的数值是否为预置数值，若是，则确定该流量节点标识对应的流量节点的属性为单隧道，若不是，则确定该流量节点标识对应的流量节点的属性为双隧道。

10、根据权利要求 2 至 9 中任一项所述的方法，其特征在于，所述 GSN 为服务 GSN 或者网关 GSN;

当所述 GSN 为服务 GSN 时，所述 CDR 为 S-CDR;

当所述 GSN 为网关 GSN 时，所述 CDR 为 G-CDR。

11、根据权利要求 10 所述的方法，其特征在于，所述 CDR 为 S-CDR;

所述根据 CDR 中的信息获取所述 CDR 的计费属性的步骤之前包括:

计费中心接收网关通用分组无线服务支持节点 GGSN 发送的 GGSN 计费

数据记录 G-CDR;

根据当前会话的计费标识以及 GGSN 互联网地址查询对应的 S-CDR 以及 G-CDR;

从所述 S-CDR 中获取第一数据流量以及 G-CDR 中获取第二数据流量;

判断所述第一数据流量与所述第二数据流量之间的差值是否满足预置条件，若是，则执行计费的操作。

12、根据权利要求 10 所述的方法，其特征在于，所述根据 CDR 以及其计费属性进行计费的步骤包括:

查询与所述 CDR 的计费属性对应的计费规则;

根据所述计费规则以及 CDR 对当前会话进行计费。

13、根据权利要求 11 所述的方法，其特征在于，当所述 S-CDR 的计费属性为单隧道时，

判断所述当前会话的服务质量参数或者费率参数是否发生变更，若变更，则根据所述变更后的服务质量参数或费率参数在所述 S-CDR 中生成新的流量节点。

14、一种通用分组无线服务支持节点，用于接收并传送终端通过基站子系统传输的通信数据，并与计费网关相连进行计费处理，其特征在于，包括:

会话信息获取单元，用于获取当前会话信息，从所述会话信息中提取当前会话的计费属性;

CDR 封装单元，用于将所述计费属性携带于每一个 CDR 中，所述计费属性用户指示所述 CDR 的隧道相关信息;

CDR 发送单元，用于向计费网关发送所述携带计费属性的 CDR。

15、根据权利要求 14 所述的 GSN，其特征在于，所述 CDR 封装单元包括:

第一封装单元，用于在所述 CDR 中设置直接隧道标识用于指示所述 CDR 中所有的流量节点的属性均为单隧道; 或

第二封装单元，用于在所述 CDR 中设置直接隧道标识，当所述 CDR 中所有的流量节点的属性均为单隧道，将所述直接隧道标识的数值设置为预置的数值；或

第三封装单元，用于在所述 CDR 中某个流量节点字段中设置直接隧道标识用于指示所述流量节点的属性均为单隧道；或

第四封装单元，用于在所述 CDR 中某个流量节点字段中设置直接隧道标识，当所述流量节点的属性均为单隧道，将所述直接隧道标识的数值设置为预置的数值。

16、根据权利要求 14 所述的 GSN，其特征在于，

当所述 GSN 为服务 GSN 时，所述 CDR 封装单元将所述计费属性携带于每一个 S-CDR 中，所述 CDR 发送单元向计费网关发送所述携带计费属性的 S-CDR;

当所述 GSN 为网关 GSN 时，所述 CDR 封装单元将所述计费属性携带于每一个 G-CDR 中，所述 CDR 发送单元向计费网关发送所述携带计费属性的 G-CDR。

17、根据权利要求 16 所述的 GSN，其特征在于，所述 GSN 还包括:

流量节点生成单元，用于当所述 CDR 的计费属性为单隧道时，判断所述当前会话的服务质量参数或者费率参数是否发生变更，若变更，则根据所述变更后的服务质量参数或费率参数在所述 CDR 中生成新的流量节点。

18、一种计费中心，其特征在于，包括:

话单接收单元，用于接收 CDR;

计费属性获取单元，用于根据接收到的 CDR 中的信息获取所述 CDR 的计费属性，所述计费属性用于指示所述 CDR 的隧道相关信息;

计费规则查询单元，用于根据所述计费属性查询对应的计费规则;

计费单元，用于根据所述计费规则以及 CDR 对当前会话进行计费。

19、根据权利要求 18 所述的计费中心，其特征在于，所述计费属性获取

单元包括:

第一获取单元，用于判断所述 CDR 中是否包含直接隧道标识，若包含，则确定所述 CDR 的中的所有流量节点的属性均为单隧道，若不包含，则确定所述 CDR 中所有的流量节点的属性均为双隧道;

或

第二获取单元，用于判断所述 CDR 中包含的直接隧道标识的数值是否为预置数值，若是，则确定所述 CDR 的中的所有流量节点的属性均为单隧道，若不是，则确定所述 CDR 中所有的流量节点的属性均为双隧道;

或

第三获取单元，用于判断所述 CDR 中的流量节点标识字段是否包含直接隧道标识，若包含，则确定该流量节点标识对应的流量节点的属性为单隧道，若不包含，则确定该流量节点标识对应的流量节点的属性为双隧道;

或

第四获取单元，用于判断所述 CDR 中的流量节点标识字段中包含的直接隧道标识的数值是否为预置数值，若是，则确定该流量节点标识对应的流量节点的属性为单隧道，若不是，则确定该流量节点标识对应的流量节点的属性为双隧道。

一种计费控制方法及计费中心以及相关设备

技术领域

本发明涉及通讯领域，尤其涉及一种计费控制方法及计费中心以及相关设备。

背景技术

在现有的计费网络结构中，服务通用分组无线服务支持节点（SGSN，Serving General packet radio service Support Node）和网关 GPRS 支持节点（GGSN，Gateway GPRS Support Node）都是通过 Ga 接口与计费网关（CGF，Charging Gateway Functionality）相连，当用户开始会话时，SGSN 和 GGSN 都会针对该会话分别生成 SGSN 计费数据记录（S-CDR，SGSN Charging Data Record）以及 GGSN 计费数据记录（G-CDR，GGSN Charging Data Record），并通过 Ga 接口发送至 CGF，CGF 对两个话单进行合并后送至计费中心进行计费。

在上述过程中，当用户开始会话时，分组数据协议（PDP，Packet Data Protocol）将会被激活，具体 PDP 被激活的方式有两种，一种是激活双隧道 Two Tunnels 的 PDP，另外一种是激活单隧道 One Tunnel 的 PDP，其中，后者 PDP 的用户面是直接在无线网络控制器（RNC，Radio Network Controller）与 GGSN 之间建立 GPRS 隧道协议（GTP，GPRS Tunnelling Protocol）隧道，而不经过 SGSN，但激活 Two Tunnels 的 PDP 的用户面隧道则分为两段，一段是从 RNC 到 SGSN，另外一段是从 SGSN 到 GGSN。

在具体应用过程中，根据用户所使用的具体业务的不同，被激活的 PDP 有可能会在 One Tunnel 方式和 Two Tunnels 之间进行切换，而计费中心需要知道接收到的话单对应的 PDP 被激活的方式才能够进行精确的计费。

现有技术中一种计费控制方法为：在 S-CDR 中的流量节点（List of Traffic Data Volumes）字段中的 Change Condition 字段中增添一个参数 Direct Tunnel establishment/removal，其中 Direct Tunnel 即表示 One Tunnel，该参数用于表

示后续话单对应的 PDP 被激活的方式，当 One Tunnel 被建立时生成一个流量节点，其中的 Change Condition 字段中包含参数 Direct Tunnel establishment，表示 One Tunnel 已经建立，当 One Tunnel 被释放时再生成一个流量节点，其中的 Change Condition 字段中包含参数 Direct Tunnel removal，表示 One Tunnel 已经被释放，则中间部分的话单并不需要携带这些信息，例如一共有 6 个 S-CDR，当 One Tunnel 建立时，在第一个 S-CDR 中携带 Direct Tunnel establishment，假设发送前三个 S-CDR 时均为 One Tunnel 方式，则计费中心接收到第二个和第三个 S-CDR 时，判断前面并未接收到包含 Direct Tunnel removal 的 S-CDR，则判定第二个和第三个 S-CDR 为 One Tunnel 方式，若发送第四个 S-CDR 时，激活方式发生了变化，则在第四个 S-CDR 中携带参数 Direct Tunnel removal，计费中心接收到第五个和第六个 S-CDR 时，判断前面接收到了携带 Direct Tunnel removal 的 S-CDR，则判定第五个和第六个 S-CDR 为 Two Tunnels 方式。

但是，在上述现有技术中，只有当激活方式发生变化，即从 One Tunnel 方式到 Two Tunnels 方式，或从 Two Tunnels 到 One Tunnel 时，才会在 S-CDR 中携带用于表示当前 S-CDR 属性的参数 Direct Tunnel establishment/removal，而其他 S-CDR 则不会携带，例如上面所说的第二个，第三个，第五个以及第六个 S-CDR 均不会携带这个参数，所以一旦携带参数 Direct Tunnel establishment/removal 的 S-CDR 发生错误，导致计费中心没有接收到该 S-CDR，或者是接收失败，则会导致后续一系列的 S-CDR 的属性产生错位，即导致一连串的错误，从而严重地影响了计费的精确性。

发明内容

本发明实施例提供了一种计费控制方法及计费中心以及相关设备，能够提高计费的精确性。

本发明实施例提供的计费控制方法，包括：通用分组无线服务支持节点 GSN 获取当前会话的计费属性；将所述计费属性携带于每一个 GSN 计费数据记录 CDR 中，所述计费属性用于指示所述 CDR 的隧道相关信息；向计费中心发送所述 CDR；计费中心根据所述 CDR 中的信息获取所述 CDR 的计费属性；计费中心根据所述 CDR 以及其计费属性进行计费。

本发明实施例提供的通用分组无线服务支持节点，用于接收并传送终端通过基站子系统传输的通信数据，并与计费网关相连进行计费处理，包括：会话信息获取单元，用于获取当前会话信息，从所述会话信息中提取当前会话的计费属性；CDR 封装单元，用于将所述计费属性携带于每一个 CDR 中，所述计费属性用户指示所述 CDR 的隧道相关信息；CDR 发送单元，用于向计费网关发送所述携带计费属性的 CDR。

本发明实施例提供的计费中心，包括：话单接收单元，用于接收 CDR；计费属性获取单元，用于根据接收到的 CDR 中的信息获取所述 CDR 的计费属性，所述计费属性用于指示所述 CDR 的隧道相关信息；计费规则查询单元，用于根据所述计费属性查询对应的计费规则；计费单元，用于根据所述计费规则以及 CDR 对当前会话进行计费。

从以上技术方案可以看出，本发明实施例具有以下优点：

本发明实施例中，由于 GSN 在每一个 CDR 都设置有用于指示该 CDR 隧道相关信息的计费属性，所以可以直接根据该 CDR 获取得到对应的计费属性，从而根据该计费属性进行计费，所以当出现某个 CDR 丢失，或接收错误的情况时，并不会影响计费过程中对其他的 CDR 的计费属性的判断，所以能够降低 CDR 错误对计费的影响，从而提高了计费的精确性。

附图说明

图 1 为本发明实施例中计费控制方法实施例流程图；

图 2 为本发明实施例中通讯系统实施例示意图；

图 3 为本发明实施例中 SGSN 实施例示意图；

图 4 为本发明实施例中计费中心实施例示意图。

具体实施方式

本发明实施例提供了一种计费控制方法及计费中心以及相关设备，用于提高计费的精确性。

本发明实施例中，由于 GSN 在每一个 CDR 都设置有用于指示该 CDR 隧道相关信息的计费属性，所以可以直接根据该 CDR 获取得到对应的计费属性，

从而根据该计费属性进行计费，所以当出现某个 CDR 丢失，或接收错误的情况时，并不会影响计费过程中对其他的 CDR 的计费属性的判断，所以能够降低 CDR 错误对计费的影响，从而提高了计费的精确性。

下面首先对本发明实施例中的计费控制方法实施例进行说明，本发明实施例中，GSN 既可以是 SGSN，也可以是 GGSN，则生成的 CDR 分别是 S-CDR 和 G-CDR，由于具体生成 CDR 的过程类似，所以下面的实施例中以 GSN 为 SGSN 为例进行说明，可以理解的是，同样可以为 GGSN，处理流程类似，请参阅图 1，本发明实施例中计费控制方法实施例包括：

101、SGSN 获取当前会话的计费属性；

当用户开始进行会话之后，则会激活 PDP，具体激活 PDP 的方式有两种，一种是单隧道方式（One Tunnel），另外一种是双隧道方式（Two Tunnels），本实施例中将这两种方式作为 S-CDR 中的流量节点的属性，即流量节点的属性为 One Tunnel 或 Two Tunnels，在用户会话的过程中，SGSN 可以通过其他外部网元（例如 RNC）或自身确定当前会话过程中的计费属性，其中，该计费属性用于指示该 S-CDR 的隧道相关信息，除该计费属性之外，还可以获取其他计费相关信息（例如计费标识，PDP 激活时间，用户位置信息，GGSN 的 IP 地址、话单的持续时间等信息），具体过程为：当用户进行会话之后，SGSN 根据该会话的标识获取对应的会话信息，该会话信息中包含有当前的计费属性。SGSN 获取会话信息的过程为现有技术，此处不再赘述。

102、将计费属性携带于 S-CDR 中；

本实施例中，当 SGSN 需要向计费中心发送 S-CDR 时即会获取当前会话信息，并从会话信息中获取计费属性，将获取到的计费属性携带于 S-CDR 中，该步骤的具体实现方式在本发明实施例中有多种，下面具体介绍：

携带方式大致可以分为两类：

一、直接将计费属性携带于 S-CDR 中：

这种方式中，直接在现有的 S-CDR 数据格式中扩展一个字段 Direct Tunnel Flag，用于指示计费属性中的隧道相关信息，在这种方式下若该计费属性为 One Tunnel，则表示该 S-CDR 中的所有流量节点的属性均为 One Tunnel，若

该计费属性为 Two Tunnels，则表示该 S-CDR 中的所有流量节点的属性均为 Two Tunnel，具体的指示方式也分为两种：

1、采用字段的携带情况标识计费属性：

在此方式中，若 S-CDR 中携带了该字段 Direct Tunnel Flag，则表示该 S-CDR 的计费属性为 One Tunnel，即该 S-CDR 中的所有流量节点的属性均为 One Tunnel，若不携带该字段 Direct Tunnel Flag，则表示该 S-CDR 的计费属性为 Two Tunnels，即该 S-CDR 中的所有流量节点的属性均为 Two Tunnels。

在此方式中，字段 Direct Tunnel Flag 不需要有具体的数值，仅通过其是否存在来确定计费属性。

2、采用字段的数值标识计费属性：

在此方式中，字段 Direct Tunnel Flag 需要被赋值才能够判断计费属性，即每一个 S-CDR 均携带字段 Direct Tunnel Flag，只是不同计费属性的 S-CDR 中字段 Direct Tunnel Flag 的数值不同，例如可以约定数值为 1 时表示计费属性为 One Tunnel，即该 S-CDR 中的所有流量节点的属性均为 One Tunnel，其他数值则表示计费属性为 Two Tunnels，即该 S-CDR 中的所有流量节点的属性均为 Two Tunnels。可以理解的是，本实施例仅以一个例子进行说明，在实际应用中，该数值可以根据实际情况进行约定，此处不做限定。

二、通过 S-CDR 中的 List of Traffic Data Volumes 字段标识计费属性：

这种方式中的计费属性体现于 S-CDR 中每一个流量节点的属性，即在现有的 S-CDR 数据格式 List of Traffic Data Volumes 字段中的扩展一个字段 Direct Tunnel Flag，用于指示该流量节点的属性，需要说明的是，原 List of Traffic Data Volumes 字段中包含四个参数，分别是数据卷上行（Data Volume Uplink），数据卷下行（Data Volume Downlink），切换条件（Change Condition）以及切换时间（Change Time），具体的通过 Direct Tunnel Flag 指示计费属性的方式也分为两种：

1、采用字段的携带情况标识流量节点的属性：

在此方式中，若 S-CDR 中的 List of Traffic Data Volumes 字段中携带了该

字段 Direct Tunnel Flag，则表示该流量节点的属性为 One Tunnel，若不携带该字段 Direct Tunnel Flag，则表示该流量节点的属性为 Two Tunnels。

在此方式中，字段 Direct Tunnel Flag 不需要有具体的数值，仅通过其是否存在来确定流量节点的属性。

2、采用字段的数值标识流量节点的属性:

在此方式中，字段 Direct Tunnel Flag 需要被赋值才能够判断流量节点的属性，即是 S-CDR 中每一个的 List of Traffic Data Volumes 字段中均携带字段 Direct Tunnel Flag，只是不同属性的流量节点中的字段 Direct Tunnel Flag 的数值不同，例如可以约定数值为 1 时表示流量节点的属性为 One Tunnel，其他数值则表示流量节点的属性为 Two Tunnels。可以理解的是，本实施例仅以一个例子进行说明，在实际应用中，该数值可以根据实际情况进行约定，此处不做限定。

上述仅以四个具体实现方式对将计费属性携带于 S-CDR 中的情况进行了说明，可以理解的是，在实际应用过程中，除上述方式之外，还可以采取其他的方式将计费属性携带于 S-CDR 中，只要能够实现将计费属性携带于 S-CDR 中即可，实现手段此处不做限定。

需要说明的是，若 S-CDR 的计费属性为单隧道，则 SGSN 需要对当前会话进行监控，判断当前会话的服务质量参数或者费率参数是否发生变化，若发生变化，则需要根据变更后的服务质量参数或费率参数在 S-CDR 中生成新的流量节点。

103、将 S-CDR 发送至 CGF;

当 SGSN 将计费属性携带于 S-CDR 之后，则可以将该 S-CDR 发送至 CGF 进行下一步处理。

104、GGSN 将 G-CDR 发送至 CGF;

本实施例中，为能实现后续的计费，除了需要 SGSN 生成的 S-CDR 之外，还需要 GGSN 生成的 G-CDR，需要说明的是，GGSN 生成 G-CDR 的过程以及 GGSN 将 G-CDR 发送至 CGF 的过程均为现有技术，此处不再赘述。

本实施例中是以 SGSN 作为 GSN 的例子进行说明，可以理解的是，若以 GGSN 作为 GSN 的例子进行说明，则此步骤则为“SGSN 将 S-CDR 发送至 CGF”。

105、计费网管对 S-CDR 以及 G-CDR 进行合并后发送至计费中心;

106、计费中心判断接收到的 S-CDR 以及 G-CDR 之间的流量差值是否满足预置条件，若是，则执行步骤 107，若否，则执行步骤 110;

具体判断方法为:

计费中心根据当前会话的计费标识以及 GGSN 互联网地址查询对应的 S-CDR 以及 G-CDR，需要说明的是，S-CDR 以及 G-CDR 中都包含当前会话的计费标识以及 GGSN 的 IP 地址，即计费中心查询与当前的会话计费表示以及 GGSN 的 IP 地址相同的 S-CDR 以及 G-CDR;

从查询到的 S-CDR 中获取第一数据流量以及从查询到的 G-CDR 中获取第二数据流量;

判断第一数据流量与所述第二数据流量之间的差值是否满足预置条件，若是，则执行计费的操作。

本实施例中的预置条件可以为一个具体的数值，即表示第一数据流量与第二数据流量的差值是否小于某个数值，若小于，则进行计费，若否，则执行步骤 110。

107、计费中心从 S-CDR 中获取计费属性;

当 S-CDR 中的第一数据流量与 G-CDR 中的第二数据流量之间的差值小于某个预置数值时，则计费中心从 S-CDR 中获取计费属性，根据计费属性携带的方式的不同，具体获取计费属性的方式包括:

一、直接从 S-CDR 中获取计费属性:

这种方式中，直接根据接收到的 S-CDR 数据格式中的字段 Direct Tunnel Flag 获取计费属性，具体的获取方式也分为两种:

1、采用字段的携带情况获取计费属性:

在此方式中，若 S-CDR 中携带了该字段 Direct Tunnel Flag，则表示该 S-CDR 的计费属性为 One Tunnel，即该 S-CDR 中的所有流量节点的属性均为 One Tunnel，若不携带该字段 Direct Tunnel Flag，则表示该 S-CDR 的计费属性为 Two Tunnels，即该 S-CDR 中的所有流量节点的属性均为 Two Tunnels。

在此方式中，字段 Direct Tunnel Flag 不需要有具体的数值，仅通过其是否存在来确定计费属性。

2、采用字段的数值获取计费属性:

在此方式中，需要获取字段 Direct Tunnel Flag 的数值才能够获取计费属性，即是每一个 S-CDR 均携带字段 Direct Tunnel Flag，只是不同计费属性的 S-CDR 中字段 Direct Tunnel Flag 的数值不同，例如可以约定数值为 1 时表示计费属性为 One Tunnel，其他数值则表示计费属性为 Two Tunnels。可以理解的是，本实施例仅以一个例子进行说明，在实际应用中，该数值可以根据实际情况进行约定，此处不做限定。

二、从 S-CDR 中的 List of Traffic Data Volumes 字段中获取计费属性:

这种方式中，S-CDR 的计费属性体现于该 S-CDR 中每一个流量节点的属性，即从接收到的 S-CDR 数据格式中读取 List of Traffic Data Volumes 字段，并根据该字段中的字段 Direct Tunnel Flag 获取该流量节点的属性，得到该 S-CDR 中所有的流量节点的属性后即可获知该 S-CDR 的计费属性，具体的获取方式也分为两种:

1、采用字段的携带情况获取流量节点的属性:

在此方式中，若 S-CDR 中的 List of Traffic Data Volumes 字段中携带了该字段 Direct Tunnel Flag，则表示该流量节点的属性为 One Tunnel，若不携带该字段 Direct Tunnel Flag，则表示该流量节点的属性为 Two Tunnels。

在此方式中，字段 Direct Tunnel Flag 不需要有具体的数值，仅通过其是否存在来确定计费属性。

2、采用字段的数值获取流量节点的属性:

在此方式中，需要获取字段 Direct Tunnel Flag 的数值才能获取流量节点

的属性，即每一个 S-CDR 中的 List of Traffic Data Volumes 字段中均携带字段 Direct Tunnel Flag，只是不同属性的流量节点中的字段 Direct Tunnel Flag 的数值不同，例如可以约定数值为 1 时表示流量节点的属性为 One Tunnel，其他数值则表示流量节点的属性为 Two Tunnels。可以理解的是，本实施例仅以一个例子进行说明，在实际应用中，该数值可以根据实际情况进行约定，此处不做限定。

上述仅以四个具体实现方式获取 S-CDR 中的计费属性，可以理解的是，在实际应用过程中，除上述方式之外，还可以采取其他的方式从 S-CDR 中获取计费属性，实现手段此处不做限定。

108、查询与计费属性对应的计费规则；

当计费中心获取了计费属性后，根据该计费属性查询对应的计费规则，例如针对计费属性为 One Tunnel（即表示该 S-CDR 中所有的流量节点的属性都是 One Tunnel）的 S-CDR 以及计费属性为 Two Tunnels（即表示该 S-CDR 中所有的流量节点的属性都是 Two Tunnels）的 S-CDR，将分别采取不同的计费策略，具体的计费策略为现有技术，此处不做限定。

109、根据计费规则，S-CDR 以及 G-CDR 进行计费，并结束流程；

当计费中心查询到了对应的计费策略后，即可根据该计费策略，并结合接收到的 S-CDR 以及 G-CDR 对当前会话进行计费，需要说明的是，计费还可以使用获取到的计费相关信息，例如计费标识，PDP 激活时间，用户位置信息，GGSN 的 IP 地址、话单的持续时间等信息。

110、执行异常处理流程。

当 S-CDR 中的第一数据流量与 G-CDR 中的第二数据流量的差值不满足预置条件时，例如该差值大于预置门限，则执行异常处理流程，具体可以为：请求 CGF 重新发送 S-CDR 以及 G-CDR，还可以为：提示出错并结束流程，可以理解的是，同样可以是其他类型的异常处理流程。

本发明实施例中，由于 GSN 在每一个 CDR 都设置有用于指示该 CDR 隧道相关信息的计费属性，所以可以直接根据该 CDR 获取得到对应的计费属性，从而根据该计费属性进行计费，所以当出现某个 CDR 丢失，或接收错误的情

况时，并不会影响计费过程中对其他的 CDR 的计费属性的判断，所以能够降低 CDR 错误对计费的影响，从而提高了计费的精确性。

下面请参阅图 2，本发明实施例中的通讯系统实施例包括：

SGSN201，用于获取当前会话的计费属性，并将所述计费属性携带于每一个 S-CDR 中，向计费中心 202 发送所述 S-CDR；

计费中心 202，用于接收 SGSN201 发送的 S-CDR，根据所述 S-CDR 中的信息获取所述 S-CDR 的计费属性（所述计费属性用于指示所述 S-CDR 的隧道相关信息），根据所述 S-CDR 以及其计费属性进行计费。

本实施例中的通讯系统还可以进一步包括：

GGSN203，用于向计费中心 202 发送 G-CDR，所述 G-CDR 中携带计费属性，该计费属性指示该 G-CDR 的隧道相关信息。

本实施例中的通讯系统还可以进一步包括：

计费网关 204，用于接收 SGSN 发送的 S-CDR 以及 GGSN 发送的 G-CDR，对接收到的 S-CDR 以及 G-CDR 进行合并，并将合并后话单发送至计费中心。

请参阅图 3，本发明实施例中 GSN 实施例包括：

会话信息获取单元 301，用于获取当前会话信息，从所述会话信息中提取当前会话的计费属性；

CDR 封装单元 302，用于将所述计费属性携带于每一个 CDR 中，所述计费属性用于指示所述 CDR 的隧道相关信息；

CDR 发送单元 303，用于向计费网关发送所述携带计费属性的 CDR。

本实施例中，CDR 封装单元 302 还可以进一步包括：

第一封装单元，用于在所述 CDR 中设置直接隧道标识用于指示所述 S-CDR 中所有的流量节点的属性均为单隧道；

或

第二封装单元，用于在所述 CDR 中设置直接隧道标识，当所述 CDR 中所有的流量节点的属性均为单隧道，将所述直接隧道标识的数值设置为预置

的数值;

或

第三封装单元，用于在所述 CDR 中某个流量节点字段中设置直接隧道标识用于指示所述流量节点的属性均为单隧道;

或

第四封装单元，用于在所述 CDR 中某个流量节点字段中设置直接隧道标识，当所述流量节点的属性均为单隧道，将所述直接隧道标识的数值设置为预置的数值。

需要说明的是，当所述 GSN 为 SGSN 时，所述 CDR 封装单元 302 将所述计费属性携带于每一个 S-CDR 中，所述 CDR 发送单元 303 向计费网关发送所述携带计费属性的 S-CDR;

当所述 GSN 为 GGSN 时，所述 CDR 封装单元 302 将所述计费属性携带于每一个 G-CDR 中，所述 CDR 发送单元 303 向计费网关发送所述携带计费属性的 G-CDR。

本实施例中，该 GSN 还可以进一步包括:

流量节点生成单元，用于当所述 CDR 的计费属性为单隧道时，判断所述当前会话的服务质量参数或者费率参数是否发生变更，若变更，则根据所述变更后的服务质量参数或费率参数在所述 CDR 中生成新的流量节点。

请参阅图 4，本发明实施例中计费中心实施例包括:

话单接收单元 401，用于接收 CDR 以及 CDR;

计费属性获取单元 402，用于根据接收到的 CDR 中的信息获取所述 CDR 的计费属性，所述计费属性用于指示所述 CDR 的隧道相关信息;

计费规则查询单元 403，用于根据所述计费属性查询对应的计费规则;

计费单元 404，用于根据所述计费规则以及 CDR 对当前会话进行计费。

本实施例中，计费属性获取单元 402 还可以进一步包括:

第一获取单元，用于判断所述 CDR 中是否包含直接隧道标识，若包含，

则确定所述 CDR 的中的所有流量节点的属性均为单隧道，若不包含，则确定所述 CDR 中所有的流量节点的属性均为双隧道；

或

第二获取单元，用于判断所述 CDR 中包含的直接隧道标识的数值是否为预置数值，若是，则确定所述 CDR 的中的所有流量节点的属性均为单隧道，若不是，则确定所述 CDR 中所有的流量节点的属性均为双隧道；

或

第三获取单元，用于判断所述 CDR 中的流量节点标识字段是否包含直接隧道标识，若包含，则确定该流量节点标识对应的流量节点的属性为单隧道，若不包含，则确定该流量节点标识对应的流量节点的属性为双隧道；

或

第四获取单元，用于判断所述 CDR 中的流量节点标识字段中包含的直接隧道标识的数值是否为预置数值，若是，则确定该流量节点标识对应的流量节点的属性为单隧道，若不是，则确定该流量节点标识对应的流量节点的属性为双隧道。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括如下步骤：GSN 获取当前会话的计费属性；将所述计费属性携带于每一个 GSN 计费数据记录 CDR 中，所述计费属性用于指示所述 CDR 的隧道相关信息；向计费中心发送所述 CDR；计费中心根据所述 CDR 中的信息获取所述 CDR 的计费属性；计费中心根据所述 CDR 以及其计费属性进行计费。

上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上对本发明所提供的一种计费控制方法及计费中心以及相关设备进行了详细介绍，对于本领域的一般技术人员，依据本发明实施例的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

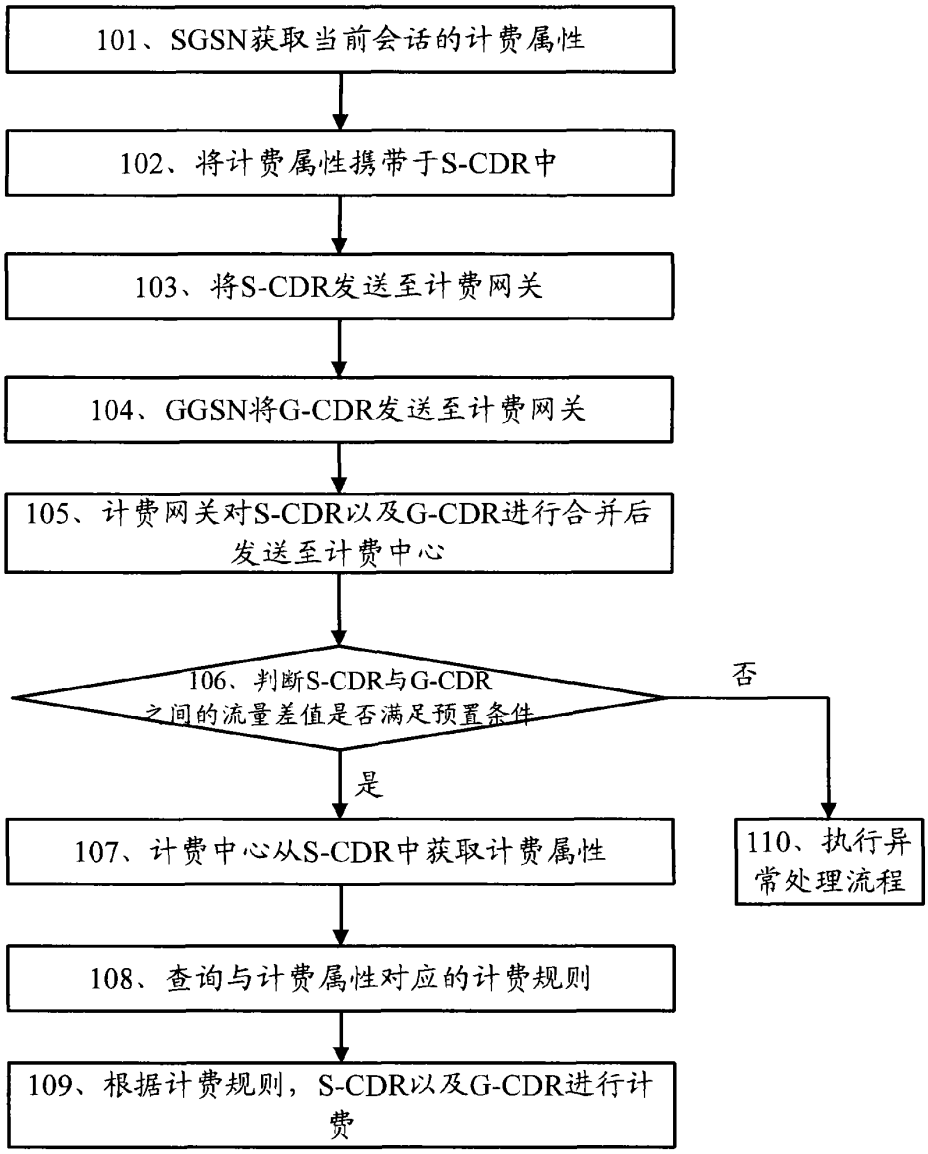

101、SGSN获取当前会话的计费属性
102、将计费属性携带于S-CDR中
103、将S-CDR发送至计费网关
104、GGSN将G-CDR发送至计费网关
105、计费网关对S-CDR以及G-CDR进行合并后发送至计费中心
106、判断S-CDR与G-CDR之间的流量差值是否满足预置条件
否
是
107、计费中心从S-CDR中获取计费属性
110、执行异常处理流程
108、查询与计费属性对应的计费规则
109、根据计费规则，S-CDR以及G-CDR进行计费

图 1

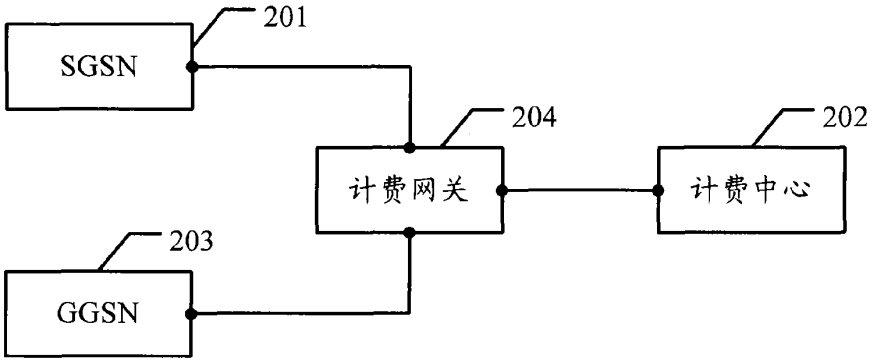

201
SGSN
204
202
计费网关
计费中心
203
GGSN

图 2


301
会话信息获取单元
302
CDR封装单元
303
CDR发送单元

图 3

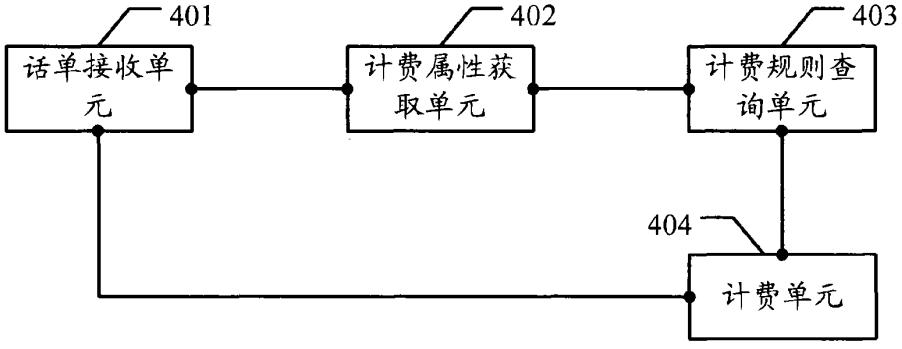

401
话单接收单元
402
计费属性获取单元
403
计费规则查询单元
404
计费单元

图 4

Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Charging control method, charging center and related equipment

CN 101183958 A

Publication number	CN101183958 A
Publication type	Application
Application number	CN 200710302140
Publication date	May 21, 2008
Filing date	Dec 14, 2007
Priority date	Dec 14, 2007
Inventors	靖 陈, 石迎生, 袁潮灏
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Classifications (2), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT translated from Chinese

The present invention discloses a method for controlling charging and billing center and related apparatus for improving the accuracy of charging. The method of the present invention comprises: a general packet radio service support node GSN receives charging properties of the current session; carried on the charging property of said charging attribute carried in each CDR, the charging property is used to indicate the CDR said tunnel-related information; transmitting the CDR to the billing center; the CDR billing center to acquire the property in accordance with the CDR billing information; billing center for billing based on the CDR and its billing property . The present invention also provides the billing center and related equipment. The present invention can effectively improve the accuracy of charging.

DESCRIPTION translated from Chinese

A charging control method, and the Charging Center and associated equipment

[0001] Technical Field

[0002] The present invention relates to the field of communications, particularly to a method for controlling charging and billing center and related equipment.

[0003] BACKGROUND

[0004] In the conventional charging network architecture, a serving general packet radio service support node (SGSN, Serving General packet radio service Support Node) and a gateway GPRS support node (GGSN, Gateway GPRS Support Node) through Ga interface charging gateway (CGF, Charging Gateway Functionality) connected, when a user starts a session, SGSN SGSN and GGSN are separately generate charging data records (S-CDR, SGSN Charging DataRecord) and GGSN charging data record (for the session G-CDR, GGSN Charging Data Record), and sent to the billing center for billing after sending via Ga interface to the CGF, CGF bill to merge the two.

[0005] In the above process, when a user starts a session, packet data protocol (PDP, Packet DataProtocol) will be activated, depending PDP is activated in two ways, one is double tunnel Two Tunnels activate the PDP, in addition One is the activation of a single tunnel One Tunnel of PDP, where the user plane which is established between the GGSN PDP directly in the radio network controller (RNC, Radio Network Controller) GPRS Tunneling Protocol (GTP, GPRS Tunnelling Protocol) tunnel, without passing through the SGSN, but the activation of the PDP Two Tunnels user plane tunnel is divided into two sections, a section from the RNC to SGSN, another section from the SGSN to GGSN.

[0006] In a specific application process, depending on the user's specific business use, is active PDP there may be between the Two Tunnels One Tunnel mode and switch, and billing center needs to know if the single received corresponding PDP is a way to be able to activate the precise accounting.

[0007] A charging control prior art methods: the S-CDR in traffic node (List of TrafficData Volumes) field Change Condition field to add a parameter Direct

CLAIMS (19) translated from Chinese

1. A charging control method characterized by comprising:

General Packet Radio Service Support Node GSN charging property to obtain the current session;

The charging property is carried in each GSN billing data record CDR, the CDR charging attribute for indicating the tunnel related information;

Sending the CDR to the billing center;

The billing center to obtain the properties of the CDR of charging information according to the CDR;

Accounting center for billing billing according to the CDR and its properties.

2. A method according to claim 1, characterized in that the charging properties of each of said steps is carried in the CDR comprises:

Set direct tunnel in identifying attributes of the CDR indicates that the CDR in all traffic nodes for both single tunnel

3. The method according to claim 1, characterized in that the charging properties of each of said steps is carried in the CDR comprises:

Set directly in the tunnel identification CDR;

If the property CDR in all traffic nodes are single tunnel, the value set for the direct tunnel identification will be the preset value.

4. The method according to claim 1, characterized in that the charging properties of each of said steps is carried in the CDR comprises:

CDR settings directly in a tunnel in the field of traffic node identifier property indicating the flow node for all single tunnel.

5. The method according to claim 1, characterized in that the charging properties of each of said steps is carried in the CDR comprises:

Set direct tunnel identified in the CDR in a traffic node field;

Tunnelestablishment / removal, which means that the One Direct Tunnel Tunnel, this parameter is used to indicate the way PDP is activated if a single follow-up correspondence to generate a flow node when the One Tunnel was built, where the Change Condition field contains parameters Direct Tunnel establishment, expressed One Tunnel has been established, when the One Tunnel and then generate a flow node when it is released, which Change Condition field contains parameters Direct Tunnel removal, expressed One Tunnel has been released, the middle part of the bill does not need to carry this information, for example, a total of six S-CDR, when When the One Tunnel is established, the first one carrying the Direct Tunnelestablishment S-CDR, and when the transmission of the first three S-CDR are the One Tunnel mode, the accounting center receives the second and third S-CDR hypothesis, Analyzing the front does not receive containing Direct Tunnelremoval the S-CDR, it is determined that the second and third S-CDR of One Tunnel mode, if transmitting a fourth S-CDR, activation changes, in the first When the four S-CDR carries parameter Direct Tunnel removal, billing center receives the fifth and sixth S-CDR, judge previously received a portable Direct Tunnel removal of S-CDR, it is determined that the fifth and sixth an S-CDR for Two Tunnels way.

[0008] However, in the prior art, is activated only when the mode changes from mode to the Two Tunnels One Tunnel mode, or from the Two Tunnels to the One Tunnel, will be carried in the S-CDR is used to represent the current Direct S-CDR parameters attribute Tunnel establishment / removal, and other S-CDR is not portable, such as the above mentioned second, third, fifth, and sixth S-CDR will not carry the parameters, the parameters once carrying Direct Tunnelestablishment / removal of the S-CDR error occurred is not received in the billing center S-CDR, or a reception failure, a subsequent series of S-CDR result in misalignment of the properties, i.e., leading to a series of errors, which seriously affected the billing accuracy.

[0009] SUMMARY

[0010] The present embodiment of the invention there is provided a method for controlling charging and billing center and related equipment, can improve the accuracy of charging.

Charging control method according to an embodiment [0011] The present invention, including: a general packet radio service support node GSN receives charging properties of the current session; carried on the charging property of each GSN billing data record CDR, and the said charging attribute is used to indicate the CDR tunnel related information; transmitting the CDR to the billing center; the billing center to obtain the properties of the CDR of charging according to the CDR information; billing center according to the CDR as well as its billing attributes for billing purposes.

[0012] embodiment of the present invention, a general packet radio service support node embodiments provide for receiving and transmitting terminal via the communication base station subsystem transfer the data, and the billing gateway for billing processing is connected, comprising: a session information acquiring unit, with for acquiring information of the current session, the current session charging attribute extracted from the session information; CDR packaging unit, for carrying on the charging property of each CDR in the charging attribute of the user to indicate the CDR tunnel-related information; CDR sending unit for sending the billing gateway carries charging attribute CDR.

[0013] The present embodiment provides the billing center, comprising: a bill receiving means for receiving a CDR; charging attribute acquisition unit for acquiring the charging CDR according to the received attribute information in the CDR, tunnel-related information for indicating the charging properties of the CDR's; charging rule query unit according to said charging attribute query corresponding charging rule; accounting unit, according to said charging rules and CDR billing for the current session.

If the properties of the flow nodes are single tunnel, the value set for the direct tunnel identification will be the preset value.

6. The method according to claim 2, wherein, wherein the step according to the information in the CDR of the CDR of charging attribute acquisition comprises:

The CDR is determined whether the identifier contains a direct tunnel, if included, determine the properties of the CDR's of all nodes are single traffic tunnels, if included, to determine the properties of the CDR in the nodes are all traffic double tunnel.

7. The method according to claim 3, wherein said step of CDR according to the information obtained in the CDR charging attributes include:

Direct tunnel identification value to determine whether the CDR contains the preset value, and if so, determine the properties of the CDR's of all nodes are single tunnel flow, if yes, it is determined that all of the traffic of the CDR attribute nodes are dual tunnel.

8. The method according to claim 4, wherein said step of CDR according to the information obtained in the CDR charging attributes include:

Analyzing the flow rate of the CDR node identifier field contains a direct tunnel ID, if included, to determine the properties of the flow corresponding to the flow rate of the node identifier of the node is a single tunnel, if not contained, determining that the traffic flow of the node corresponding to the node identifier The property is double tunnel.

9. The method according to claim 5, wherein said step of CDR according to the information obtained in the CDR charging attributes include:

Direct tunnel identification value to determine the flow rate of the CDR in a node ID field is included in the preset value, and if so, to determine the properties of the flow corresponding to the flow rate of the node identifier of the node is a single tunnel, if yes, it is determined that the traffic node identifying the node corresponding to the flow properties of the double tunnel.

10. A method according to any of claim 2-9, characterized in that the GSN or a service GSN gateway GSN;

When the GSN service GSN, the CDR is S-CDR;

When the gateway GSN GSN, the CDR for G-CDR.

11. The method according to claim 10, wherein said CDR is S-CDR;

The CDR according to the previous information acquiring step of CDR billing attributes include:

Accounting center receives a gateway general packet radio service support node GGSN GGSN sending the charging data records G-CDR;

Discover the corresponding S-CDR and G-CDR billing based on the current session identifier and GGSN Internet address;

Get the first G-CDR data traffic and data traffic from the acquisition in the second S-CDR;

Analyzing the difference between the first data and the second

[0014] As can be seen from the above technical solution, embodiments of the present invention has the following advantages:

[0015] The present embodiment of the invention, since the GSN in each CDR are provided with the properties of the CDR billing-related information for indicating the tunnel, it is possible to obtain direct access to the corresponding CDR according to the charging property, whereby the basis of the charging property for billing, so that when there is a missing CDR, or reception error occurs, the billing process does not affect the determination of the properties of the other CDR billing, it is possible to reduce the influence of the error on the charging CDR, thus improve the accuracy of charging.

[0016] Brief Description

[0017] Figure 1 is a flowchart of an embodiment of the invention the method of charging control;

[0018] Figure 2 embodiment of the present invention, a schematic diagram of the communication system according to the embodiment;

[0019] Example 3 is an embodiment schematic view of an embodiment of the SGSN;

[0020] Figure 4 is a schematic view of the invention embodiment the billing center embodiments.

[0021] Specific embodiments

[0022] The present embodiment of the invention there is provided a method for controlling charging and billing center and related apparatus for improving the accuracy of charging.

[0023] The present embodiment of the invention, since the GSN in each CDR are provided with the properties of the CDR billing-related information for indicating the tunnel, it is possible to obtain direct access to the corresponding CDR according to the charging property, whereby the basis of the charging property for billing, so that when there is a missing CDR, or reception error occurs, the billing process does not affect the determination of the properties of the other CDR billing, it is possible to reduce the influence of the error on the charging CDR, thus improve the accuracy of charging.

[0024] Hereinafter, the first embodiment of the present invention, the charge control method of the embodiment will be described below, embodiments of the present invention, GSN can be either SGSN, or may be GGSN, the resulting CDR are S-CDR and G-CDR Since the process is similar to the particular CDR is generated, so the following examples for the SGSN to the GSN as an example, it is understood that the same may be similar as the GGSN, the processing flow, see Figure 1, the embodiment of the present invention, the charge Control method of an embodiment comprises:

[0025] 101, SGSN charging property to obtain the current session;

[0026] When the user starts a session, it will activate the PDP, the specific activation of the PDP in two ways, one is a single tunnel mode (One Tunnel), the other is a double tunnel mode (Two Tunnels), this embodiment In these two modes as properties of the S-CDR flow node, that node is the flow properties or the One Tunnel Two Tunnels, during the user session, SGSN via other external network element (e.g. RNC) or self determine billing during the current session attributes, wherein the charging property is used to indicate that the S-CDR tunnel-related information, in addition to the charging property, you can also get other billing related information (such as billing identification, PDP activation time, user location information, IP address of the GGSN, and if the duration of a single message), the specific procedure is: when the user session, SGSN obtain the corresponding session according to the identification information of the session, the session information is included in the current billing property. SGSN obtain session information for the prior art process, not repeat them

data traffic flow meets a preset condition between, and if so, the charging operation is performed.

12. The method according to claim 10, characterized in that, according to the CDR and billing of its charging attribute comprises:

The CDR billing query attribute of the corresponding charging rule;

According to the accounting rules, and CDR billing for the current session.

13. A method according to claim 11, characterized in that when the S-CDR accounting attribute is a single tunnel.

Judging the quality of service parameter or parameters of the current rate of the session is changed, if changed, the new flow is generated in the node according to the S-CDR quality of service parameter or parameters of the rate after the change.

14. A general packet radio service support node for receiving and transmitting terminal via the communication base station subsystem transfer the data, and the billing gateway for billing processing is connected, characterized by comprising:

Session information acquiring unit for acquiring information of the current session, the current session charging attribute extracted from the session information;

CDR packaging unit, for carrying on the charging property of each CDR in the charging CDR indicating the attribute of the user related information of the tunnel;

CDR transmitting unit for transmitting to the charging gateway CDR charging property of the carry.

15. GSN 14 according to the preceding claims, characterized in that said CDR packing unit comprises:

The first package unit for setting a direct tunnel in the identification of the CDR attribute indicates the CDR for all traffic nodes are single tunnel; or

The second package unit for setting the direct identification of the CDR in the tunnel when the properties of the CDR in all traffic nodes are single tunnel, the tunnel ID value is set to direct a preset value; or

A third encapsulating unit, in said CDR of a node in the flow field is provided for the direct tunnel identifier indicative of the flow properties of a node are a single tunnel; or

A fourth packaging unit, for the CDR of a traffic node in a direct tunnel identifier field is set, when the attribute of the flow nodes are single tunnel, the value is set to a direct tunnel is identified as a preset value.

16. GSN 14 according to the preceding claims, characterized in that,

When the GSN as a service GSN, the CDR package unit carries the charging attribute to each S-CDR, the CDR transmitting unit to the charging gateway sends the billing property carrying S-CDR;

When the gateway GSN GSN, said CDR package unit carries the charging attribute to each G-CDR, the CDR billing gateway sending unit to send the portable charging properties of G-CDR.

17. The according to claim GSN 16, characterized in that the GSN further comprising:

here.

[0027] 102, the charging property carried in the S-CDR;

Billing property [0028] In the present embodiment, when the SGSN needs to send S-CDR to the billing center that is will get the current session information and to obtain billing information from the session attribute will get to carry on the S-CDR in specific implementations of the steps in the practice of the present invention in a variety of, the following detailed description:

[0029] The method of carriage can be roughly divided into two categories:

[0030] First, the direct billing property carried in the S-CDR in:

[0031] In this manner, the extension of a field directly in the conventional S-CDR data format Direct TunnelFlag, for indicating charging properties of the tunneling-related information in such a manner, the charging property One Tunnel , it means that all of the properties in the S-CDR traffic nodes are One Tunnel, if the charging property for Two Tunnels, it indicates that the properties of the S-CDR all traffic nodes are Two Tunnel, specific instructions way also divided into two types:

[0032] 1, using the field carrying case identifies the accounting attributes:

[0033] In this way, if the S-CDR carried in the field Direct Tunnel Flag, it indicates that the S-CDR billing attributes for One Tunnel, that is, all the properties of the S-CDR in traffic nodes are One Tunnel, if not carrying the field Direct Tunnel Flag, it indicates that the S-CDR billing attributes for Two Tunnels, namely the properties of the S-CDR all traffic nodes are the Two Tunnels.

[0034] In this manner, the Direct Tunnel Flag field is not required to have a specific value, the charging property is determined only by its presence or absence.

[0035] 2, the value identifies the accounting field attributes:

[0036] In this manner, the field Direct Tunnel Flag needs to be assigned to be able to judge the charging property, i.e., a S-CDR of each field carry the Direct Tunnel Flag, just different in the S-CDR charging attribute fields in the Direct Tunnel Flag different values, such as may be agreed upon value of 1:00 indicates charging property is One Tunnel, that is, all the properties of the S-CDR in traffic nodes are One Tunnel, other values indicate charging property to Two Tunnels, namely the S- All nodes in the flow properties of the CDR are Two Tunnels. Be understood that the present embodiment will be described in only one example, in practical applications, this value can be stipulated in accordance with the actual situation, not defined here.

[0037] Second, through the S-CDR in List ofTraffic Data Volumes field identifies the accounting attributes:

[0038] in this manner is reflected in the charging properties of the S-CDR flow properties of each node, i.e. in the conventional S-CDR data format List of Traffic Data Volumes field extension field Direct Tunnel Flag, with attribute of the node to indicate the flow, to be noted that the original List ofTraffic Data Volumes field contains four parameters, namely, the uplink data volume (Data VolumeUplink), downlink data volume (Data Volume Downlink), the switching condition (Change Condition) and a switching time (Change Time), specific instructions by Direct Tunnel Flag billing property is divided into two ways:

[0039] 1, carrying case flow node identification field attributes:

[0040] In this way, if the S-CDR in the List of Traffic DataVolumes field carries the field Direct Tunnel Flag, it indicates that the properties of the flow node is One Tunnel, if not carrying the field Direct Tunnel Flag, said the properties of the flow node is Two Tunnels.

[0041] In this manner, the Direct Tunnel Flag field is not required to have specific numerical values to determine the flow

Flow node generating unit for, when the charging property of a single CDR tunnel judges that the current quality of service parameter or parameters of the session whether to change the rate of the occurrence, if changed, the parameters according to the changed quality of service or the flow rate of the parameters to generate a new node in said CDR.

18. A billing center, characterized by comprising:

If a single receiving unit for receiving CDR;

Charging attribute acquisition unit for acquiring the CDR charging CDR according to the received attribute information in the attribute is used to indicate the CDR charging tunnel related information;

Charging Rules inquiry unit, used to query the corresponding charging rule according to the charging property;

Charging means for charging rules based on the current session, and CDR for billing.

19. A billing center according to claim 18, characterized in that said charging attribute acquisition unit includes:

A first acquisition unit configured to determine whether the CDR includes a direct tunnel ID, if included, determine the properties of the CDR's of all nodes are single traffic tunnels, if included, is determined for all of the CDR attribute nodes are dual-flow tunnel;

Or

A second acquisition unit for judging whether the value of the direct tunnel identity included in CDR whether the preset value, and if so, determine the properties of the CDR's are single node for all traffic tunnels, if yes, it is determined Properties of the CDR in all traffic nodes are dual tunnel;

Or

Third obtaining means, for determining the flow rate of the CDR node identifier field contains a direct tunnel ID, if included, to determine the properties of the flow corresponding to the flow rate of the node identifier of the node is a single tunnel, if not contained, determining that the traffic the node identifier corresponding to the flow rate of the node attribute is a double tunnel;

Or

A fourth acquisition unit configured to identify the value of a direct tunnel to determine the flow rate of the CDR in a node ID field is included in the preset value, and if so, to determine the properties of the flow corresponding to the flow rate of the node identifier of the node is a single tunnel, if not, it is determined that the flow properties of the flow corresponding to the node ID of the node for the double tunnel.

properties of a node only by its presence or absence.

[0042] 2, using numerical flow node identification field attributes:

[0043] In this manner, the field Direct Tunnel Flag needs to be assigned to be able to judge the flow properties of the node, that is, S-CDR of each of the List of Traffic Data Volumes field carry the field Direct Tunnel Flag, but different properties traffic node field Direct Tunnel Flag different values, such as may be agreed property value of 1:00 indicates flow node is One Tunnel, other values indicate properties traffic node is Two Tunnels. Be understood that the present embodiment will be described in only one example, in practical applications, this value can be stipulated in accordance with the actual situation, not defined here.

[0044] The only four specific implementations of the charging property is carried in the S-CDR in the case has been described, it is understood that in the actual application process, in addition to the above-described manner can also take other way charging property carried in S-CDR, as long as possible to achieve the charging property carried in S-CDR can be, not limited means to achieve here.

[0045] It should be noted that, if the S-CDR accounting attribute is a single tunnel, the SGSN needs to monitor the current session to determine the current quality of service parameter or parameters of the session whether the rate of change, if change is required generating a new S-CDR traffic node according to quality of service parameter or parameters of the changed rate.

[0046] 103, S-CDR will be sent to CGF;

[0047] When the SGSN will carry on charging property after S-CDR, you can send the S-CDR to CGF for further processing.

[0048] 104, GGSN sends the G-CDR to CGF;

[0049] In the present embodiment, in order to achieve the subsequent billing, in addition to the SGSN generated S-CDR, but also need GGSN generated G-CDR, to be noted that the process GGSN generates G-CDR and the GGSN will be sent to the CGF G-CDR process of the prior art are not described here.

[0050] The present embodiment is the SGSN will be described as an example GSN can be understood that, if the GGSN GSN as an example will be described, this step was "SGSN will send to the S-CDR CGF".

Send to a billing center after the [0051] 105, billing and network management for the S-CDR G-CDR merger;

[0052] 106, the accounting center determines the flow rate difference between the preset condition of the received S-CDR and between G-CDR is met, and if so, step 107 is executed, and if not, step 110 is performed;

[0053] to determine the specific method is:

[0054] According to the billing center the billing identifier for the current session and the GGSN Internet address corresponding to the query S-CDR and the G-CDR, to be noted that, S-CDR and the G-CDR are included in the current session charging identifier and IP address of the GGSN, i.e. the billing center the billing query to the current session and the IP address of the GGSN indicates the same S-CDR and the G-CDR;

[0055] Gets the first data traffic from the query to the S-CDR as well as obtaining a second data traffic from the query to the G-CDR in;

[0056] Analyzing the difference between the first data and the second data traffic flow meets a preset condition between, and if so, the charging operation is performed.

[0057] This may be a specific value, it means that the difference between the first data and the second data traffic flow is less than a certain value, if less, then the billing embodiment preset condition, and if not, Step 110.

[0058] 107, Accounting Center for billing the property from the S-CDR;

[0059] When the difference S-CDR of the first data and the second data traffic flow in a G-CDR is less than a preset value, the billing center to obtain the S-CDR charging attribute in Depending on the way of carrying the charging property, the specific method to obtain the charging property comprising:

[0060] First, get the billing property directly from the S-CDR in:

[0061] In this manner, the charging attribute Direct TunnelFlag direct access to the received S-CDR data format fields, the specific access mode is also divided into two types:

[0062] 1, using the field carrying case to obtain billing attributes:

[0063] In this way, if the S-CDR carried in the field Direct Tunnel Flag, it indicates that the S-CDR billing attributes for One Tunnel, that is, all the properties of the S-CDR in traffic nodes are One Tunnel, if not carrying the field Direct Tunnel Flag, it indicates that the S-CDR billing attributes for Two Tunnels, namely the properties of the S-CDR all traffic nodes are the Two Tunnels.

[0064] In this manner, the Direct Tunnel Flag field is not required to have a specific value, the charging property is determined only by its presence or absence.

[0065] 2, using a numeric field acquisition accounting attributes:

[0066] In this way, you need to get the field Direct Tunnel Flag of value to be able to get the charging property, that is, each S-CDR carry the field Direct Tunnel Flag, just different attributes of S-CDR billing field in Direct Tunnel Flag of different values, such as may be agreed upon value of 1 indicates the charging property is One Tunnel, other values indicate charging property to Two Tunnels. Be understood that the present embodiment will be described in only one example, in practical applications, this value can be stipulated in accordance with the actual situation, not defined here.

[0067] Second, get billing property from the S-CDR in List ofTraffic Data Volumes field:

[0068] In this manner, S-CDR billing attributes to reflect the properties of the S-CDR of each node in the flow reading List ofTraffic Data Volumes field from the received S-CDR data format and, based on This field is a field in Direct Tunnel Flag obtain the flow properties of the node to obtain the S-CDR can be learned in the S-CDR billing property attribute all traffic nodes, specific access mode is also divided into two types:

[0069] 1, using the field carrying case to get traffic node attributes:

[0070] In this way, if the S-CDR in List ofTraffic Data Volumes field carries the field Direct Tunnel Flag, it indicates that the properties of the flow node is One Tunnel, if not carrying the field Direct Tunnel Flag, said the properties of the flow node is Two Tunnels.

[0071] In this manner, the Direct Tunnel Flag field is not required to have a specific value, the charging property is determined only by its presence or absence.

[0072] 2, using the numeric field to get traffic node attributes:

[0073] In this way, you need to get the field Direct Tunnel Flag attribute values in order to obtain traffic node, that is, each S-CDR in the List of Traffic Data Volumes field are carrying field Direct Tunnel Flag, just flow with different attributes node field Direct Tunnel Flag different values, such as may be agreed property value of 1:00 indicates flow node is One Tunnel, other values indicate properties traffic node is Two Tunnels. Be understood that the present embodiment will be described in only one example, in practical applications, this value can be stipulated in accordance with the actual situation, not defined here.

[0074] The only way to get the specific implementation of the four S-CDR in the charging properties, it is understood that in the actual application process, in addition to the above-described manner can also be taken from other ways to obtain the S-CDR billing property, the means to achieve here not limited.

[0075] 108, the query attribute corresponding billing and accounting rules;

[0076] When the billing center to obtain a charging property, according to the charging attribute query corresponding accounting rules, such as for billing property is One Tunnel (it means that the properties of the S-CDR in all traffic nodes are One Tunnel) of S-CDR and billing attributes for Two Tunnels (it means that the S-CDR in all traffic node attributes are Two Tunnels) of S-CDR, will each take a different accounting policy, specific terms charge strategy prior art, not limited herein.

[0077] 109, according to the charging rule, S-CDR and G-CDR for billing, and ends the process;

[0078] When the billing center the billing query to the corresponding policy, the can in accordance with the accounting policy, and combining of the received S-CDR and the G-CDR for billing for the current session, a description of that, the billing You can also use the acquired billing-related information, such as billing identification, PDP activation time, user location information, IP address of the GGSN, then a single duration and other information.

[0079] 110, performs exception processing.

[0080] When the difference S-CDR of the first G-CDR data flow and the second flow of data does not satisfy the preset condition, for example, the difference is greater than the preset threshold, the exception processing is performed, specifically, To: Request CGF resend S-CDR and G-CDR, also thought: prompt an error and terminates the process, it is understood that the same may be other types of exception handling processes.

[0081] The present embodiment of the invention, since the GSN in each CDR are provided with the properties of the CDR

billing-related information for indicating the tunnel, it is possible to obtain direct access to the corresponding CDR according to the charging property, whereby the basis of the charging property for billing, so that when there is a missing CDR, or reception error occurs, the billing process does not affect the determination of the properties of the other CDR billing, it is possible to reduce the influence of the error on the charging CDR, thus improve the accuracy of charging.

[0082] See Figure 2 below, for example, the communication system according to embodiments of the invention include:

[0083] SGSN201, used to obtain the current session of billing property, and the charging property carried in each S-CDR in the billing center 202 transmits the S-CDR;

[0084] Billing center 202 for receiving the S-CDR SGSN201 transmitted, to acquire the S-CDR charging properties according to the S-CDR information (the charging property is used to indicate the S- CDR tunnel-related information), billing according to the S-CDR and its charging properties.

[0085] In the present embodiment, the communication system may further comprises:

[0086] GGSN203, used to send to the billing center 202 G-CDR, the G-CDR billing attribute carries the billing attribute indicates that the G-CDR tunnel-related information.

[0087] In this example embodiment of a communication system may further comprises:

[0088] Charging Gateway 204 for receiving the S-CDR SGSN sending and G-CDR GGSN sent, received S-CDR and G-CDR to merge, and the bill is sent to the billing center after the merger .

[0089] Please refer to FIG. 3, for example, in the embodiment of the present invention GSN embodiment includes:

[0090] session information acquisition unit 301, is used to obtain the current session information, billing attribute extraction current session information from the session;

[0091] CDR packaging unit 302, for each of the charging property is carried in a CDR, the CDR charging attribute for indicating the tunnel related information;

[0092] CDR transmitting unit 303, the charging gateway for sending to carry CDR billing property.

[0093] In the present embodiment, CDR packaging unit 302 may further comprises:

[0094] The first package unit for setting the CDR direct tunnel in the identification of the S-CDR is used to indicate all of the properties are single tunnel traffic nodes;

[0095] or

[0096] The second package unit for setting the direct identification of the CDR in the tunnel when the properties of the CDR in all traffic nodes are single tunnel, the tunnel ID value is set to direct a preset value ;

[0097] or

[0098] The third package unit for the CDR node in a traffic tunnel identification field settings directly attribute indicates the flow rate for both single node tunnel;

[0099] or

[0100] The fourth package unit for setting a direct tunnel traffic node identification field in the CDR, when the properties of the flow nodes are single tunnel, the tunnel will set the value of the direct identification of the preset value.

[0101] Note that when the GSN SGSN when the CDR encapsulating unit 302 carried on the charging property of each S-CDR, the CDR to the transmission unit 303 transmits the charging gateway portable charging attribute S-CDR;

[0102] When the GSN as GGSN, said CDR package unit 302 carries the charging attribute to each G-CDR, the CDR transmitting unit 303 transmits to the portable charging gateway billing property G-CDR.

[0103] In the present embodiment, the GSN may further comprises:

[0104] Flow node generating means for, when the CDR charging attribute is a single tunnel, to judge the quality of service parameter or the parameters of the current session of the rate is changed, if the change is changed according to the post quality of service parameter or the flow rate of the parameters to generate a new node in said CDR.

[0105] Refer to Figure 4, the embodiment of the present invention, embodiments of the billing center comprising:

[0106] if a single receiving unit 401 for receiving the CDR and CDR;

[0107] charging attribute obtaining unit 402 for obtaining the CDR of charging CDR according to the received attribute

information in the attribute is used to indicate the CDR charging tunnel related information;

[0108] Charging Rules inquiry unit 403, is used to query the corresponding charging rule according to the charging property;

[0109] charging unit 404, used in accordance with the accounting rules, and CDR billing for the current session.

[0110] In the present embodiment, the charging attribute acquisition unit 402 may further comprises:

[0111] a first obtaining unit configured to determine whether the CDR includes a direct tunnel ID, if included, determine the properties of the CDR's of all nodes are single traffic tunnels, if included, determining that the Property CDR in all traffic nodes are dual tunnel;

[0112] or

[0113] a second obtaining unit configured to determine whether the value of the direct tunnel identity included in the CDR is the preset value and if so, determine the properties of the CDR's of all nodes are single tunnel traffic, if it is determining that the CDR in the properties of all the traffic nodes are dual tunnel;

[0114] or

[0115] The third acquisition unit configured to determine the flow rate of the CDR in the node ID field contains a direct tunnel ID, if included, to determine the properties of the flow corresponding to the flow rate of the node identifier of the node is a single tunnel, if included, attribute determines the flow of traffic node identifies the corresponding node is double tunnel;

[0116] or

[0117] The fourth acquiring unit configured to identify the value of a direct tunnel to determine the flow rate of the CDR in a node ID field is included in the preset value, and if so, to determine the attributes of the node ID corresponding to the traffic flow as a single node tunnels, if yes, it is determined that the flow properties of the flow corresponding to the node ID of the node for the double tunnel.

[0118] Those skilled in the art can understand the implementation of the above-described embodiments of the method can be all or part of the steps by a program instructing relevant hardware, the program may be stored in a computer readable storage medium, the program When executed, comprising the steps of: GSN Get the current session charging attribute; carried on the charging property of each data record CDR GSN charging, the charging property is used to indicate the CDR tunnel infos ; send to the billing center of the CDR; billing center to acquire the property in accordance with the CDR CDR billing information; billing center for billing based on the CDR and its charging properties.

[0119] the above-mentioned storage medium may be a read-only memory, magnetic or optical disk.

[0120] A charging control method of the above and the present invention provides the billing center and related equipment are described in detail for those of ordinary skill, the idea of an embodiment according to the present invention, in particular embodiments and applications were subject to change on a place, In summary, the present specification, the content should not be construed as limiting the present invention.

CLASSIFICATIONS

International Classification	H04L12/14, H04L12/56

LEGAL EVENTS

Date	Code	Event	Description
Sep 14, 2011	C12	Rejection of an application for a patent	
Jul 16, 2008	C10	Request of examination as to substance	
May 21, 2008	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Electronic Acknowledgement Receipt

EFS ID:	21656769
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	03-MAR-2015
Filing Date:	15-NOV-2013
Time Stamp:	16:10:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	612257 4b6ef73aaf1bcb968937d02b888f33c6fd92b439	no	5
Warnings:					
Information:					

2	Foreign Reference	2059.pdf	2523856 a966775427c913978f6580b049bab43a01a3cdd8	no	28

Warnings:	
Information:	
Total Files Size (in bytes):	3136113

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6119933	A	2000-09-19	Wong et al.	
	2	7149229	B1	2006-12-12	Leung, Kent K.	
	3	7242668	B2	2007-07-10	Kan et al.	
	4	8095640	B2	2012-01-10	Guingo et al.	
	5	8347104	B2	2013-01-01	Pathiyal, Krishna K.	
	6	8694772	B2	2014-04-08	Kao et al.	
	7	8705361	B2	2014-04-22	Venkataraman et al.	
	8	8719423	B2	2014-05-06	Wyld	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	8780857	B2	2014-07-15	Balasubramanian et al.	
	10	8811991	B2	2014-08-19	Jain et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050135264	A1	2005-06-23	Popoff et al.	
	2	20050245241	A1	2005-11-03	Durand et al.	
	3	20070165630	A1	2007-07-19	Rasanen et al.	
	4	20080125079	A1	2008-05-29	O'Neil et al.	
	5	20100287599	A1	2010-11-11	He et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	1	1503548	EP	A1	2005-02-02	FG Microtec GmbH		☐
	2	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		☐
	3	2008301121	JP	A	2008-12-11	Kyocera Corp.		☐
	4	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		☐
	5	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐
	6	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	7	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.		☐
	8	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2014-12-09
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 503 548 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.02.2005 Bulletin 2005/05

(51) Int Cl.[7]: **H04L 12/56**, G06F 13/38, H04L 29/06, H04M 11/06

(21) Application number: **03017485.8**

(22) Date of filing: **01.08.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(71) Applicant: **fg microtec GmbH**
81677 München (DE)

(72) Inventors:
- **Hofmann, Matthias**
87719 Mindelheim (DE)
- **Kelz, Thomas, Dr.**
16767 Germendorf (DE)
- **Mirbaha Vahid, Robert**
85386 Eching (DE)

(74) Representative: **Köllner, Malte**
Köllner & Partner
Patentanwälte
Kennedyallee 109
60596 Frankfurt am Main (DE)

(54) Distributed Quality of Service Management System

(57) An application unit and a modem unit for mobile communication are provided. The application unit comprises at least one application that exchanges data traffic with at least one protocol stack, wherein said at least one protocol stack transfers data between at least one of the applications and at least one physical interface. The modem unit comprises a broadcast facility for setting up a wireless connection, and at least one transmission protocol stack for transferring data traffic between the at least one physical interface and the broadcast facility. The at least one physical interface is adapted for transmitting data traffic as well as flow control information between the modem unit and at least one application unit.

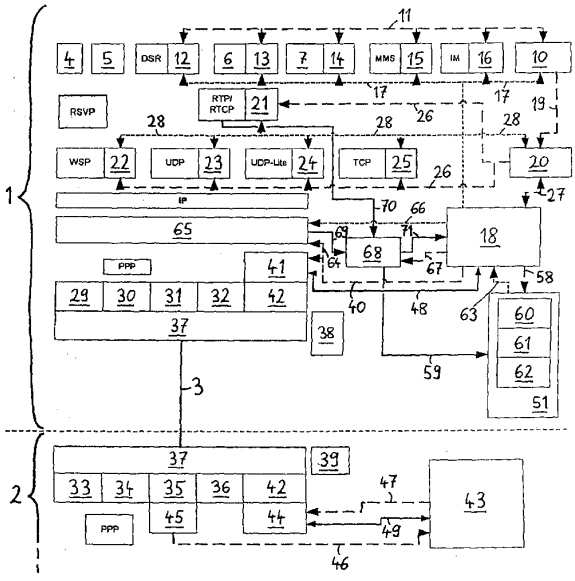


Fig. 1

EP 1 503 548 A1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

[0001] The present invention relates to an application unit, to a modem unit, to a user equipment for mobile communication, and to an interface facility. Furthermore, the present invention relates to a method for coordinating data flow.

[0002] Mobile devices might comprise applications, protocol stacks as well as a modem unit adapted for establishing a wireless connection with a mobile communication network, whereby all said entities may run on one processing system. The modem unit might as well be installed on a different processing resource than the applications. Besides that, for the modem unit, a first operating system might be used, and for the applications, another operating system might be employed. It is expected that in the future, more and more user terminals will be available that do not comprise a proprietary modem unit. Instead, said user terminals will comprise a physical interface for establishing a connection between said user terminal and an external modem unit, whereby the external modem unit will be responsible for setting up a wireless connection with the mobile communication network. Besides that, phones will be available where an additional processing resource and/or an additional operating system like e.g. Symbian is provided for running the applications.

[0003] In the European Patent Application "Quality-of-Service Management System", Application No. 03012613.0, which has been filed by the applicant of the present invention, a QoS management system comprising a plurality of different entities is described. The disclosure of said application is herewith incorporated into this specification by reference.

SUMMARY OF THE INVENTION

[0004] It is an object of the invention to improve flow control in a distributed user equipment comprising a modem unit and at least one application unit. The object of the invention is solved by the independent claims. Preferred embodiments are shown by the dependent claims.

[0005] An application unit according to embodiments of the present invention comprises at least one application, wherein said at least one application is adapted for exchanging data traffic for wireless communication with at least one protocol stack.

[0006] Said at least one protocol stack is adapted for transferring data traffic between at least one of said applications and at least one physical interface. The at least one physical interface is adapted for transmitting data traffic as well as flow control information between said application unit and a modem unit.

[0007] The application unit is connected with the modem unit via at least one physical interface, whereby both uplink traffic and downlink traffic related to the applications is transmitted via said at least one physical interface. According to the invention, flow control information may be transmitted via the at least one physical interface. The data traffic and the flow control information might e.g. be transmitted in a multiplexed mode via said at least one physical interface. Alternatively, the flow control information might e.g. be transmitted via different physical interfaces than the data traffic.

[0008] In prior art solutions, the application unit has not been aware of the flow parameters on the modem unit, and the modem unit has not been aware of the applications and the flow parameters on the application unit. The embodiments of the present invention allow for an exchange of flow control information between the application unit and the modem unit. On both of the units, said flow control information is helpful for utilizing the available resources and the available bandwidth of the wireless connection as efficiently as possible. Each of the units is informed about the overall system state and may react accordingly. As a result, the system's overall performance is increased. A smooth adaptation of the system's control settings is achieved, and the applications' QoS requirements can be fulfilled to a degree that has not been possible yet.

[0009] According to a preferred embodiment of the invention, said at least one physical interface is realized as or comprises at least one serial interface, in particular at least one of a RS232, IrDA, Bluetooth, USB, PCMCIA, UART interface. A serial interface provides sufficient bandwidth for transmitting both application-related data traffic and flow control information between the modem unit and the application unit.

[0010] According to a preferred embodiment of the invention, said flow control information comprises at least one of: QoS profiles of said applications, actual parameters indicating the actual state of the data flow on at least one of the application unit and the modem unit, and predicted parameters indicating a future state of the data flow on at least one of the application unit and the modem unit. On the application unit, the applications and their QoS requirements may be known. By transmitting these QoS profiles to the modem unit and adjusting the modem unit's parameters accordingly, the distributed system's overall data flow can be optimised, and the applications' QoS requirements can be fulfilled as far as possible. Furthermore, actual parameters indicating the system's actual flow situation might be collected on at least one of the application unit and the modem unit. In order to optimise the overall data flow in a distributed system, each of the units has to be aware about the data flow on the remote units, because this allows to adjust the parameters of the own unit in accordance with the system's overall data flow. Flow parameters and QoS parameters collected on the modem unit might e.g. be provided, as a part of the flow control information, to the application unit. The settings on the application unit may then be adapted accordingly. Vice

versa, the application unit might inform the modem unit about types of data traffic, about buffer fill levels and other flow parameters. The exchange of flow parameters helps to find suitable control settings for improving the overall data flow. Both the modem unit and the application unit get a complete picture, and therefore, the decision-making is improved. By means of prediction methods, parameters indicating a future system state might be derived from the actual flow parameters. Said predictions might e.g. anticipate the occurrence of congestion, of cell reselections, of sudden changes of the available bandwidth, etc. By predicting the system behaviour in the near future, a smooth control of the system's settings is accomplished. In order to inform the application unit about predictions that have been calculated on the modem unit, said predictions are transmitted, as a part of the flow control information, to the application unit. Vice versa, the application unit might provide its predictions to the modem unit.

[0011] According to another preferred embodiment of the invention, said flow control information comprises control settings adapted for controlling the data flow on at least one of the application unit and the modem unit. For example, control settings for the entire system may be generated on the part of the modem unit. Said control settings comprise control settings for entities on the application unit that have to be transmitted, as a part of the flow control information, from the modem unit to the application unit. Whenever control settings for an entity on a remote unit are generated, said control settings have to be transmitted, as a part of the flow control information, via the at least one physical interface.

[0012] In a preferred embodiment of the invention, said application unit is adapted for receiving, from said modem unit, at least one of control settings for said applications, control settings for said protocol stacks, control settings for buffers. Said control settings are transmitted as a part of said flow control information.

[0013] According to another preferred embodiment of the invention, said application unit is adapted for transmitting to said modem unit at least one of: information about said applications, QoS profiles of said applications, information about the protocols used by said applications, types of data traffic, bandwidth per traffic type, maximum buffer sizes, buffer fill levels. Said information is transmitted as a part of said flow control information.

[0014] According to another preferred embodiment, said application unit is adapted for transmitting to said modem unit at least one of: predictions related to cell reselections, predictions related to throughput, predictions related to bit error rate, predictions related to coding scheme, predictions related to one way delay, predictions related to round trip time, wherein said predictions are transmitted as a part of said flow control information. Predictions that have been calculated on the application unit might be provided to the modem unit, because, as an example, settings of the transmission protocol stack might have to be adjusted accordingly. Because of the low transmission delay, the predictions will still be valuable when they arrive at the modem unit. In case the modem unit's processing system is employed for performing calculations, e.g. in order to predict cell reselections, the application units connected to said modem unit might be notified. In both cases, the predictions are transmitted as a part of the flow control information via the at least one physical interface.

[0015] According to a preferred embodiment, a set of virtual interfaces is used for setting up, maintaining and terminating one or more data connections via said at least one physical interface. Via the at least one physical interface, a lot of different data streams have to be transmitted, whereby said data streams might have completely different properties, and whereby different priorities might be assigned to said data streams. Some of the data streams might arise from different kinds of applications, others might contain flow control information, etc. Said data streams are provided to different virtual interfaces. This allows to distinguish between said data streams, and to process each of the data streams in accordance with its priority and its specific needs.

[0016] According to a preferred embodiment of the invention, a permanent high-priority connection is set up between said application unit and said modem unit, with said flow control information being transmitted via said high-priority connection. When measured data, QoS parameters, predictions and control settings are transmitted between the modem unit and the application unit, the transmission delay must not be too high. Otherwise, the flow control information will already be outdated when it is received. For this reason, a high priority has to be assigned to the flow control channel.

[0017] According to a preferred embodiment, said at least one physical interface is adapted for transmitting said data traffic and said flow control information in a multiplexed mode between said application unit and said modem unit. The transmission bandwidth provided by the at least one physical interface has to be shared between various different data streams. By transmitting data of different data streams in a multiplexed mode, a plurality of different data streams may be transmitted at the same time, whereby said data streams will not interfere with each other.

[0018] In another preferred embodiment, said application unit comprises at least two physical interfaces, whereby said flow control information is transmitted via different physical interfaces than said data traffic.

[0019] According to a preferred embodiment of the invention, the application unit comprises a first communication handler module adapted for coordinating and prioritising data traffic between functional entities of the application unit and the modem unit. The first communication handler may e.g. provide a variety of services that relate to allocating, administrating and terminating connections via the at least one physical interface. It may assign priorities to the data streams that are to be trans-

mitted via the at least one physical interface, in order to make sure that the most important data streams are transmitted even if the available bandwidth is not sufficient to carry all traffic.

[0020] According to another preferred embodiment of the invention, the application unit comprises a first controller module adapted for receiving at least one of flow control information collected on the application unit and flow control information received via said at least one physical interface, and for deriving, from said inputs, control settings in a way that the overall data flow is optimised. Said first controller module might e.g. be provided with flow control information from the application unit, from the modem unit, or from both units. The first controller module might e.g. be aware of the applications' QoS profiles, of the actual state of the data flow within the user equipment, and of predictions that have been made. The first controller module is responsible for decision-making, i.e. it has to derive control settings from the known information. The task is to adjust arbitrary parameters on the application unit, on the modem unit, or on both units in a way that the overall data flow on the distributed system is optimised. It is attempted to use the available resources in a way that the requirements of the various types of data traffic can be fulfilled as far as possible.

[0021] In a preferred embodiment of the invention, said first controller module may act as a primary controller that controls a second controller module on the modem unit. In case there exists a first controller module on the application unit and a second controller on the modem unit, it might be advantageous to select one of the two controller modules as a primary controller that is responsible for generating the control settings for the entire system, or at least for parts of the entire system. If one central instance is responsible for deciding about the control settings, a coherent and well-coordinated set of control settings will be generated. It might be advantageous to select the application unit's first controller module as a primary controller, because there might be much more memory and computation power available on the application unit than on the modem unit.

[0022] According to another preferred embodiment of the invention, said first controller module may act as a secondary controller that is controlled by a second controller module on the modem unit. The second controller module on the modem unit might as well be selected as a primary controller. In this case, the first controller module on the application unit might act as the second controller module's slave. Especially if two or more application units are connected with one modem unit, it is advantageous to establish the second controller module on the modem unit as the primary controller.

[0023] According to a preferred embodiment of the invention, the application unit comprises at least one protocol optimiser module adapted for accessing the settings of corresponding protocol stacks, preferably in accordance with control settings.

[0024] According to a preferred embodiment of the invention, the application unit comprises a first QoS packet processor module adapted for at least one of monitoring and modifying the data traffic between at least one of the protocol stacks and said at least one physical interface. Before data traffic of any one of the applications installed on the application unit may be forwarded, via the at least one physical interface, to the modem unit, said data traffic has to pass the first QoS packet processor. This provides an opportunity for monitoring the data traffic, and unknown types of data traffic may be detected and considered by the QoS management system. Furthermore, the first QoS packet processor module may actively modify certain data streams by holding back or even discarding data packets. The first QoS packet processor module might receive control settings from a respective primary controller, no matter whether said primary controller is located on the application unit or on the modem unit.

[0025] According to a preferred embodiment of the invention, the protocol stacks comprise at least one of WAP, TCP, WTCP, UDP, UDP Lite, RTP/RTCP protocol stacks.

[0026] A modem unit for mobile communication according to embodiments of the present invention comprises a broadcast facility adapted for setting up a wireless connection for mobile communication. The modem unit further comprises at least one transmission protocol stack adapted for transferring data traffic between said broadcast facility and at least one physical interface. Said at least one physical interface is adapted for transmitting data traffic as well as flow control information between the modem unit and at least one application unit. The modem unit according to embodiments of this invention allows for an exchange of flow control information between the at least one application unit and the modem unit. In particular, the modem unit might e.g. be informed about the data flow on the application unit, and it might e.g. inform said at least one application unit about its actual status. By exchanging flow control information, the system's overall control is improved. A smooth adaptation of the system's control settings is achieved, and the applications' QoS requirements may be fulfilled to a degree that has not been possible yet.

[0027] In a preferred embodiment of the invention, said modem unit is adapted for transmitting to at least one of the application units at least one of: parameters of the air link, signal strength of the wireless connection, parameters of the transmission protocol stack, available bandwidth, maximum buffer sizes, buffer fill levels, information about PDP contexts, radio resource management information. Said information is transmitted as a part of said flow control information.

[0028] According to a preferred embodiment of the invention, said modem unit is adapted for receiving, from at least one of the application units, at least one of: information about said applications, QoS profiles of said applications, information about the protocols used by

said applications, types of data traffic, bandwidth per traffic type, maximum buffer sizes, buffer fill levels. Said information is transmitted as a part of said flow control information. Thus, the control settings on the modem unit can e.g. be adjusted to the QoS requirements of the data streams that have to be transmitted.

[0029] According to a preferred embodiment of the invention, said modem unit is adapted for receiving, from at least one of the application units, at least one of: control settings for the transmission protocol stack, control settings for PDP contexts, control settings for buffers. Said control settings are transmitted as a part of said flow control information.

[0030] In a preferred embodiment of the invention, the applications' QoS profiles are taken into account by at least one of: setting PDP contexts, setting PDP subcontexts, setting or modifying GGSN filter rules. A PDP (Packet Data Protocol) context allows to define the transmission properties for a certain kind of data traffic. By means of a PDP context, it is possible to specify the transmission parameters of the transmission protocol stack as well as the transmission properties of the wireless link up to the mobile communication network's GGSN (Gateway GPRS Support Node).

[0031] According to a preferred embodiment of the invention, the modem unit comprises a second QoS packet processor module adapted for at least one of monitoring and modifying the data traffic between said at least one physical interface and the transmission protocol stack. In addition to data traffic generated by applications on the application unit, the second QoS packet processor module might also detect traffic that arises from applications on the modem unit, and it may identify bandwidths and QoS requirements of said data traffic. Control settings can then be chosen in a way that the respective requirements of the applications (including those on the modem unit) are fulfilled as far as possible.

[0032] According to a preferred embodiment of the invention, the modem unit comprises a command interpreter adapted for receiving and processing at least one of messages and commands issued by at least one of the application units, in particular for receiving and processing initialisation messages. The command interpreter monitors the data traffic that is transmitted to the modem unit via the at least one physical interface. If a certain command is detected within said data traffic, said command will be interpreted, and the corresponding actions will be carried out. The services provided by the command interpreter are especially useful in case an application on any one of the application units intends to transmit data via the air interface though the entities on the modem unit have not been initialised yet. In this case, the respective application unit sends initialisation messages via the at least one physical interface. On the modem unit, said initialisation messages are detected by the command interpreter. The command interpreter might induce an initialisation of the required entities, and then, the modem can start transmitting data via the wireless link. Thus, the command interpreter allows for a remote initialisation of entities on the modem unit.

[0033] In a preferred embodiment of the invention, said transmission protocol stack is a stack for at least one of: GPRS/GSM, GPRS/EDGE, CDMA, UMTS, wireless LAN, Bluetooth, HiperLan. The invention is in no way limited to any of said transmission protocols, though.

[0034] A user equipment might comprise at least one application unit and a modem unit as described above, whereby the units are connected via at least one physical interface. Data traffic as well as flow control information is transmitted, via said at least one physical interface, between at least one of the application units and said modem unit. By exchanging flow control information between the modem unit and the one or more application units, said units can be brought together more closely. Measured data and predictions are collected from various parts of the system, and the application units might e.g. inform the modem unit about the QoS profiles of the various applications. From these inputs, control settings for the entire system are derived, and said control settings are distributed to the various entities. As a result, the modem unit and the one or more application units merge and work together as one system.

[0035] According to a preferred embodiment of the invention, said modem unit and at least one of the application units are implemented as one embedded mobile device, preferably as a smartphone. Within the embedded device, the application unit and the modem unit might e.g. run on different processing systems. On the modem unit, a first operating system might be employed, while on the application unit, another operating system like e.g. Symbian might be used that is better suited for the respective applications.

[0036] According to another preferred embodiment, said modem unit is implemented as a separate device, preferably as a CF card, as a PCMCIA card, or as a part of a mobile phone. According to a preferred embodiment of the invention, at least one of the application units is implemented as a separate device, preferably as a laptop, as a mobile terminal, or as a PDA. A user terminal does not necessarily have to comprise a modem unit. Instead, it might comprise at least one physical interface for establishing a connection with an external modem unit.

[0037] The modules according to embodiments of the present invention can be partly or entirely embodied or supported by suitable software, which can be stored on or otherwise provided by any kind of data carrier, and which might be executed in or by any suitable data processing unit.

BRIEF DESCRIPTION OF THE DRAWINGS

[0038] Other objects and many of the attendant advantages of the present invention will be readily appre-

ciated and become better understood by reference to the following detailed description when considering in connection with the accompanied drawings.

Fig. 1 shows an application unit that is part of a user equipment for mobile communication, together with a portion of a modem unit;

Fig. 2 shows a modem unit that is part of a user equipment for mobile communication, together with a portion of the application unit of Fig. 1; and

Fig. 3 depicts the protocol layers that can be used for transmitting data in a multiplexed mode via the physical interface.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0039] Fig. 1 and Fig. 2 depict a user equipment for mobile communication that comprises an application unit 1 and a modem unit 2. The application unit 1 and the modem unit 2 are connected via a physical interface 3. A plurality of user applications might run on the application unit 1. In the example shown in Fig. 1, the applications comprise e-mail 4, a web-browser 5, DSR (Digital Surveillance Recorder), Push2Talk 6, Video Conference 7, MMS (Multimedia Messaging Service), IM (Instant Messaging), etc. The application unit 1 might further comprise transport protocol stacks with protocol layers like e.g. RTP/RTCP (Real Time Transport Protocol, Real Time Transport Control Protocol), RSVP (Resource Reservation Protocol), WSP (Wireless Session Protocol), UDP (User Datagram Protocol), UDP-Lite, TCP (Transmission Control Protocol), WTCP (Wireless profiled TCP), WAP (Wireless Application Protocol), etc. The transport protocol stacks transform the data payload of the various applications into IP (Internet Protocol) packets. The application-related data, and in particular the IP packets, are exchanged, via the physical interface 3, with the modem unit 2. The physical interface 3 might e.g. be realized according to one of the standards RS232, USB (Universal Serial Bus), Bluetooth, IrDA (Infrared Data Association), PCMCIA, etc. or by means of UARTs (Universal Asynchronous Receiver - Transmitter).

[0040] The modem unit 2 is implemented as a separate unit. The modem unit 2 is responsible for establishing and maintaining a wireless connection to a mobile communication network. For this purpose, the modem unit 2 comprises at least one transmission protocol stack 8. Said transmission protocol stack 8 might e.g. be a GPRS/GSM stack, or a GPRS/EDGE stack, or a stack for a future transmission protocol such as UMTS. IP packets that are received from the application unit 1 via the physical interface 3 are transferred to the transmission protocol stack 8. Vice versa, data received via the wireless connection is provided to the transmission protocol stack 8 and is routed, via the physical interface 3, to the application unit 1. The modem unit 2 might further comprise internal applications 9 and corresponding protocol stacks adapted for exchanging data traffic with the transmission protocol stack 8.

[0041] In the set-up shown in Fig. 1 and Fig. 2, the application unit 1 and the modem unit 2 are realized as separate units. For example, the application unit 1 might run on a first CPU (or on a first DSP), whereby a first operating system is used, while the modem unit 2 might run on a second CPU (or on a second DSP), wherewhereby a second operating system is used. Such a set-up might e.g. be found on a so-called smartphone, whereby a dedicated operating system like e.g. Symbian might be installed on the smartphone's application unit. To the end-user, these devices look the same as mobile phone devices, though the application unit and the modem unit are implemented as separate units. The application unit 1 and the modem unit 2 might as well be implemented on different mobile terminals. For example, a mobile device like a phone might be used as a modem for a second device like e.g. a laptop or a PDA (Personal Digital Assistant), whereby applications like e-mail, web-browser, VoIP client, Video applications etc. are executed on the part of the second device. The mobile phone comprises the modem unit, and the second device acts as an application unit. Alternatively, the modem unit 1 might be a dedicated piece of hardware like a CF (Compact Flash) card, a PCMCIA card, or the like.

[0042] In the following, the structure and functionality of a QoS management system for the above mentioned kind of user equipment will be described. It has to be noted that the invention can also be used if two or more application units are connected to one modem unit. Furthermore, the at least one application unit might be connected with two or more different modem units that support different transmission standards.

[0043] The applications that are running on the part of the application unit 1 are provided by different third party companies. Some of said applications, for example e-mail 4 and web-browser 5, might not be aware of the QoS management system. Other applications, like DSR, Push2Talk 6, Video Conference 7, MMS and IM, might be aware of the QoS management system. For these applications, the external application manager 10 is visible. The applications that are aware of the QoS management system register (11) with the external application manager 10 and forward their respective QoS requirements to the external application manager 10. The applications' QoS requirements are usually specified in terms of QoS classes. In general, four basic QoS classes are used that have been defined by 3GPP (3rd Generation Partnership Project), though other classifications might be used as well.

Conversational class

[0044] Traffic of the conversational class is very delay sensitive, and transfer delay and time variance between packets must stay below a certain value so that the human perception will accept the quality of the link. For traffic of the conversational class, it is most important that data is delivered in time. The bit error rate (BER) of the data traffic is not that critical. Examples for traffic of the conversational class comprise IP telephony and video telephony. In the example of Fig. 1, data traffic of the application Video Conference 7 belongs to the conversational class.

Streaming class

[0045] Traffic of the streaming class comprises one way real-time traffic. For traffic of the streaming class, a low transfer delay is not necessarily required, but the delay variation of the real-time data stream should be limited. In Fig. 1, data traffic of the application Push2talk 6 belongs to the streaming class.

Interactive class

[0046] Traffic of this class might e.g. emerge from an application where a user exchanges data interactively with an opposite party, which might either be another user or a computer system. The response to a request is generally expected within a certain time limit. Although the transfer delay may be higher than in case of traffic of the conversational class, the round trip time (RTT) is a key parameter. Traffic of the interactive class should show a low BER. Examples for this kind of traffic comprise web browsing or Telnet. In the example of Fig. 1, data traffic of the application IM belongs to the interactive class.

Background class

[0047] For data traffic of the background class, low delay or a short delivery time is not an issue, but the bit error rate (BER) has to be low. Data traffic of this class is usually received by a computer. Email traffic is a typical example for this kind of traffic. Accordingly, data traffic of the application e-mail 4 in Fig. 1 belongs to the background class.

[0048] For at least some of the applications that are aware of the QoS management system, so-called application optimisers might be installed. In Fig. 1, the applications DSR, Push2Talk 6, Video Conference 7, MMS and IM comprise corresponding application optimisers 12-16. When an application intends to send data, the corresponding application optimiser might adjust the way said data is generated to the overall data flow, to the available bandwidth, to the properties of the wireless connection, etc. In particular, the application optimisers 12-16 might influence the timing, the packaging of data, and the number of application frames per data packet, whereby the applications' QoS profiles are taken into account. During initialisation, the application optimisers 12-16 register with the external application manager 10. During operation, the application optimisers 12-16 might receive control information 17 from the external main controller 18, with said control information 17 comprising control settings for the application optimisers 12-16.

[0049] Next, the external application manager 10 initialises (19) the external protocol manager 20. The external protocol manager 20 is informed about the applications that run on the application unit 1, about the transport protocols used by said applications, and about the respective QoS profiles of the applications' data traffic.

[0050] For at least some of the transport protocol stacks, so-called protocol optimisers might be installed. In Fig. 1, protocol optimisers 21-25 corresponding to the transport protocol stacks RTP/RTCP, WSP, UDP, UDP-Lite ahd TCP are shown. The external protocol manager 20 initialises (26) the protocol optimisers 21-25 in accordance with the applications' QoS profiles. Each of the protocol optimisers 21-25 is responsible for dynamically accessing and adjusting the properties of its corresponding transport protocol stack. Said adjustment is performed in accordance with the corresponding applications' QoS requirements, in accordance with the overall data flow, and in accordance with measured or predicted system parameters.

[0051] Next, the external protocol manager 20 initialises (27) the external main controller 18 and transfers the control of the protocol optimisers 21-25 to said external main controller 18. Further on, both the protocol optimisers 21-25 and the external protocol manager 20 will receive their respective control settings 28 from the external main controller 18.

[0052] During operation, changes of the system's setup and of the data traffic generated by the applications might occur, and accordingly, a re-initialisation of at least one of the external application manager 10, the application optimisers 12-16, the external protocol manager 20 and the protocol optimisers 21-25 might be necessary. Said re-initialisations can either be induced by the applications themselves or by the external main controller 18.

[0053] The application unit 1 and the modem unit 2 communicate via the physical interface 3. In addition to uplink and downlink data traffic related to various applications, also flow control information is transmitted between the application unit 1 and the modem unit 2. Said flow control information might e.g. comprise measured parameters that indicate the actual system state, predictions indicating a future system state, and information related to the system's configuration. The flow control information might also comprise control settings for entities on the application unit 1 and on the modem unit 2.

[0054] The different data streams transmitted via the physical interface 3 should be handled separately and in accordance with their respective priorities. On the ap-

plication unit 1 and on the modem unit 2, a plurality of virtual interfaces 29-32 and 33-36 are provided, and said virtual interfaces may be used for setting up one or more virtual channels between the application unit 1 and the modem unit 2. According to a first embodiment, a corresponding physical interface is assighed to each of the virtual interfaces in a way that a one-to-one correspondence is established between the virtual interfaces and the physical interfaces. Alternatively, if only one physical interface is available, or if less physical interfaces than virtual interfaces are available, the data streams may be transmitted in a multiplexed mode. In this embodiment, a multiplexing protocol 37 is implemented both on the application unit 1 and on the modem unit 2. The multiplexing protocol 37 is adapted for providing a plurality of separate virtual interfaces. The multiplexing protocol 37 allows to transmit a plurality of data streams via different virtual channels in parallel, whereby priorities assigned to said data streams are considered. Accordingly, the transmission of lower priority traffic may be interrupted by higher priority traffic. The multiplexing is controlled by a mux controller 38 on the application unit 1 and by a mux controller 39 on the modem unit 2. Said mux controllers 38, 39 are responsible for setting up and tearing down virtual channels between the virtual interfaces.

[0055] For transmitting data via the physical interface 3 in a multiplex mode, the PPP (Point-to-Point Protocol) suite might be used together with some extensions. Said extensions allow for virtual serial lines and traffic prioritisation. A detailed description of the PPP protocol suite can be found in the document IETF RFC 1661. Alternatively, the PPP protocol suite without the above mentioned extensions can be combined with one of the multiplexing protocols defined by ETSI (European Telecommunications Standards Institute). Technical specifications of said multiplexing protocols can be found in ETSI, 3GPP TS 07.010 and 27.010. According to a third alternative, the application unit 1 and the modem unit 2 might be linked by an IP connection.

[0056] In the following, the initialisation of the interface facility will be described. The external main controller 18 addresses the mux controller 38 and allocates a virtual interface for establishing a Fast QoSM Connection between the application unit 1 and the modem unit 2. Next, the external main controller 18 initialises (40) the Comm Handler 41 and the Fast QoSM Connection 42. The Comm Handler 41 is responsible for handling the communication between entities of the QoS management system located on the application unit 1 and entities located on the modem unit 2. In case of congestion, the Comm Handler 41 has to decide about the priorities of the various data streams.

[0057] The Fast QoSM Connection 42 is a fast communication channel adapted for transmitting flow control information between the application unit 1 and the modem unit 2. The Fast QoSM Connection 42 is permanently set up on one channel of the interface. Flow control information, in particular measured data, control settings and predictions, have to be transmitted with low delay. For this reason, one of the highest available priorities is assigned to the Fast QoSM Connection 42.

[0058] Next, the application unit's Comm Handler 41 issues commands for starting up a main controller 43 and a Comm Handler 44 on the part of the modem unit 2. Said commands are transmitted, via the Fast QoSM Connection 42, to the modem unit 2. There, said commands are detected and interpreted by an AT command interpreter 45. In accordance with said commands, the main controller 43 is initialised (46). Then, the main controller 43 initialises (47) the modem unit's Comm Handler 44. Between the application unit's Comm Handler 41 and the modem unit's Comm Handler 44, a link is established. As soon as this link is available, the Comm Handler 41 will inform the external main controller 18.

[0059] The external main controller 18 may now forward flow control information via the data link 48 to the Comm Handler 41. From the Comm Handler 41, the flow control information is transmitted, via the Fast QoSM Connection 42, to the Comm Handler 44. The Comm Handler 44 forwards the flow control information via the data link 49 to the main controller 43. In the opposite direction, the main controller 43 may transmit flow control information via the data link 49, the Fast QoSM Connection 42 and the data link 48 to the external main controller 18. The external main controller 18 and the main controller 43 may now exchange all kinds of flow control information comprising QoS profiles, measured parameters, statistics, predictions, control settings, etc.

[0060] At first, the main controller 43 is installed as a primary controller that controls the external main controller 18. The external main controller 18 acts as a secondary controller (slave). The external main controller 18 and the main controller 43 exchange information about their respective capabilities and about the configuration of the application unit 1 and the modem unit 2. Then, the main controller 43 has to decide whether it is favourable to transfer the primary control of the QoS management system to the external main controller 18 or not. The CPU of the application unit 1 might have much more resources in terms of processing power and memory, and the modem unit's CPU would be offloaded from some of its tasks. However, if two or more application units are connected to the modem unit, the main controller 43 will most likely continue to act as a primary controller and control the tasks of the external main controllers.

[0061] The primary main controller is responsible for setting up the whole QoS management system. It has to decide how to distribute the required functionalities to the entities of the distributed QoS management system. Then, the respective entities are initialised accordingly. For example, the primary main controller has to decide whether a state predictor should be initialised on the application unit 1, on the modem unit 2, or on both of said units. The state predictors might use complex

algorithms for deriving the respective predictions, and accordingly, the state predictors will demand a lot of computation power. For this reason, it might be advantageous for the modem unit 2 to offload some of the computations to an external state predictor running on the application unit 1.

[0062] In the set-up of Fig. 1 and Fig. 2, the modem unit 2 comprises a state predictor 50, and the application unit 1 comprises an external state predictor 51. The state predictor 50 on the modem unit 2 is initialised (52) by the main controller 43. The state predictor 50 receives (53) measured data and system parameters. The predictions of the state predictor 50 are derived from measured data and system parameters that indicate the actual state of the system. The state predictor 50 comprises a multitude of different state predictor modules. For example, the state predictor 50 might comprise a state predictor module 54 adapted for predicting one way delay, round trip time (RTT) and throughput, a state predictor module 55 adapted for predicting coding scheme and BER (Bit Error Rate), and a state predictor module 56 adapted for predicting cell reselections. During a cell reselection, data transmission is interrupted for a period of time in the order of seconds, and therefore, the main controller 43 should be informed about cell reselections. The predictions of the state predictor 50 are provided (57) to the main controller 43. Similarly, the external state predictor 51 is initialised (58) by the external main controller 18. The external state predictor 51 receives (59) measured data and system parameters. It comprises state predictor modules 60, 61, 62 adapted for deriving a variety of different predictions. Said predictions are provided (63) to the external main controller 18.

[0063] Further, the external main controller 18 initialises (64) an external QoS packet processor 65. The external QoS packet processor 65 is responsible for detecting and keeping track of the various types of data traffic between the transport protocol stacks and the interface facility. For this purpose, it monitors both the uplink traffic and the downlink traffic. The external QoS packet processor 65 detects the bandwidths and the QoS profiles of the different types of data traffic.

[0064] On the application unit 1, there might exist applications that are not aware of the QoS management system. For example, the applications e-mail 4 and web-browser 5 shown in Fig. 1 might belong to the group of applications that is not aware of the QoS management system. If one of said applications starts sending data traffic, the external QoS packet processor 65 will detect this new kind of data traffic. Whenever a new type of data traffic is detected, the external QoS packet processor 65 will identify this traffic, the bandwidth and QoS profile of said traffic, and it will identify the application that has generated said traffic. In addition to that, the external QoS packet processor 65 may modify the flow of data packets. For this purpose, the external QoS packet processor 65 may hold back and buffer IP packets of certain data streams, whereby data packets of minor importance may even be discarded. The external QoS packet processor 65 receives control settings 66 from the external main controller 18 that indicate how the filters and buffers have to be set up.

[0065] Furthermore, the external main controller 18 initialises (67) an external collector 68 on the application unit 1. The external collector 68 is responsible for collecting information from different entities of the application unit 1. For example, the external collector 68 receives (69) information including the types of traffic, the current bandwidth per traffic type, maximum buffer sizes, current fill levels of various buffers, etc. from the external QoS packet processor 65. Furthermore, the external collector 68 might receive feedback information 70 from the transport protocol stacks, e.g. from the RTP/RTCP protocol stack. The external collector 68 provides (59, 71) the collected information to the external state predictor 51 and to the external main controller 18. Similarly, the modem unit 2 might comprise a collector 72 that is responsible for collecting information from the entities of the modem unit 2.

[0066] In addition to the applications that run on the application unit 1, internal applications 9 and the corresponding protocols might as well be installed on the modem unit 2. The internal applications and protocols indicated in Fig. 2 might additionally comprise at least one of: an application manager, a protocol manager, application optimisers and protocol optimisers. Said entities are part of the QoS management system. They are initialised (73) by the main controller 43, and they receive control settings 74 from the main controller 43.

[0067] Besides the external QoS processor 65 on the application unit 1, also the modem unit 2 might comprise a QoS packet processor 75 that is initialised (76) by the main controller 43. The QoS packet processor 75 monitors the uplink and downlink traffic. Besides that, it might modify the data traffic passing through it. Data packets may be buffered before they are forwarded to the transmission protocol stack 8, or they may even be discarded.

[0068] In particular, the QoS packet processor 75 detects and analyses data traffic arising from the internal applications 9. Information about different types of data traffic and their respective bandwidths is forwarded (77) to the collector 72. The primary main controller, e.g. the main controller 43, processes the information provided by the external QoS packet processor 65 and by the QoS packet processor 75. Based on this information, the primary main controller decides whether the overall QoS can be improved by setting up another PDP context, a PDP subcontext, or a new filter list for the GGSN (Gateway GPRS Support Node). PDP contexts and PDP subcontexts allow to define the transmission properties for a certain type of data traffic. The primary main controller might instruct (78) the mobility/radio resource management 79 to set up or modify a PDP context or a PDP subcontext. The parameters of said PDP contexts

and PDP subcontexts are chosen in accordance with the QoS requirements of the respective traffic. When the respective PDP context or PDP subcontext has been activated, the primary main controller will instruct (80) the QoS packet processor 75 to use this PDP context or PDP subcontext for the further transmission of certain types of data traffic.

[0069] The transmission protocol stack 8 might e.g. be a GPRS/GSM stack, a GPRS/EDGE stack, a UMTS stack, or a HiperLan stack, or a WLAN stack. In the future, other transmission protocol stacks that relate to future transmission protocols might be employed. In case of a GPRS/GSM or a GPRS/EDGE stack, the stack's uppermost layer is a SNDCP (Sub-Network Dependent Convergence Protocol) layer. In case of a UMTS stack, the uppermost layer is a PDCP (Packet Data Convergence Protocol) layer. The subsequent layer, the LLC (Logical Link Control), is responsible for segmenting the IP packets into data blocks suitable for transmission. For this purpose, the LLC comprises a LLC buffer 81. The data blocks are forwarded to a RLC (Radio Link Control) layer comprising a RLC buffer 82. The data blocks are provided to the physical layer L1, which is the lowest layer of the transmission protocol stack 8. The main controller 43 may initialise (83) a LLC manager 84 that is part of the QoS management system. The LLC manager 84 may set various parameters of the LLC, delete LLC blocks or reorder LLC blocks. Similarly, the main controller 43 may initialise (85) a RLC manager 86 that is adapted for accessing the settings of the RLC, and for modifying the RLC data blocks.

[0070] The control settings of the transmission protocol stack 8 may be dynamically adapted (87) by a stack manager 88, which is initialised (89) and controlled (90) by the main controller 43. There exist a variety of possibilities how the stack manager 88 can do that: the stack manager 88 might e.g. influence (91) the mobility/radio resource management 79 in a way that a cell reselection is either initiated or delayed. Furthermore, it might reset the RLC buffer 82 and/or delete selected PDUs (Protocol Data Units) in the RLC buffer 82. Besides that, the stack manager 88 might be involved in administrating PDP contexts and PDP subcontexts. Furthermore, the stack manager 88 might be involved in setting the filter rules of the GGSN in accordance with the QoS requirements of the respective traffic. By setting the RLC mode, the stack manager 88 might specify whether an acknowledged or an unacknowledged mode shall be used for the data transmission, and how the delivery of defective RLC blocks shall be handled.

[0071] The mobility/radio resource management 79 is responsible for the mobility management, for authorization, and for establishing and terminating a wireless connection. It is also responsible for performing cell reselections, i.e. for switching from one base station to an adjacent base station. The mobility/radio resource management is instructed to set up PDP contexts and PDP subcontexts with suitable attributes for all kinds of data traffic as well as filter lists for the GGSN.

[0072] After the collector 72 on the part of the modem unit 2 has been initialised (92), it starts collecting information from different entities on the modem unit 2. For example, from the physical layer L1, information relating to the signal power and the available bandwidth of the wireless connection might be obtained (93). The collector 72 might further collect information from the RLC (94), from the LLC (95), from the SNDCP/PDCP (96), from the QoS packet processor 75 (77), and from the internal applications 9 (97). The collected data is provided (53, 98) to the state predictor 50 as well as to the main controller 43. Between the application unit's external collector 68 and the modem unit's collector 72, a direct communication might be established, and collected data might be exchanged via the Fast QoSM Connection 42.

[0073] During operation, the respective primary controller will receive flow parameters from the application unit's external collector 68, and from the modem unit's collector 72. Furthermore, the respective primary controller is provided with predictions from the state predictor 50 and from the external state predictor 51. The primary controller is responsible for making decisions, and for determining the control settings for the entire system in accordance with predefined strategies. The aim is to smoothly adapt the control settings to the requirements of the various data streams. In case the external main controller 18 is selected as the primary controller, flow parameters and predictions provided by the collector 72 and the state predictor 50 are transmitted via the Fast QoSM connection 42 and the data link 48 to the external main controller 18. Control settings that are destined for the modem unit 2 are transmitted via the data link 48 and the Fast QoSM connection 42 to the entities on the modem unit 2. The main controller 43, which acts as a secondary controller, might be responsible for distributing the control settings on the modem unit 2.

[0074] In case the main controller 43 is selected as the primary controller, flow parameters and predictions provided by the external collector 68 and the external state predictor 51 are transmitted via the Fast QoSM connection 42 and the data link 49 to the main controller 43. Control settings for the application unit 1 are transmitted via the data link 49 and the Fast QoSM connection 42 to the entities on the application unit 1. In this case, the external main controller 18 acts as a slave of the main controller 43. Said external main controller 18 might be responsible for distributing the control settings on the application unit 1.

[0075] It has to be pointed out that a QoS management system according to the present invention doesn't have to comprise every single one of the modules shown in Fig. 1 and Fig. 2. A QoS management system according to an embodiment of the present invention might as well comprise a subset of the above-mentioned modules.

[0076] In the European Patent Application "Quality-

of-Service Management System", Application No. 03012613.0, which has been filed by the applicant of the present invention, a detailed description of the QoS management system's entities and their respective functionality can be found. The disclosure of said application is herewith incorporated into this specification by reference.

[0077] Fig. 3 shows the layers of the transport protocol stack together with the layers of a multiplexing protocol that is used for transmitting data via the physical interface 3. For example, user data 99 that is part of a real-time data traffic might be generated on the application unit 1. A header 100 for payload is added to said user data 99, and the obtained payload 101 is forwarded to a corresponding transport protocol stack 102. In Fig. 3, the transport protocol stack 102 comprises protocol layers for RTP, UDP and IP. The transport protocol stack 102 provides IP packets to the interface facility. For setting up a connection between the application unit 1 and the modem unit 2, protocols of the PPP protocol suite might be employed (103, 104) on both units. Alternatively or additionally, services provided by a Comm Handler 105 on the application unit 1 and by a Comm Handler 106 on the modem unit 2 might be utilized.

[0078] In order to allow for the transmission of multiple data streams via the physical interface 3, a multiplexing protocol is implemented on the application unit 1 and on the modem unit 2. For example, a multiplexing protocol according to one of the standards 3GPP 27.010 or 7.010 might be used. On the application unit 1, the multiplexing protocol 107 provides a set of virtual interfaces 108, 109. Accordingly, virtual interfaces 111, 112 are provided by the multiplexing protocol 110 on the modem unit 2. Said virtual interfaces may be used for setting up virtual channels between the application unit 1 and the modem unit 2. Then, IP packets may be transmitted from the application unit 1 to the modem unit 2, and vice versa, via the physical layer 113. In addition to user data, messages and commands might be transmitted via the physical layer 113 between the Comm Handlers 105 and 106. The AT command interpreter 114 is used to set up and modify the virtual interfaces.

Claims

1. An application unit (1) that comprises at least one application adapted for exchanging data traffic for wireless communication with at least one protocol stack; wherein said at least one protocol stack is adapted for transferring data traffic between at least one of said applications and at least one physical interface (3); **characterized in that**
said at least one physical interface (3) is adapted for transmitting data traffic as well as flow control information between said application unit (1) and a modem unit (2).

2. The application unit of claim 1, **characterized in that** said at least one physical interface (3) is realized as or comprises at least one serial interface, in particular at least one of a RS232, IrDA, Bluetooth, USB, PCMCIA, UART interface.

3. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said flow control information comprises at least one of:

   - QoS profiles of said applications;
   - actual parameters indicating the actual state of the data flow on at least one of the application unit (1) and the modem unit (2);
   - predicted parameters indicating a future state of the data flow on at least one of the application unit (1) and the modem unit (2).

4. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said flow control information comprises control settings adapted for controlling the data flow on at least one of the application unit (1) and the modem unit (2).

5. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said application unit (1) is adapted for receiving, from said modem unit (2), at least one of control settings for said applications, control settings for said protocol stacks, control settings for buffers, wherein said control settings are transmitted as a part of said flow control information.

6. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said application unit (1) is adapted for transmitting to said modem unit (2) at least one of: information about said applications, QoS profiles of said applications, information about the protocols used by said applications, types of data traffic, bandwidth per traffic type, maximum buffer sizes, buffer fill levels, wherein said information is transmitted as a part of said flow control information.

7. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said application unit (1) is adapted for transmitting to said modem unit (2) at least one of: predictions related to cell reselections, predictions related to throughput, predictions related to bit error rate, predictions related to coding scheme, predictions related to one way delay, predictions related to round trip time, wherein said predictions are transmitted as a part of said flow control information.

8. The application unit of claim 1 or any one of the preceding claims, **characterized in that** a set of virtual interfaces (29-36) is used for setting up, maintaining

and terminating one or more data connections via said at least one physical interface (3).

9. The application unit of claim 1 or any one of the preceding claims, **characterized by** a permanent high-priority connection (42) that is set up between said application unit (1) and said modem unit (2), with said flow control information being transmitted via said high-priority connection (42).

10. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said at least one physical interface (3) is adapted for transmitting said data traffic and said flow control information in a multiplexed mode between said application unit (1) and said modem unit (2).

11. The application unit of claim 1 or any one of the preceding claims, **characterized in that** said application unit (1) comprises at least two physical interfaces, whereby said flow control information is transmitted via different physical interfaces than said data traffic.

12. The application unit of claim 1 or any one of the preceding claims, **characterized by** a first communication handler module (41) adapted for coordinating and prioritising data traffic between functional entities of the application unit (1) and the modem unit (2).

13. The application unit of claim 1 or any one of the preceding claims, **characterized by** a first controller module (18) adapted for receiving at least one of flow control information collected on the application unit (1) and flow control information received via said at least one physical interface (3), and for deriving, from said inputs, control settings in a way that the overall data flow is optimised.

14. The application unit of claim 13, **characterized in that** said first controller module (18) may act as a primary controller that controls a second controller module (43) on the modem unit (2).

15. The application unit of claim 13, **characterized in that** said first controller module (18) may act as a secondary controller that is controlled by a second controller module (43) on the modem unit (2).

16. The application unit of claim 1 or any one of the preceding claims, **characterized by** at least one protocol optimiser module (21-25) adapted for accessing the settings of corresponding protocol stacks, preferably in accordance with control settings.

17. The application unit of claim 1 or any one of the preceding claims, **characterized by** a first QoS packet processor module (65) adapted for at least one of monitoring and modifying the data traffic between at least one of the protocol stacks and said at least one physical interface (3).

18. A modem unit (2) for mobile communication comprising

- a broadcast facility adapted for setting up a wireless connection for mobile communication;
- at least one transmission protocol stack (8) adapted for transferring data traffic between said broadcast facility and at least one physical interface (3);
- said at least one physical interface (3), which is adapted for transmitting data traffic as well as flow control information between the modem unit (2) and at least one application unit (1).

19. The modem unit of claim 18, **characterized in that** said flow control information comprises at least one of:

- QoS profiles of said applications;
- actual parameters indicating the actual state of the data flow on at least one of the modem unit (2) and one or more of the application units (1);
- predicted parameters indicating a future state of the data flow on at least one of the modem unit (2) and one or more of the application units (1).

20. The modem unit of claim 18 or any one of the preceding claims, **characterized in that** said flow control information comprises at least one of:

- control settings adapted for controlling the data flow on at least one of the modem unit (2) and one or more of the application units (1).

21. The modem unit of claim 18 or any one of the preceding claims, **characterized in that** said modem unit (2) is adapted for transmitting to at least one of the application units (1) at least one of: parameters of the air link, signal strength of the wireless connection, parameters of the transmission protocol stack (8), available bandwidth, maximum buffer sizes, buffer fill levels, information about PDP contexts, radio resource management information, wherein said information is transmitted as a part of said flow control information.

22. The modem unit of claim 18 or any one of the preceding claims, **characterized in that** said modem unit (2) is adapted for receiving, from at least one of the application units (1), at least one of: information about said applications, QoS profiles of said applications, information about the protocols used by

said applications, types of data traffic, bandwidth per traffic type, maximum buffer sizes, buffer fill levels, wherein said information is transmitted as a part of said flow control information.

23. The modem unit of claim 18 or any one of the preceding claims, **characterized in that** said modem unit (2) is adapted for receiving, from at least one of the application units (1), at least one of: control settings for the transmission protocol stack (8), control settings for PDP contexts, control settings for buffers, wherein said control settings are transmitted as a part of said flow control information.

24. The modem unit of claim 18 or any one of the preceding claims, **characterized in that** said modem unit (2) is adapted for transmitting to at least one of the application units (1) at least one of: predictions related to cell reselections, predictions related to throughput, predictions related to bit error rate, predictions related to coding scheme, predictions related to one way delay, predictions related to round trip time, wherein said predictions are transmitted as a part of said flow control information.

25. The modem unit of claim 18 or any one of the preceding claims, **characterized by** a second communication handler module (44) adapted for coordinating and prioritising data traffic between functional entities on at least one of the modem unit (2) and one or more of the application units (1).

26. The modem unit of claim 18 or any one of the preceding claims, **characterized by** a second controller module (43) adapted for receiving at least one of flow control information collected on the modem unit (2) and flow control information received via said at least one physical interface, and for deriving, from said inputs, control settings in a way that the overall data flow is optimised.

27. The modem unit of claim 18 or any one of the preceding claims, **characterized in that** the applications' QoS profiles are taken into account by at least one of: setting PDP contexts, setting PDP subcontexts, setting or modifying GGSN filter rules.

28. The modem unit of claim 18 or any one of the preceding claims, **characterized by** a second QoS packet processor module (75) adapted for at least one of monitoring and modifying the data traffic between said at least one physical interface (3) and the transmission protocol stack (8).

29. The modem unit of claim 18 or any one of the preceding claims, **characterized by** a command interpreter (45) adapted for receiving and processing at least one of messages and commands issued by at least one of the application units (1), in particular for receiving and processing initialisation messages.

30. A user equipment comprising at least one application unit (1) according to any of claims 1 to 17 that is connected, via said at least one physical interface (3), with a modem unit (2) according to any of claims 18 to 29, wherein data traffic as well as flow control information is transmitted, via said at least one physical interface (3), between at least one of the application units (1) and said modem unit (2).

31. The user equipment of claim 30, **characterized in that** said modem unit (2) and at least one of the application units (1) are implemented as one embedded mobile device, preferably as a smartphone.

32. The user equipment of claim 30, **characterized in that** said modem unit (2) is implemented as a separate device, preferably as a CF card, as a PCMCIA card, or as a part of a mobile phone, and wherein at least one of the application units (1) is implemented as a separate device, preferably as a laptop, as a mobile terminal, or as a PDA.

33. An interface facility adapted for transmitting data between at least one application unit (1) and a modem unit (2), with at least one application being installed on at least one of the application units (1), and with said modem unit (2) being adapted for establishing a wireless connection for mobile communication,

- said interface facility being adapted for transferring data traffic of said at least one application between said modem unit (2) and at least one of the application units (1); and
- said interface facility comprising a dedicated high-priority connection (42) adapted for transmitting flow control information between said modem unit (2) and at least one of the application units (1).

34. A method for coordinating data flow in a user equipment for mobile communication, said user equipment comprising at least one application unit and a modem unit (2), with at least one application being installed on at least one of the application units (1), said method comprising steps of:

- setting up one or more connections between at least one of the application units (1) and the modem unit (2) via at least one physical interface (3);
- transmitting data traffic of at least one of the applications as well as flow control information via said one or more connections.

35. Computer program product, comprising computer program means adapted to perform the method steps as defined in claim 34 when said computer program product is executed on a mobile device, processing system, digital signal processor, or the like.

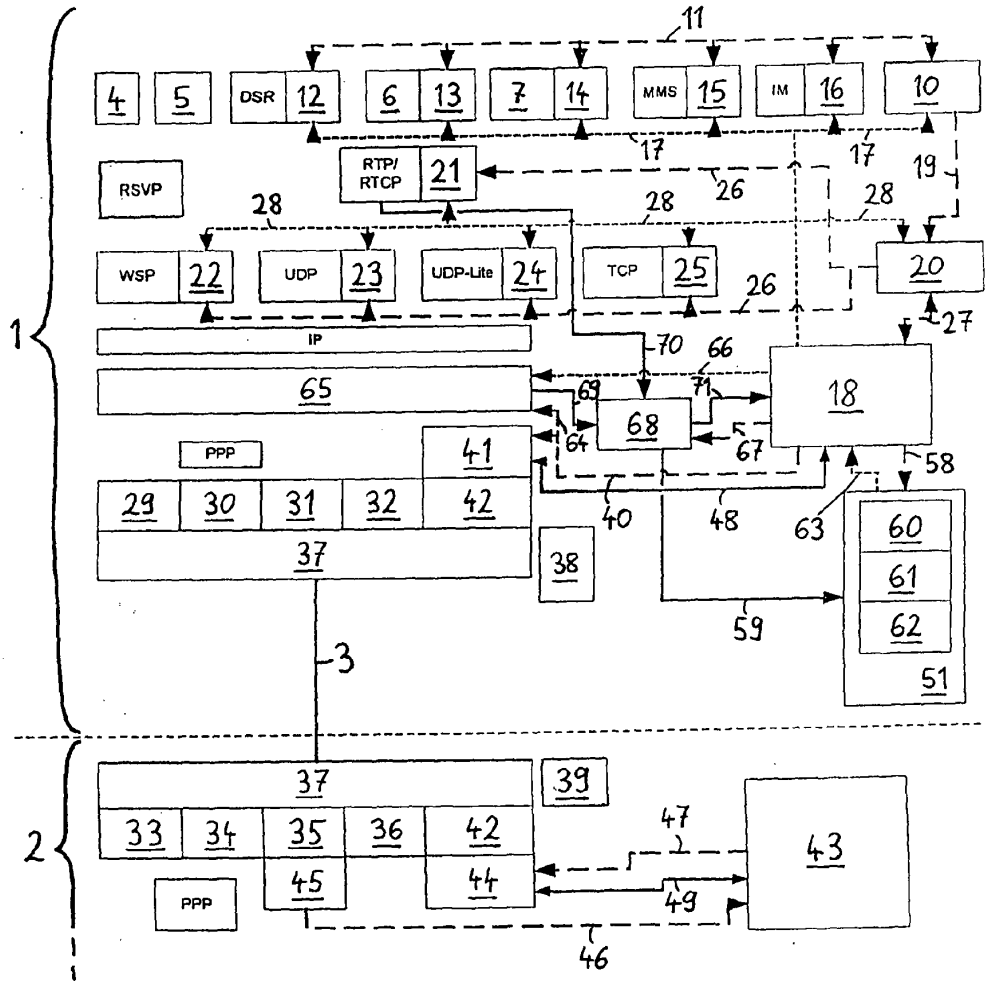

11
4
5
DSR
12
6
13
7
14
MMS
15
IM
16
10
17
17
19
RSVP
RTP/
RTCP
21
26
28
28
28
WSP
22
UDP
23
UDP-Lite
24
TCP
25
20
26
27
1
IP
70
66
65
69
71
18
68
64
67
58
PPP
41
29
30
31
32
42
40
48
63
60
37
38
61
62
59
51
3
37
39
33
34
35
36
42
47
43
2
45
44
49
PPP
46

Fig. 1

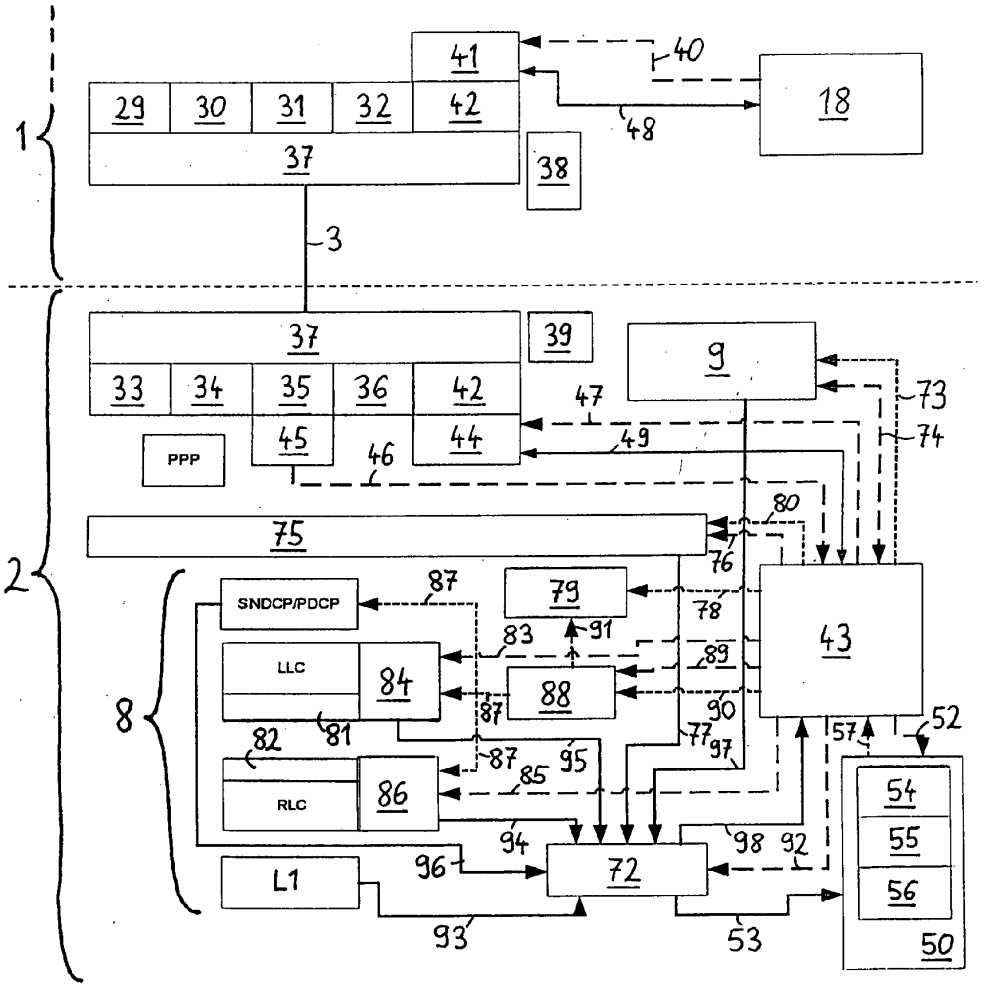

1
2
3
8
29
30
31
32
41
42
37
38
40
48
18
37
39
33
34
35
36
42
45
44
PPP
46
47
49
9
73
74
75
80
76
SNDCP/PDCP
87
79
78
43
83
91
LLC
84
88
89
90
87
82
81
77
97
95
RLC
86
85
52
57
54
55
56
50
94
98
92
96
72
L1
93
53

Fig. 2

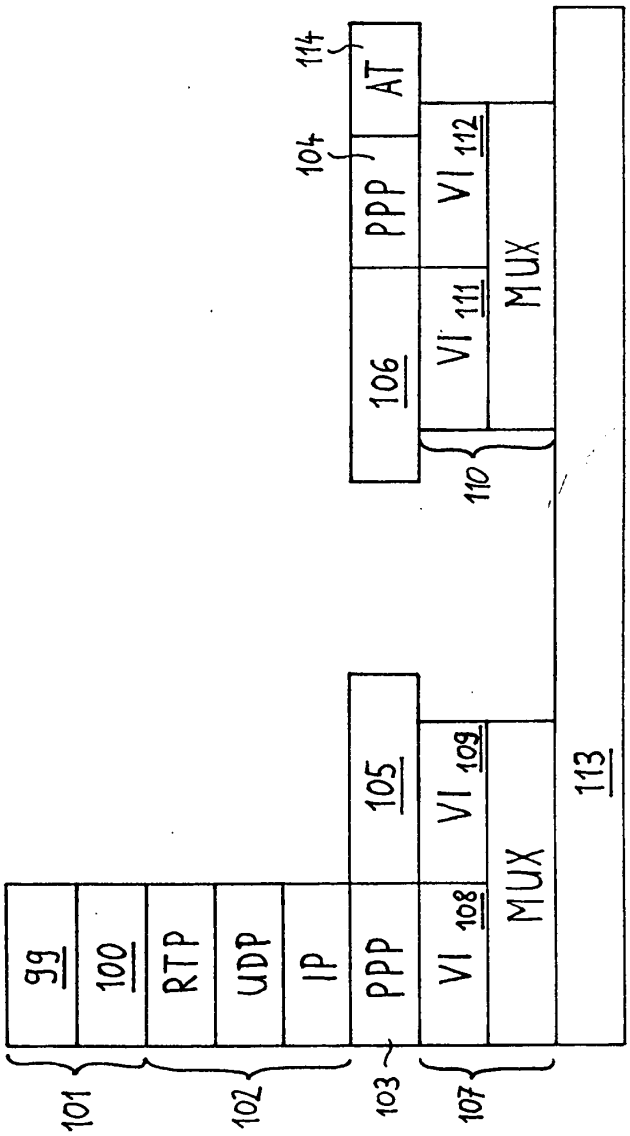

99
100
RTP
UDP
IP
PPP
105
VI 108
VI 109
MUX
113
106
VI 111
MUX
VI 112
PPP
AT
101
102
103
107
110
104
114

Fig. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 01 7485

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 2003/145119 A1 (BENDER PAUL E ET AL) 31 July 2003 (2003-07-31) * figures 3A,3B,4 * * paragraphs [0005],[0006],[0012]-[0014],[0027] * ---	1-35	H04L12/56 G06F13/38 H04L29/06 H04M11/06
A	BLAKE ET AL: "RFC 2475 - An Architecture for differentiated services" IETF, 31 December 1998 (1998-12-31), XP002267765 INET Retrieved from the Internet: <URL:ftp://ftp.isi.edu/in-notes/rfc2475.txt> [retrieved on 2004-01-22] * paragraph [2.3.3] - paragraph [2.3.3.4] * ---	12,13, 16,17, 25,26	
A	XYLOMENOS ET AL.: "LINK LAYER SUPPORT FOR QUALITY OF SERVICE ON WIRELESS INTERNET LINKS" IEEE PERSONAL COMMUNICATIONS, IEEE COMMUNICATIONS SOCIETY, US, vol. 6, no. 5, October 1999 (1999-10), pages 52-60, XP000853485 ISSN: 1070-9916 * page 58, right-hand column, line 1 - page 59, right-hand column, line 1 * * figure 11 * ---	3,7,19, 24	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L G06F H04M H04Q
A	EP 1 168 730 A (NOKIA INC) 2 January 2002 (2002-01-02) * figures 1-3,7 * ---	1,18,30, 33-35	
	-/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	16 February 2004	Siebel, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 01 7485

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	LEMME H: "INFRAROT-DATEN-UBERTRAGUNG WIRD SCHNELLER. IRDA-SCHNITTSTELLE JETZT MIT BIS ZU 4 MBIT/S" ELEKTRONIK, FRANZIS VERLAG GMBH. MUNCHEN, DE, vol. 45, no. 3, 6 February 1996 (1996-02-06), pages 38-40,42,44, XP000553701 ISSN: 0013-5658 * page 42, left-hand column, line 1-5 * ---	1,2	
A	TRAVIS B: "EASE FILE TRANSFERS WITH IRDA-PROTOCOL WIRELESS INFRARED" EDN ELECTRICAL DESIGN NEWS, CAHNERS PUBLISHING CO. NEWTON, MASSACHUSETTS, US, vol. 40, no. 7, 30 March 1995 (1995-03-30), pages 59-64,66,68, XP000524757 ISSN: 0012-7515 * page 63 * ---	1-35	
A	PANIAN J ET AL: "The IP Modem Interface Standard" IP MODEM INTERFACE STANDARD DRAFT, XX, XX, 6 May 1998 (1998-05-06), pages 1-26, XP002120914 * page 10 * -----	1,18,30, 33-35	TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	16 February 2004	Siebel, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 01 7485

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-02-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003145119 A1	31-07-2003	US 6535918 B1	18-03-2003
		AU 6047399 A	10-04-2000
		CN 1115825 B	23-07-2003
		EP 1116359 A2	18-07-2001
		JP 2002525973 T	13-08-2002
		WO 0018066 A2	30-03-2000
EP 1168730 A	02-01-2002	EP 1168730 A2	02-01-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－275145

(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ａ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ａ

審査請求　有　　請求項の数８　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－74095

(22)出願日　平成10年(1998)３月23日

特許法第30条第１項適用申請有り　平成９年９月24日～９月26日　社団法人情報処理学会主催の「情報処理学会第55回（平成９年後期）全国大会」において文書をもって発表

(71)出願人　396011680
株式会社エイ・ティ・アール環境適応通信研究所
京都府相楽郡精華町大字乾谷小字三平谷５番地

(72)発明者　小菅　昌克
京都府相楽郡精華町大字乾谷小字三平谷５番地　株式会社エイ・ティ・アール環境適応通信研究所内

(72)発明者　松田　潤
京都府相楽郡精華町大字乾谷小字三平谷５番地　株式会社エイ・ティ・アール環境適応通信研究所内

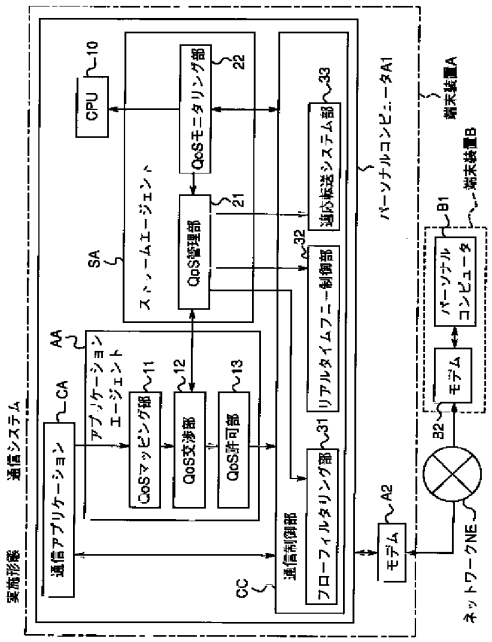
(74)代理人　弁理士　青山　葆　（外２名）

(54)【発明の名称】　通信サービス品質制御方法及び装置

(57)【要約】

【課題】　通信システムの環境の変動に対してリアルタイムに対応してＱｏＳを適切に制御することができる通信サービス品質制御方法及び装置を提供する。

【解決手段】　通信ストリーム毎にアプリケーションエージェントＡＡと、ストリームエージェントＳＡとを生成する。アプリケーションエージェントＡＡは、対応する通信ストリームに対して適当な通信サービスの品質とその制御基準を設定し、自端末装置内及び相手方との間で通信サービスの品質の交渉を行って通信サービスの品質を選択してテストし実現可能であるときに当該通信サービスの品質を通信制御部ＣＣに通知して設定し、通信ストリーム集合に対する総合の効用値を表わす評価関数値が、リソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときはその調整を行って設定し、ストリームエージェントＳＡはそれに基づいて自律的に制御する。



【特許請求の範囲】
【請求項１】　ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた端末装置の通信サービス品質制御方法において、
通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントと、ストリームエージェントとを生成し、
上記アプリケーションエージェントは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、
上記ストリームエージェントは、上記アプリケーションエージェントによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御することを特徴とする通信サービス品質制御方法。
【請求項２】　上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数であることを特徴とする請求項１記載の通信サービス品質制御方法。
【請求項３】　上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする請求項１又は２記載の通信サービス品質制御方法。
【請求項４】　上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする請求項１乃至３のうちの１つに記載の通信サービス品質制御方法。
【請求項５】　ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた通信サービス品質制御装置において、
通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントの第１の機能処理手段と、ストリームエージェントの第２の機能処理手段とを生成する生成手段とを備え、
上記第１の機能処理手段は、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、
上記第２の機能処理手段は、上記第１の機能処理手段によって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御することを特徴とする通信サービス品質制御装置。
【請求項６】　上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数であることを特徴とする請求項５記載の通信サービス品質制御装置。
【請求項７】　上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする請求項５又は６記載の通信サービス品質制御装置。
【請求項８】　上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする請求項５乃至７のうちの１つに記載の通信サービス品質制御装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばネットワークを介して接続された複数の端末装置間の通信サービスの品質（以下、ＱｏＳという。）を制御する通信サービス品質制御方法及び装置に関する。
【０００２】
【従来の技術】従来より、モバイル通信、マルチメディア通信、および、パーソナル通信を利用する形態の情報通信アプリケーションが普及し、今後また、日常生活の様々な場面で個人に密に関わってくると予想される。このような情報通信アプリケーションでは、利用の都度、

あるいは利用中においても、その動作環境（ネットワーク環境、端末環境、ユーザ環境）が変わるため、そのときどきの動作環境に即した通信のコーディネーションを行う機能が求められている。

【０００３】動画や音声等の連続ストリームを扱うマルチメディア通信を実現するためには、端末のリソース（ＣＰＵ、メモリ、デバイス等）やネットワークのリソース（帯域等）を端末装置－端末装置間で管理して制御する必要がある。現在、そのための技術として、ＱｏＳブローカー（Ｂｒｏｋｅｒ）（以下、従来例という。）が提案されている（例えば、従来技術文献１「Ｋｌａｒａ Ｎａｈｒｓｔｅｄｔｅｔ ａｌ．，“Ｔｈｅ ＱｏＳ Ｂｒｏｋｅｒ”，ＩＥＥＥ Ｍｕｌｔｉｍｅｄｉａ，Ｓｐｒｉｎｇ １９９５，Ｖｏｌ．２，Ｎｏ．１，ｐｐ．５３－６７」参照。」）。

【０００４】

【発明が解決しようとする課題】しかしながら、従来例のＱｏＳブローカーにおけるリソース管理の仕組みでは、自端末装置のリソース、ネットワークリソース、相手端末装置のリソースを順にサイクルで制御し、管理している。この仕組みでは、リソースの状況が刻々と変化するような環境では、リソースの再確保が頻繁に起こり、環境の変動に対してリアルタイムに対応できないという問題点があった。

【０００５】本発明の目的は以上の問題点を解決し、通信システムの環境の変動に対してリアルタイムに対応してＱｏＳを適切に制御することができる通信サービス品質制御方法及び装置を提供することにある。

【０００６】

【課題を解決するための手段】本発明に係る請求項１記載の通信サービス品質制御方法は、ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた端末装置の通信サービス品質制御方法において、通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントと、ストリームエージェントとを生成し、上記アプリケーションエージェントは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、上記ストリームエージェントは、上記アプリケーションエージェントによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御することを特徴とする。

【０００７】また、請求項２記載の通信サービス品質制御方法は、請求項１記載の通信サービス品質制御方法において、上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数である。

【０００８】さらに、請求項３記載の通信サービス品質制御方法は、請求項１又は２記載の通信サービス品質制御方法において、上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする。

【０００９】またさらに、請求項４記載の通信サービス品質制御方法は、請求項１乃至３のうちの１つに記載の通信サービス品質制御方法において、上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする。

【００１０】本発明に係る請求項５記載の通信サービス品質制御装置は、ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた通信サービス品質制御装置において、通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントの第１の機能処理手段と、ストリームエージェントの第２の機能処理手段とを生成する生成手段とを備え、上記第１の機能処理手段は、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、上記第２の機能処理手段は、上記第１の機能処理手段によって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービ

スの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御することを特徴とする。

【００１１】また、請求項６記載の通信サービス品質制御装置は、請求項５記載の通信サービス品質制御装置において、上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数であることを特徴とする。

【００１２】さらに、請求項７記載の通信サービス品質制御装置は、請求項５又は６記載の通信サービス品質制御装置において、上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする。

【００１３】またさらに、請求項８記載の通信サービス品質制御装置は、請求項５乃至７のうちの１つに記載の通信サービス品質制御装置において、上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする。

【００１４】

【発明の実施の形態】以下、図面を参照して本発明に係る実施形態について説明する。

【００１５】図１は、本発明に係る一実施形態である通信サービス品質（ＱｏＳ）調整機能を備えた端末装置を備えた通信システムの構成を示すブロック図である。図１において、端末装置Ａは、通信サービス品質（ＱｏＳ）調整機能を備え、パーソナルコンピュータＡ１とモデム（変復調装置）Ａ２とを備えて構成され、ここで、パーソナルコンピュータＡ１はモデムＡ２、並びに、例えば電話回線、ＩＳＤＮ回線、インターネットなどのネットワークＮＥを介して端末装置Ｂに接続される。端末装置Ｂは、端末装置Ａと同様に、パーソナルコンピュータＢ１及びモデムＢ２を備えて構成される。

【００１６】本実施形態のパーソナルコンピュータＡ１は、（ａ）通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェント（ソフトウエアによる機能処理手段）ＡＡと、ストリームエージェント（ソフトウエアによる機能処理手段）ＳＡとを生成し、

（ｂ）アプリケーションエージェントＡＡは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、（ｃ）ストリームエージェントＳＡは、上記アプリケーションエージェントＡＡによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して通信制御部ＣＣに通知して設定することにより自律的に通信ストリームを制御することを特徴としている。ここで、上記評価関数は、好ましくは、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数である。また、上記リソースは、好ましくは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含む。

【００１７】従って、本実施形態の通信システムは、通信ストリーム毎にエージェントを配置し、事前に決定したＱｏＳと制御ポリシに基づいて、それぞれのエージェントが自律的に通信ストリームを制御し、リソース管理を行うことで、環境の変動に迅速に対応することを特徴としている。ここで、エージェントとは、外部からの入力に対して自律的に動作の判断と制御を行うソフトウェアモジュールのことであり、制御ポリシー又は制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含む。ここで、ＱｏＳの調整方法では、例えば、（Ｉ）平均的なＱｏＳではじめに制御を行ない、現在のリソースの状態に従って、指定されたＱｏＳ範囲内でＱｏＳを上昇（又は下降）させる方法、（II）現在のＱｏＳで制御が困難になった場合に、優先度が低いパタメータから順にＱｏＳを下降させる方法、もしくは、（III）次にユーザの満足度の高いパラメータ集合にＱｏＳを変更する方法、などの方法がある。

【００１８】図１に示すように、パーソナルコンピュータＡ１は、通信処理の動作を制御するハードウエアであるＣＰＵ１０と、端末装置Ｂとデータ通信を行う通信アプリケーション（ソフトウエア）ＣＡと、上記データ通信の制御を行う通信制御部（ソフトウエア）ＣＣと、ユーザ要求に基づいてＱｏＳとＱｏＳマネジメントポリシー（ＱｏＳ管理ポリシー）を算出するアプリケーションエージェントＡＡと、マルチメディア通信のストリーム毎に生成されアプリケーションエージェントＡＡによって算出されたＱｏＳとＱｏＳマネジメントポリシー基づいて従って各ストリームを自律的に制御するストリーム

エージェントＳＡとを備える。ここで、アプリケーションエージェントＡＡは、ＱｏＳマッピング部１１と、ＱｏＳ交渉部（ＱｏＳネゴシエーション部）１２と、ＱｏＳ許可部（ＱｏＳアドミッション部）１３とを備える。また、ストリームエージェントＳＡは、ＱｏＳ管理部２１と、ＱｏＳモニタリング部２２とを備える。さらに、通信制御部ＣＣは、フローフィルタリング部３１と、リアルタイムフロー制御部３２と、適応転送システム部３３とを備える。以下、パーソナルコンピュータＡ１の処理及び動作の詳細について説明する。

【００１９】まず、適応型情報通信アプリケーションについて説明する。上述したように、今後の高度情報通信社会においては、モバイル通信、マルチメディア通信、及びパーソナル通信を利用する形態の情報通信アプリケーションが普及し、日常生活の様々な場面で個人に密に関わってくる。

【００２０】誰もがこのようなアプリケーションを日常的に気軽に利用できるようにするためには、極めて多様で流動的な動作環境で適応的に通信コーディネーションを行う機能がアプリケーションに求められる。すなわち、使用するネットワークや、ときには端末までもがアプリケーション利用の都度、異なることがあり、その結果、使用できるリソース、性能がそのときどきで異なってくる。さらに、マルチメディアストリームを取り扱う場合には、そこで処理する負荷の特性も一定していない。この場合には、使用可能なリソース、性能、メディアストリームの負荷特性などに応じて受信処理できるＱｏＳの選択などの通信コーディネーションが必要である。とくに、携帯端末を使用してワイヤレスアクセスリンク経由でモバイルマルチメディア通信を利用する場合（例えば、図６参照。）には、相手側（例えば、高速広帯域アクセスリンク経由で通信できる高性能ワークステーション）との間の、使用可能リソース量や性能の差により、双方で扱えるメディアストリームのＱｏＳに差が生じることがある。この場合には、受信処理できるメディアストリームに変換するためのＱｏＳ調整などの通信コーディネーションが必要である。

【００２１】また、ワイヤレスアクセスリンクの不安定な伝送環境や、ハンドオーバによる使用可能伝送帯域の変更、携帯端末の電池残量の変化などにより、アプリケーション利用中にも動作環境が変わり得る。この場合にも、スムーズなメディアストリーム処理を可能にするための動的なＱｏＳ調整が必要である。

【００２２】また、これらの物理的な動作環境（ネットワーク環境、端末環境）のほかに、ユーザ個々人のＴＰＯ、ニーズ、好みに応じた多様な利用形態が出現し得るが、この場合には、そのときどきのユーザの状況に合った通信形態の選択などの通信コーディネーションが必要である。また、ユーザ相互の要求が相反する場合には、お互いの要求を調整することも必要になってくる。前述のメディアストリームのＱｏＳ調整についても、ユーザ個々人の要求、好みに合わせてＱｏＳ調整が行われることが必要である。

【００２３】このように、そのときどきの動作環境（ネットワーク環境、端末環境、ユーザ環境）に即して、使用リソース、メディアストリームのＱｏＳ、通信形態、さらにはアプリケーション自身の機能・構成までをも自律的に調整して通信コーディネーションを行う適応型情報通信アプリケーションを実現するためのシステムアーキテクチャについて以下に開示する。

【００２４】次いで、適応型情報通信アプリケーションのためのフレームワークについて説明する。図７は、図１の通信システムで用いるＱｏＳアーキテクチャのためのフレームワークの基本構成を示すブロック図である。このフレームワークは主として次の４つのモジュール群から構成されている。（ａ）パーソナルエージェント群、（ｂ）アプリケーションエージェント群、（ｃ）ストリームエージェント群、及び、（ｄ）リソースマネージャ群。

【００２５】ここで、通信アプリケーションＣＡを含むパーソナルエージェントはユーザの好みや要求を把握し、ユーザ要求の変更を受けつける。また、アプリケーションエージェントＡＡは各アプリケーション毎に生成され、ＱｏＳの交渉とリソース予約の制御を行う。ストリームエージェントＳＡは、各ストリーム毎に生成され、指定されたＱｏＳに従ってストリームを自律的に制御する。通信制御部ＣＣを含むリソースマネージャはＣＰＵや通信リンク帯域等のリソースの管理を行う。フレームワークにおけるエージェント群は、ＱｏＳメカニズムの機能を利用もしくは実現し、アプリケーションに適応性を付与する。

【００２６】次いで、ＱｏＳメカニズムとフレームワークについて説明する。ここで、リソース管理（マネジメント）におけるＱｏＳメカニズムは以下の３つに分類することができる。（ａ）ＱｏＳ提供機構（QoS Provision Mechanisms）、（ｂ）ＱｏＳ制御機構（QoS Control Mechanisms）、及び、（ｃ）ＱｏＳ管理機構（QoS Management Mechanisms）。ここで、ＱｏＳ提供機構は、フローの確立とＱｏＳ交渉といった静的なリソース管理を行う。一方、ＱｏＳ制御機構とＱｏＳ管理機構は、メディア転送時の動的なリソース管理を行う。ＱｏＳ制御機構はＱｏＳ管理機構より処理のタイムスケールが短い、リアルタイムなフロー制御やフローのフィルタリング等を行う。アプリケーションエージェントＡＡはＱｏＳマッピングや許可、テスト等のＱｏＳ提供機構を利用してＱｏＳの交渉とリソース予約の制御を行い、フローを確立する。

【００２７】ストリームエージェントＳＡはＱｏＳの保守管理やＱｏＳ適応制御等のＱｏＳ管理機構の機能を実現し、ストリーム制御に適応性を付与する。またそれぞ

れのエージェントは、フローのリアルタイムな制御のためにＱｏＳ制御機構の機能を利用する。

【００２８】次いで、フレームワーク内のアプリケーションエージェントＡＡとストリームエージェントＳＡの基本動作フローについて図１を参照して説明する。

【００２９】まず、各アプリケーションエージェントＡＡは、例えば通信アプリケーションＣＡであるパーソナルエージェントからのユーザ要求をもとにＱｏＳとＱｏＳマネジメントポリシーを算出する。通信アプリケーションＣＡからストリームの生成要求が発生した場合、各アプリケーションエージェントＡＡはネットワークや端末のリソース環境を考慮し、ユーザ要求をもとにアプリケーションに対して妥当なＱｏＳをストリーム毎に算出することにより、ＱｏＳのマッピングを行う。同時に、複数のアプリケーションが存在する場合は、各アプリケーションエージェントＡＡ間で交渉を行い、許可及びテスト機能を利用して、実現可能なＱｏＳを選択する。必要な場合は通信相手や通信コーディネーションサーバのアプリケーションエージェントＡＡと端末装置Ａと端末装置Ｂとの間で交渉を行う。このようにして選択した１つ又は複数のＱｏＳとＱｏＳマネジメントポリシーをそれぞれのストリームエージェントＳＡに通知する。この処理は、ユーザの品質要求が変化した場合にも行われる。また、リソースが不足した場合等にはストリームエージェントＳＡからの要求を受けてＱｏＳの再交渉も行う。

【００３０】次いで、ストリームエージェントＳＡはそれぞれのストリーム毎に生成され、アプリケーションエージェントＡＡ群によって割り出されたＱｏＳとＱｏＳマネジメントポリシー（ＱｏＳ管理ポリシー）に従って各ストリームを自律的に制御する。ストリームエージェントＳＡは端末装置Ａ内のローカルな環境でストリームとストリームに関連するリソースのモニタリングを行い、ＱｏＳ制御機構の機能を利用してストリームと使用リソースの調整を自律的に行うことでＱｏＳ保守及びＱｏＳ適応制御機能を実現する。ストリームエージェントＳＡはまず最初に、与えられたＱｏＳを維持しようとする。しかしながら、端末装置Ａ全体としてのリソース使用量が増加したり、ネットワークリソースが変動してＱｏＳの維持が困難になった場合、ストリームエージェントＳＡはＱｏＳマネジメントポリシーに従って複数のＱｏＳを自律的に切り替える。この際、必要であればストリームエージェントＳＡ間での調整を行う。ストリームエージェントＳＡ群での調整が不可能になった場合、アプリケーションエージェントＡＡ群にＱｏＳの再交渉を要求する。

【００３１】次いで、ＱｏＳとＱｏＳマネジメントポリシーについて説明する。ＱｏＳマネジメントポリシーは、与えられたＱｏＳの範囲の中からユーザ要求を最大に反映したリソース制御を行うための指針となる。ＱｏＳとＱｏＳマネジメントポリシーは、（ａ）幅を有するＱｏＳと、（ｂ）アプリケーション、ストリーム、各ＱｏＳパラメータ毎の優先度と、（ｃ）複数のＱｏＳパラメータセットとユーティリティ（ユーザにとっての効用、満足度）とに基づいて算出する。ＱｏＳ調整にユーザ要求を反映する仕組みとして、次式の数１で与えられる総合ユーティリティ関数Ｕを、次式の数２のリソース制約条件の下で最大化することにより、ユーザ要求を反映したメディアストリームのＱｏＳ調整を実現する。

【００３２】

【数１】

$$U = \sum_{\Lambda} w(A) \cdot \log u(A, q)$$

【数２】

$$\sum_{A} r_m(A, q) \leqq R_m$$

【００３３】ここで、ｕ（Ａ，ｑ）は、ストリーム集合Ａのうちの各ストリームのＱｏＳが品質ｑであるときの個別ユーティリティ（ユーザの効用値、ユーザの効用度、又はユーザの満足度をいう。）であり、ｗ（Ａ）は、ストリーム集合Ａのうちの各ストリームの優先度又は重み付け係数であり、予め決められる。また、ｒ（Ａ，ｑ）は、ストリーム集合Ａの各ストリームをＱｏＳ・ｑで処理するのに必要なリソースｍの量である。リソース量はＣＰＵの使用量と通信回線の伝送帯域を含む。R_mは、リソースｍの利用可能限度量又はリソース量の最大値である。このようにして得られるＱｏＳをストリームエージェントＳＡに通知する際の指定方法は、ＱｏＳの範囲を指定する方法や、テーブルで離散的に指定する方法を用いることができる。ストリームエージェントＳＡのリアクティブ性を考慮した場合、後者の方法が有効である。

【００３４】次いで、フレームワークのエージェントモデルについて説明する。複数のアプリケーションが存在する場合、ＱｏＳ交渉はアプリケーションエージェントＡＡによるマルチエージェントシステムを構成することとなる。フロー確立時のＱｏＳ交渉は、実時間性に対する要求はそれほど強くないため、分散人工知能の分野で研究されている高度な分散問題解決手法が利用可能である。同等な優先度やユーティリティを持つ可能性のあるＱｏＳ交渉では、譲り合いといった機能が必要となる。また、常に変化する端末やネットワーク環境においては長期的な戦略のような仕組みがなければ頻繁に再交渉が発生する可能性が考えられる。これらを実現するために、エージェントによるＱｏＳ交渉方式に社会システムや市場モデルを適用することができる。また、ＱｏＳ交渉のレベルでは準最適解を見つけだすことにとどめ、ＱｏＳマネジメントポリシーといった形で細かいＱｏＳ制御を可能なようにし、よりリアクティブな（反応的な、又は応答的な）エージェントによって環境の変動に応じ

て微調整する方法が有効である。

【００３５】さらに、ＱｏＳ調整機能を備えた図１のパーソナルコンピュータＡ１内の各機能部の基本的な処理について説明する。まず、アプリケーションエージェントＡＡ内のＱｏＳマッピング部１１は、ユーザ指定のＱｏＳをシステムやネットワークに対応したＱｏＳに変換してＱｏＳ交渉部１２に出力する。また、ＱｏＳ交渉部１２は、相手端末装置ＢのＱｏＳ交渉部１２と通信を行い、アプリケーション毎に最適なＱｏＳと制御ポリシーを算出してＱｏＳ許可部１３に出力する。さらに、ＱｏＳ許可部１３は、リソース予約プロトコル等を使ってＱｏＳで指定されたリソース量が利用可能かをテストする。

【００３６】そして、通信制御部ＣＣ内のリアルタイムフロー制御部３２は、ＱｏＳ管理部２１から与えられたＱｏＳに従ってリアルタイムにフローの品質を制御する。また、フローフィルタリング部３１は、ＱｏＳ管理部２１から与えられたＱｏＳに従ってフローのスケーリングを行い、具体的には、動画の場合は、指定されたフレームレート以上のストリームが来た場合に、過剰なフレームを落とすことを行う。さらに、適応転送システム部３３は、ＱｏＳ管理部２１から与えられたＱｏＳに最適な通信トランスポート機能を形成し、具体的には、品質が非常に悪いネットワークに対してはＦＥＣ（前方エラー訂正：Ｆｏｒｗａｒｄ　ＥｒｒｏｒＣｏｒｒｅｃｔｉｏｎ）コードを付与したり、高速かつ高品質なネットワークにおいては、誤り制御機能をはずしたりする。

【００３７】また、ストリームエージェントＳＡ内のＱｏＳ管理部２１は、ＱｏＳ交渉部１２から与えられたＱｏＳを維持できるようにシステムとネットワークのモニタリング結果（ＱｏＳモニタリング部２２による）に基づいて、通信制御部ＣＣ内のリアルタイムフロー制御部３２と、フローフィルタリング部３１と、適応転送システム部３３との処理を制御する。そして、ＱｏＳ管理部２１は、ＱｏＳが維持できない場合、制御ポリシーに従ってＱｏＳを変更する一方、変更不可能な場合は、ＱｏＳ交渉部１２に対してＱｏＳの再交渉を要求する。さらに、ＱｏＳモニタリング部２２は、ＣＰＵ１０の動作をモニタリングしてＣＰＵ使用量を検出するとともに、通信制御部ＣＣからの通信状況データに基づいてストリームで占有する伝送帯域を検出することにより、システム及びネットワークのモニタを行い、モニタリング結果を逐次ＱｏＳ管理部２１に送る。

【００３８】次いで、本実施形態におけるＱｏＳ制御手順の基本手順について説明する。

（１）ユーザが通信アプリケーションＣＡ上で希望する通信品質を指定して通信を要求する。

（２）通信アプリケーションＣＡからユーザの通信要求が発生するとアプリケーションエージェントＡＡはユーザの要求する品質を取得し、ＱｏＳマッピング部１１により実際のＱｏＳに変換する。

（３）変換されたＱｏＳに応答して、ＱｏＳ交渉部１２はストリーム毎のＱｏＳとＱｏＳ制御ポリシーを算出する。

（４）算出されたＱｏＳが実現可能かをＱｏＳ許可部１３がテストを行う。

（５）算出された実現不可能の場合は、ＱｏＳ交渉部１２に再計算を要求する。

（６）算出されたＱｏＳが実現可能な場合、リアルタイムフロー制御部３２、フローフィルタリング部３１及び適応転送システム部３３に渡され、各機能部３１，３２，３３はＱｏＳに従って通信制御のフローを制御する。

（７）算出されたＱｏＳは、ストリームエージェントＳＡにも渡される。

（８）ストリームエージェントＳＡはＱｏＳモニタリング部２２でネットワークＮＥのリソース（具体的には、伝送帯域）と端末装置Ａのリソース（具体的には、ＣＰＵ使用量）の状況をモニタしている。

（９）ＱｏＳ管理部２１は、ＱｏＳに従ってそのＱｏＳが達成されるようにリアルタイムフロー制御部３２、フローフィルタリング部３１及び適応転送システム部３３の処理を制御する。

（１０）通信制御部ＣＣ内の各機能部３１，３２，３３は、ＱｏＳの値を制御ポリシーに従ってＱｏＳモニタリング２２から得たモニタ値を元に調整する。

（１１）ＱｏＳを調整できないときは、周期的にアプリケーションエージェントＡＡにＱｏＳの再交渉を要求する。

【００３９】図２乃至図５は、図１のパーソナルコンピュータＡ１の各機能部である通信アプリケーションＣＡ、アプリケーションエージェントＡＡ、ストリームエージェントＳＡ及び通信制御部ＣＣの処理の詳細を示すフローチャートである。

【００４０】図２において、通信アプリケーションＣＡは、ステップＳ１においてストリームの作成要か否かを判断し、ＹＥＳのときステップＳ２においてストリームを作成してステップＳ３に進む一方、ステップＳ１でＮＯであれば直接にステップＳ３に進む。ステップＳ３においてユーザ要求有り又は変更有りか否かを判断し、ＮＯであればステップＳ１に戻る一方、ＹＥＳであればステップＳ４においてアプリケーションエージェントＡＡに対してユーザ要求する。すなわち、ユーザ要求があったことを通知してステップＳ１に戻る。

【００４１】図２のアプリケーションエージェントＡＡのステップＳ１０では、ユーザ要求があったか否かが判断され、あるまでステップＳ１０のループ処理を実行し、ユーザ要求があったときは、ステップＳ１１に進む。ステップＳ１１において、アプリケーションエージェントＡＡのＱｏＳマッピング部１１は、ユーザ要求に

基づいて、通信アプリケーションＣＡに対して妥当なＱｏＳとＱｏＳマネージメントポリシー（ＱｏＳ管理ポリシー）をストリーム毎に算出する。次いで、図３のステップＳ１２では、複数のアプリケーションが存在するか否かを判断し、ＹＥＳであればステップＳ１３においてＱｏＳ交渉部１２は、各アプリケーションのアプリケーションエージェントＡＡ間で通信を行ってＱｏＳの交渉を行い、アプリケーション毎に最適なＱｏＳと制御ポリシーを算出してステップＳ１４に進む。一方、ステップＳ１２でＮＯであれば直接にステップＳ１４に進む。ステップＳ１４において相手端末装置Ｂと交渉が必要か否かを判断し、ＹＥＳであればステップＳ１５においてＱｏＳ交渉部１２は、端末装置間でＱｏＳの交渉を行ってステップＳ１６に進む。一方、ステップＳ１４でＮＯであれば直接にステップＳ１６に進む。

【００４２】ステップＳ１６でＱｏＳ許可部１３は、選択されたＱｏＳが実現可能かをテストする。具体的には、リソース予約プロトコルを用いて、ＱｏＳで指定されたリソース量が利用可能であるか否かをテストする。ステップＳ１７において実現可能か否かを判断し、ＮＯであればステップＳ１２に戻る一方、ＹＥＳであればステップＳ１８で上記得られたＱｏＳを通信制御部ＣＣに対して出力して設定する。これに応答して、通信制御部ＣＣは、ステップＳ５１で受信したＱｏＳを設定する。

【００４３】アプリケーションエージェントＡＡのステップＳ１８の後に、図４のステップＳ１９では、ステップＳ１９において対応するストリームエージェントが存在するか否かを判断し、ＹＥＳのときはそのままステップＳ２１に進むが、ＮＯであればステップＳ２０においてストリームエージェントＳＡを生成してステップＳ２１に進む。これに応答して、ストリームエージェントＳＡはステップＳ３１でモニタを起動し、すなわち、ストリームエージェントＳＡのＱｏＳモニタリング部２２の処理を起動してステップＳ２１に進む。対応するストリームエージェントＳＡの処理では、ステップＳ３０からステップＳ３１を実行する。

【００４４】アプリケーションエージェントＡＡのステップＳ２１では、得られたＱｏＳとＱｏＳマネージメントポリシーをストリームエージェントＳＡに対して通知する。これに応答して、ストリームエージェントＳＡはステップＳ３２で通知されたＱｏＳでのモニタリングをＱｏＳモニタリング部２２で設定する。

【００４５】アプリケーションエージェントＡＡのステップＳ２１の後、所定の時間の待機（ステップＳ２２）を行い、ステップＳ２３で通信アプリケーションＣＡからのユーザ要求変更があるか否かを判断し、ＹＥＳであれば図２のステップＳ１０に戻る一方、ＮＯであれば図５のステップＳ２４に進む。

【００４６】ストリームエージェントステップＳＡのＱｏＳモニタリング部２２において、まず、ステップＳ４１で現在のＱｏＳ値を取得し、ステップＳ４２において取得したＱｏＳが予め与えられたＱｏＳの範囲内か否かを判断し、ＹＥＳのときステップＳ４４に進む一方、ＮＯのときはステップＳ４３でＱｏＳの範囲から外れたことをストリームエージェントＳＡのＱｏＳ管理部２１に対して通知してステップＳ４４に進む。ステップＳ４４では、所定の時間だけ待機し、ステップＳ４５においてモニタ終了か否かを判断し、ＹＥＳであれば終了する一方、ＮＯであればステップＳ４１に戻ってモニタリングを再度実行する。

【００４７】ストリームエージェントＳＡのステップＳ３２の後、所定の時間の待機（ステップＳ３３）を行い、ステップＳ３４でＱｏＳモニタリング部２２から通知があったか否かを判断し、ＮＯであればステップＳ３３に戻る一方、ＹＥＳであれば図５のステップＳ３５に進む。ステップＳ３５では、ＱｏＳ管理部２１は新しいＱｏＳの選出し、ステップＳ３６において所定の制約条件のもとで新しいＱｏＳを選出できたか否かを判断し、ＹＥＳであればステップＳ３９に進む一方、ＮＯであればステップＳ３７でストリームエージェントＳＡ間でＱｏＳを調整し、ステップＳ３８においてＱｏＳを調整できたか否かを判断し、ＹＥＳであればステップＳ３９において調整後の新しいＱｏＳを通信制御部ＣＣに対して通知して設定した後図４のステップＳ３３に戻る。一方、ステップＳ３８で調整できずＮＯであるときは、ステップＳ４０でアプリケーションエージェントＡＡに対して再交渉指示通知を出力して図４のステップＳ３０に戻る。一方、アプリケーションエージェントＡＡのステップＳ２４では再交渉指示通知があったか否かを判断し、ＹＥＳであれば図３のステップＳ１２に戻る一方、ＮＯであれば図２のステップＳ１０に戻る。

【００４８】

【実施例】さらに、本発明者は、図１の通信システムの動作評価を行うために、適応型情報通信アプリケーション実験システムを構築して以下のように実験を行った。図８は、図１の通信システムの実施例における実験システムの構成を示すブロック図である。各端末装置Ａ，Ｂにはパーソナルコンピュータ（ＯＳ：ＷｉｎｄｏｗｓＮＴ）を使用し、帯域保証が可能なＡＴＭネットワークを実験用ネットワークとして使用している。カメラを搭載した送信端末装置Ａ，Ｂで取り込んだ動画像をリアルタイムで圧縮した後、ＡＴＭスイッチＡＳＷ経由で受信端末装置Ｃに向けて送信した動画像ストリームＡ及び動画像ストリームＢを受信端末装置Ｃで受信し、画像伸長して２つのウィンドウにそれぞれ表示する環境で実験を行った。

【００４９】次いで、実験システムの動作結果について説明する。図９は、図８の実験システムの動画像ストリームに対するＱｏＳ設定画面を示す正面図であり、動画像ストリームに対するＱｏＳ（ユーザＱｏＳ）設定画面

を示す。受信端末装置Ｃにおいて、ユーザは各動画像に対して自分が要求するＱｏＳパラメータをこのＱｏＳ設定画面から設定することにより所望のＱｏＳの動画像を得る。ＱｏＳ設定画面で設定する項目は、上述下ＱｏＳマネジメントポリシーを算出するために必要な、以下の項目である。

【００５０】（１）符号化は、動画像の圧縮方法である。

（２）セット番号は、（３）～（７）までの項目を１組としたＱｏＳパラメータセットの番号であり、１つのストリームに対して複数組の設定が可能である。

（３）ユーティリティは、以下で設定するＱｏＳの、ユーザにとっての効用であり、数値が大きい程、満足度が大きいことを示す。

（４）フレームレートは、１秒間に表示する画像の枚数であり、枚数が多いほど滑らかな表示になる。

（５）画像サイズは、表示画像の大きさ（横ピクセル数×縦ピクセル数）である。

（６）カラーは、画像の表示色数である。

（７）圧縮クォリティは画像圧縮時の量子化レベルに関連するパラメータであり、数値が大きい程、鮮明な画像が得られる。

（８）優先度（又は優先順）は、ＱｏＳ調整などで考慮する（４）～（７）のパラメータの優先度を指定する。ユーザが設定したフレームレート、画像サイズ、圧縮クォリティなどのＱｏＳパラメータは、アプリケーションエージェントに通知され、そこで、ＣＰＵ使用率、伝送帯域などの必要リソース量の値に変換される。

【００５１】次いで、本システムを用いて行った動作実験の一例を示す。図１０は、図８の実験システムにおける実験開始時の表示画面を示す正面図であり、図１１は、図８の実験システムにおけるユーザ要求変更の設定画面を示す正面図であり、図１２は、図８の実験システムにおけるユーザ要求変更後の表示画面を示す正面図である。

【００５２】まず、図１０に示すように動画像Ａ（画面左のウィンドウに表示）を小さいサイズで表示し、動画像Ｂ（画面左のウィンドウに表示）を大きいサイズで表示している状況から開始する。ここで、図１１のように動画像ＡのＱｏＳ設定画面から、動画像Ａの画面を大きいサイズで表示するようにＱｏＳパラメータをセットし、そのユーティリティを大きい値に設定する。このとき、受信端末装置Ｃでは、設定したＱｏＳパラメータが、動画像Ａのアプリケーションエージェント ＡＡに通知され、必要リソース量の値に変換される。今回の設定では画像のサイズが大きくなったので処理量が増えＣＰＵ使用率が増加する。そこで、動画像Ａのアプリケーションエージェント ＡＡと動画像Ｂのアプリケーションエージェント ＡＡ間の交渉によって動画像Ｂをこのままのサイズで表示することは不可能と判断され、ＣＰＵ使用率を１００％以内に収めるために動画像Ｂを小さいサイズで表示するように交渉によってリソース（ＣＰＵ使用率）の再配分がなされる。この実験例では、両エージェントの交渉が成立するように、動画像ＢのＱｏＳについては小さい画像サイズのユーティリティも大きな値に設定している。

【００５３】受信端末装置Ｃでの交渉の結果は、受信端末の動画像Ａのアプリケーションエージェント ＡＡと送信端末装置Ａのアプリケーションエージェント ＡＡ、受信端末装置Ｃの動画像Ｂのアプリケーションエージェント ＡＡと送信端末Ｂのアプリケーションエージェント ＡＡがそれぞれ個別に交渉して、受信端末装置Ｃから送信端末装置Ａ，Ｂに新しいＱｏＳパラメータ（フレームレート、画像サイズ、圧縮クォリティ）が通知される。送信端末装置Ａ，Ｂでは新たに設定されたＱｏＳパラメータに従って動画像を圧縮し受信端末装置Ｃへ送信する。その結果、図１２に示すように動画像Ａはユーザの要求どおり大きいサイズで表示され、動画像Ｂは小さいサイズの表示に変わる。このように、ＱｏＳエージェント間の交渉によって、ユーザの要求が画像調整に反映されることを確認した。

【００５４】以上説明したように、本実施形態では、適応型情報通信アプリケーションのためのフレームワークとして、メディアストリームのＱｏＳマネジメントを中心に、エージェントに基づくシステムアーキテクチャを考案し、本フレームワークに基づく実験システム、及びそこで確認した動作例を開示した。ここでは、受信端末装置Ｃから送信端末装置Ａ，Ｂに対してＱｏＳパラメータを通知する例を示したが、途中に通信コーディネーションサーバ（フィルタリングなどを行う）を置くことにより、受信端末装置Ｃ－通信コーディネーションサーバ間でローカルにＱｏＳ調整を行うことが可能になる。通信コーディネーションサーバ方式では送信側と受信側の結合を疎にできるため、マルチキャスト環境などで受信側ユーザオリエンティドなＱｏＳ調整の実現が可能になる。

【００５５】以上説明したように本実施形態によれば、各エージェントが与えられたＱｏＳと制御ポリシーに従って自律的にＱｏＳを管理して制御することにより、動的な環境変化に対して迅速に対応できる。また、複雑なＱｏＳ制御を、簡単な装置構成で制御可能となる。ここで、動的な環境変化とは、アプリケーションが使用できるネットワークと端末のリソース、及び性能、さらには、そこで処理する負荷の特性などの状況は、アプリケーション利用の都度異なり得る。特に、ワイヤレスアクセスリンクを使用する場合には、電波状況の不安定な変動や、ハンドオーバによる使用可能伝送帯域の変更などにより、アプリケーション利用中にも動作環境が変わり得る。また、これらの物理的な動作環境のほかに、ユーザ個々人のＴＰＯ（具体的には、ユーザのその時の状態

（たとえば仕事をしているときとか遊んでいるときときとか、ユーザの立場と行なおうとしていること）を意味する。）、ニーズ、好みに応じたアプリケーション利用形態が出現し得る。

【００５６】

【発明の効果】以上詳述したように本発明に係る通信サービス品質制御方法及び装置によれば、ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた端末装置の通信サービス品質制御方法及び装置において、通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントと、ストリームエージェントとを生成し、上記アプリケーションエージェントは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、上記ストリームエージェントは、上記アプリケーションエージェントによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御部手段に通知して設定することにより自律的に通信ストリームを制御する。

【００５７】従って、各エージェントが与えられた通信サービスの品質と制御ポリシーに従って自律的に通信サービスの品質を管理して制御することにより、動的な環境変化に対して迅速に対応できる。また、複雑な通信サービスの品質の制御を、簡単な装置構成で制御可能となる。

【図面の簡単な説明】

【図１】　本発明に係る一実施形態である通信サービス品質（ＱｏＳ）調整機能を備えた端末装置を備えた通信システムの構成を示すブロック図である。

【図２】　図１のパーソナルコンピュータＡ１の各機能部である通信アプリケーションＣＡ、アプリケーションエージェントＡＡ、ストリームエージェントＳＡ及び通信制御部ＣＣの処理の詳細の第１の部分を示すフローチャートである。

【図３】　図１のパーソナルコンピュータＡ１の各機能部である通信アプリケーションＣＡ、アプリケーションエージェントＡＡ、ストリームエージェントＳＡ及び通信制御部ＣＣの処理の詳細の第２の部分を示すフローチャートである。

【図４】　図１のパーソナルコンピュータＡ１の各機能部である通信アプリケーションＣＡ、アプリケーションエージェントＡＡ、ストリームエージェントＳＡ及び通信制御部ＣＣの処理の詳細の第３の部分を示すフローチャートである。

【図５】　図１のパーソナルコンピュータＡ１の各機能部である通信アプリケーションＣＡ、アプリケーションエージェントＡＡ、ストリームエージェントＳＡ及び通信制御部ＣＣの処理の詳細の第４の部分を示すフローチャートである。

【図６】　図１の通信システムで用いるアプリケーション動作環境の一例を示すブロック図である。

【図７】　図１の通信システムで用いるＱｏＳアーキテクチャのためのフレームワークを示すブロック図である。

【図８】　図１の通信システムの実施例における実験システムの構成を示すブロック図である。

【図９】　図８の実験システムのＱｏＳ設定画面を示す正面図である。

【図１０】　図８の実験システムにおける実験開始時の表示画面を示す正面図である。

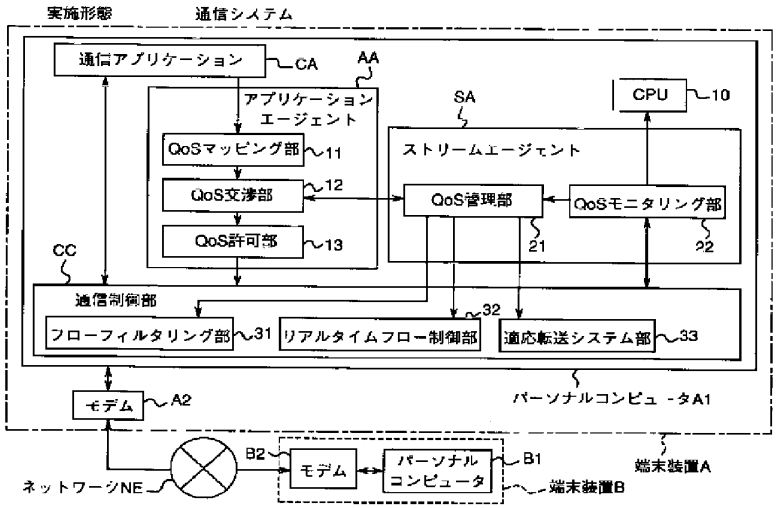
【図１１】　図８の実験システムにおけるユーザ要求変更の設定画面を示す正面図である。

【図１２】　図８の実験システムにおけるユーザ要求変更後の表示画面を示す正面図である。

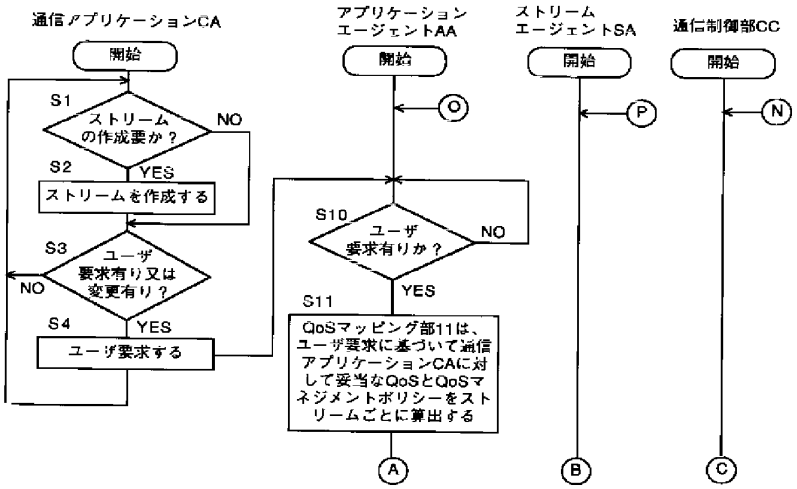
【符号の説明】

Ａ，Ｂ…端末装置、
Ａ１，Ｂ１…パーソナルコンピュータ、
Ａ２，Ｂ２…モデム、
ＮＥ…ネットワーク、
ＣＣ…通信制御部、
ＣＡ…通信アプリケーション、
ＡＡ…アプリケーションエージェント、
ＳＡ…ストリームエージェント、
１０…ＣＰＵ、
１１…ＱｏＳマッピング部、
１２…ＱｏＳ交渉部、
１３…ＱｏＳ許可部、
２１…ＱｏＳ管理部、
２２…ＱｏＳモニタリング部、
３１…フローフィルタリング部、
３２…リアルタイムフロー制御部、
３３…適応転送システム部。

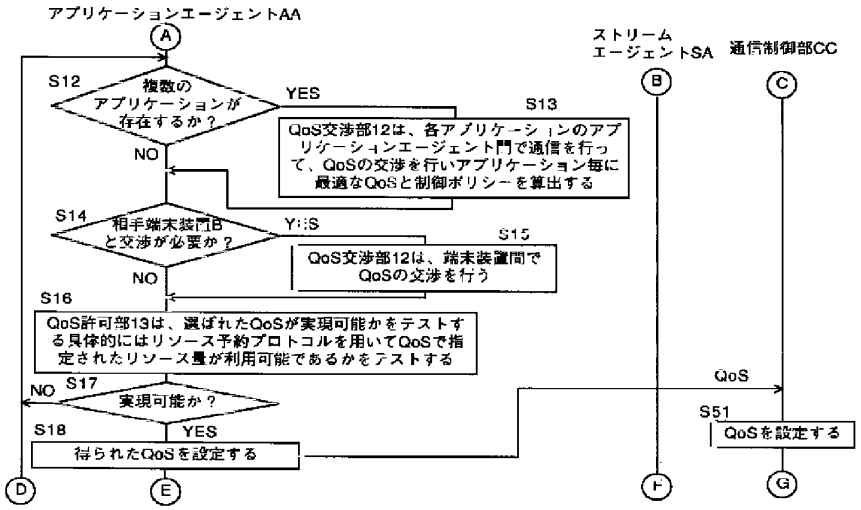
【図１】


実施形態
通信システム
通信アプリケーション
CA
AA
アプリケーション
エージェント
QoSマッピング部
11
QoS交渉部
12
QoS許可部
13
SA
CPU
10
ストリームエージェント
QoS管理部
QoSモニタリング部
21
22
CC
通信制御部
32
フローフィルタリング部
31
リアルタイムフロー制御部
適応転送システム部
33
モデム
A2
パーソナルコンピュータA1
B2
モデム
パーソナル
コンピュータ
B1
端末装置A
ネットワークNE
端末装置B

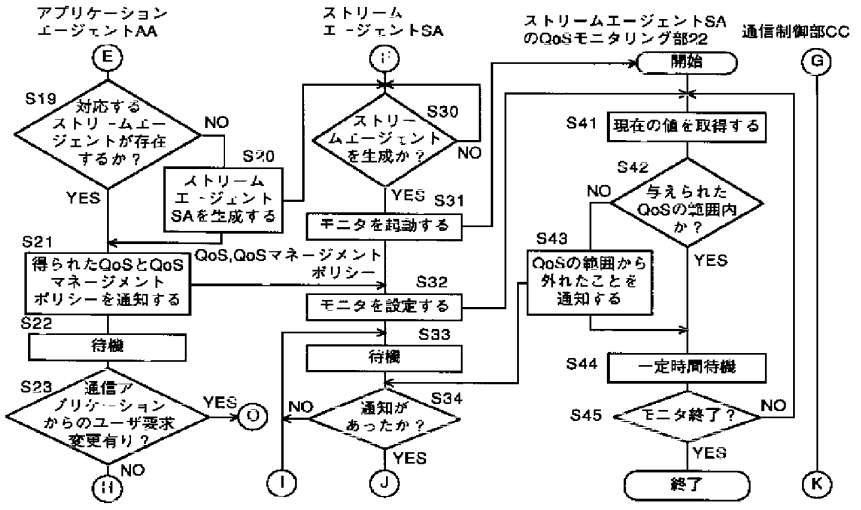
【図２】


通信アプリケーションCA
開始
S1
ストリーム
の作成要か？
NO
YES
S2
ストリームを作成する
S3
ユーザ
要求有り又は
変更有り？
NO
YES
S4
ユーザ要求する
アプリケーション
エージェントAA
開始
O
S10
ユーザ
要求有りか？
NO
YES
S11
QoSマッピング部11は、
ユーザ要求に基づいて通信
アプリケーションCAに対
して妥当なQoSとQoSマ
ネジメントポリシーをスト
リームごとに算出する
A
ストリーム
エージェントSA
開始
P
B
通信制御部CC
開始
N
C

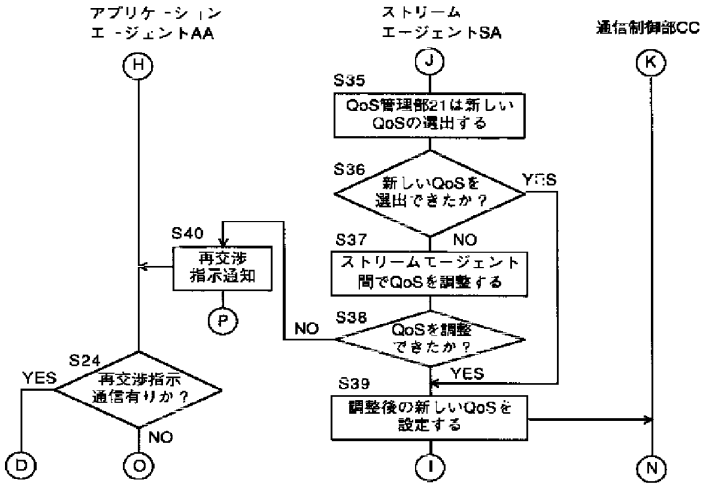
【図３】


アプリケーションエージェントAA
ストリーム
エージェントSA
通信制御部CC
A
B
C
S12
複数の
アプリケーションが
存在するか？
YES
NO
S13
QoS交渉部12は、各アプリケーションのアプリケーションエージェント間で通信を行って、QoSの交渉を行いアプリケーション毎に最適なQoSと制御ポリシーを算出する
S14
相手端末装置Bと交渉が必要か？
YES
NO
S15
QoS交渉部12は、端末装置間でQoSの交渉を行う
S16
QoS許可部13は、選ばれたQoSが実現可能かをテストする具体的にはリソース予約プロトコルを用いてQoSで指定されたリソース量が利用可能であるかをテストする
S17
実現可能か？
NO
YES
S18
得られたQoSを設定する
QoS
S51
QoSを設定する
D
E
F
G

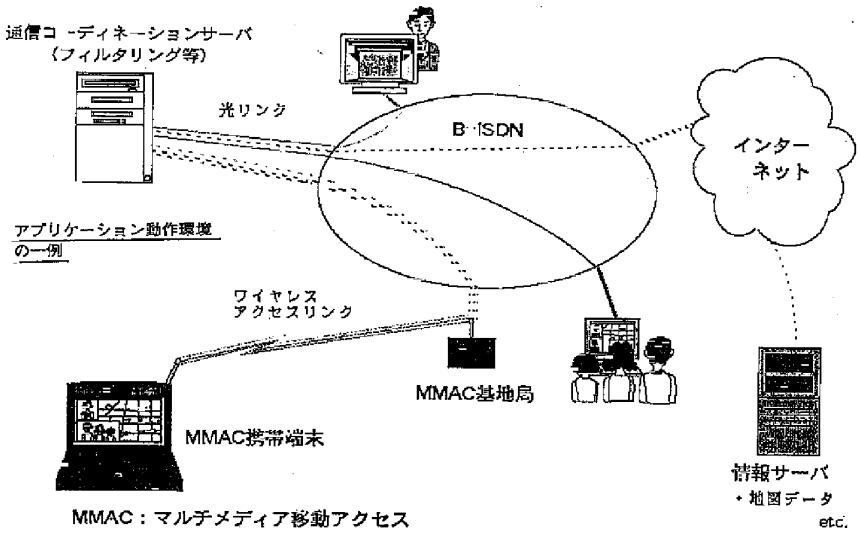
【図４】


アプリケーション
エージェントAA
ストリーム
エージェントSA
ストリームエージェントSA
のQoSモニタリング部22
通信制御部CC
E
I
開始
G
S19
対応する
ストリームエージェントが存在するか？
NO
YES
S20
ストリームエージェントSAを生成する
S30
ストリームエージェントを生成？
NO
YES
S31
モニタを起動する
S41
現在の値を取得する
S42
与えられたQoSの範囲内か？
NO
YES
S21
得られたQoSとQoSマネージメントポリシーを通知する
QoS,QoSマネージメントポリシー
S43
QoSの範囲から外れたことを通知する
S32
モニタを設定する
S22
待機
S33
待機
S44
一定時間待機
S23
通信アプリケーションからのユーザ要求変更有り？
YES
NO
O
H
I
J
通知があったか？
S34
NO
YES
S45
モニタ終了？
NO
YES
終了
K

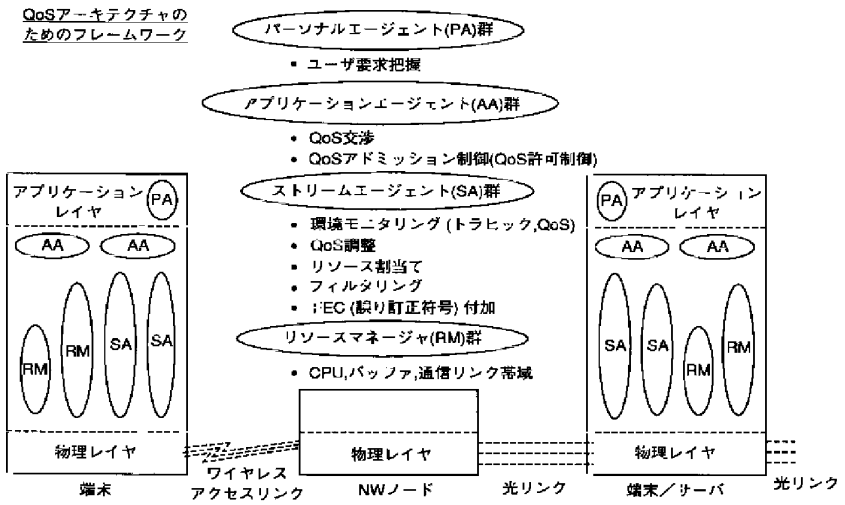
【図５】


アプリケーション
エージェントAA
ストリーム
エージェントSA
通信制御部CC
H
J
K
S35
QoS管理部21は新しい
QoSの選出する
S36
新しいQoSを
選出できたか？
YES
S40
再交渉
指示通知
S37
NO
ストリームエージェント
間でQoSを調整する
P
NO
S38
QoSを調整
できたか？
YES
S24
YES
再交渉指示
通信有りか？
S39
調整後の新しいQoSを
設定する
NO
D
O
I
N

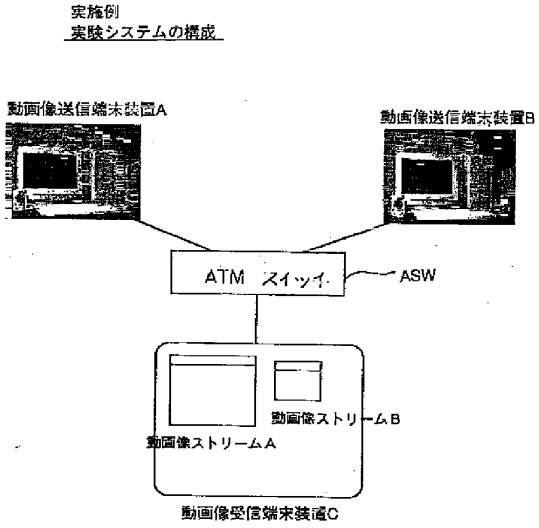
【図６】


通信コーディネーションサーバ
（フィルタリング等）
光リンク
B-ISDN
インター
ネット
アプリケーション動作環境
の一例
ワイヤレス
アクセスリンク
MMAC基地局
MMAC携帯端末
情報サーバ
＋地図データ
etc.
MMAC：マルチメディア移動アクセス

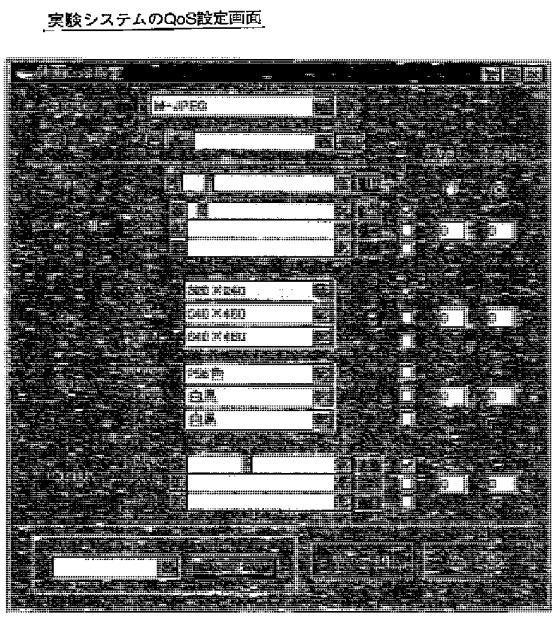
【図７】


QoSアーキテクチャのためのフレームワーク
パーソナルエージェント(PA)群
• ユーザ要求把握
アプリケーションエージェント(AA)群
• QoS交渉
• QoSアドミッション制御(QoS許可制御)
ストリームエージェント(SA)群
• 環境モニタリング (トラヒック,QoS)
• QoS調整
• リソース割当て
• フィルタリング
• FEC (誤り訂正符号) 付加
リソースマネージャ(RM)群
• CPU,バッファ,通信リンク帯域
アプリケーションレイヤ
PA
AA
RM
SA
物理レイヤ
端末
ワイヤレスアクセスリンク
NWノード
光リンク
端末／サーバ

【図８】

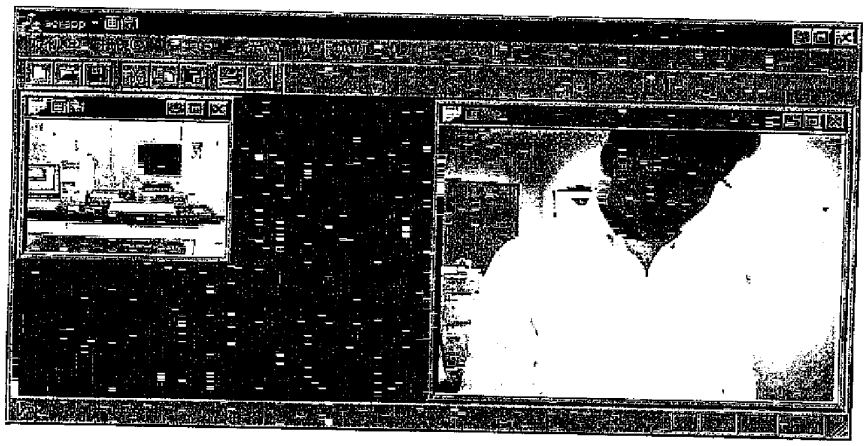

実施例
実験システムの構成
動画像送信端末装置A
動画像送信端末装置B
ATM スイッチ
ASW
動画像ストリームB
動画像ストリームA
動画像受信端末装置C

【図９】


実験システムのQoS設定画面

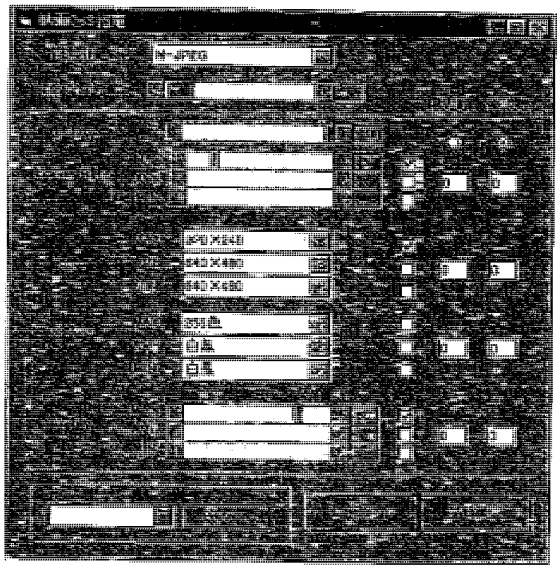
【図１０】

実験開始時の表示画面

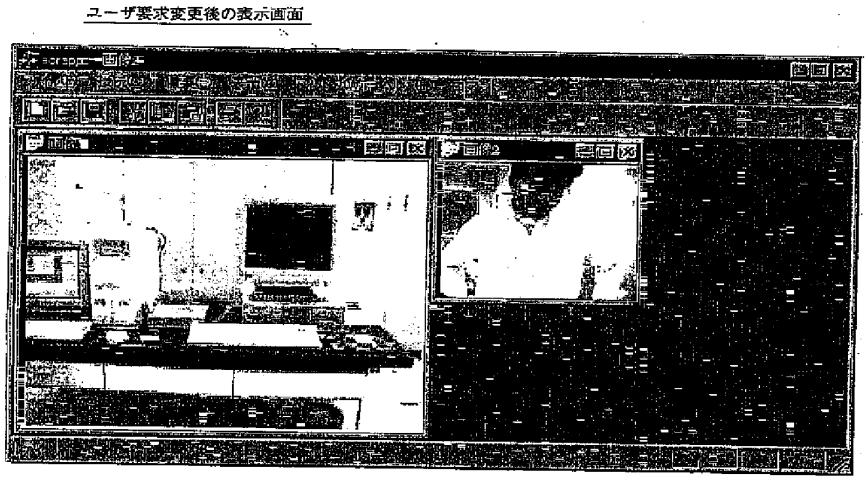


【図１１】

ユーザ要求変更の設定画面



【図１２】



【手続補正書】
【提出日】平成１１年４月２日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた端末装置の通信サービス品質制御方法において、
通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントと、ストリームエージェントとを生成し、
上記アプリケーションエージェントは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、
上記ストリームエージェントは、上記アプリケーションエージェントによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御し、
上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする通信サービス品質制御方法。
【請求項２】　上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数であることを特徴とする請求項１記載の通信サービス品質制御方法。
【請求項３】　上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする請求項１又は２記載の通信サービス品質制御方法。
【請求項４】　ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた通信サービス品質制御装置において、
通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリ

ケーションエージェントの第１の機能処理手段と、ストリームエージェントの第２の機能処理手段とを生成する生成手段とを備え、
上記第１の機能処理手段は、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、
上記第２の機能処理手段は、上記第１の機能処理手段によって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御し、
上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする通信サービス品質制御方法。
【請求項５】　上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数であることを特徴とする請求項４記載の通信サービス品質制御装置。
【請求項６】　上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする請求項４又は５記載の通信サービス品質制御装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００６
【補正方法】変更
【補正内容】
【０００６】
【課題を解決するための手段】本発明に係る請求項１記載の通信サービス品質制御方法は、ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた端末装置の通信サービス品質制御方法において、通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントと、ストリームエージェントとを生成し、上記アプリケーションエージェントは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、上記ストリームエージェントは、上記アプリケーションエージェントによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御し、上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】削除
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正内容】
【００１０】本発明に係る請求項４記載の通信サービス品質制御装置は、ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた通信サービス品質制御装置において、通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントの第１の機能処理手段と、ストリームエージェントの第２の機能処理手段とを生成する生成手段とを備え、上記第１の機能処理手段は、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信

ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、上記第２の機能処理手段は、上記第１の機能処理手段によって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御手段に通知して設定することにより自律的に通信ストリームを制御し、上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含むことを特徴とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正内容】
【００１１】また、請求項５記載の通信サービス品質制御装置によれば、請求項４記載の通信サービス品質制御装置において、上記評価関数は、各通信ストリームの通信サービスの品質毎の効用値を所定の重み付け係数で線形結合された関数であることを特徴とする。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正内容】
【００１２】さらに、請求項６記載の通信サービス品質制御装置は、請求項４又は５記載の通信サービス品質制御装置において、上記リソースは、上記端末装置のＣＰＵ使用量と、上記通信ストリームの伝送帯域を含むことを特徴とする。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】削除

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００５６
【補正方法】変更
【補正内容】
【００５６】
【発明の効果】以上詳述したように本発明に係る通信サービス品質制御方法及び装置によれば、ネットワークを介して接続された複数の端末装置間の通信サービスの品質を制御する通信制御手段を備えた端末装置の通信サービス品質制御方法及び装置において、通信ストリーム毎に、それぞれ予め決められた通信サービスの品質とその制御基準に基づいて自律的に通信ストリームを制御して通信のリソースの管理を行う、アプリケーションエージェントと、ストリームエージェントとを生成し、上記アプリケーションエージェントは、対応する通信ストリームに対して適当な通信サービスの品質と、その制御基準を設定し、自端末装置内及び相手方の端末装置との間で通信サービスの品質の交渉を行って通信サービスの品質を選択し、選択した通信サービスの品質によりテストを実行して実現可能であるときに当該通信サービスの品質を上記通信制御手段に通知して設定し、通信ストリーム集合に対する総合の効用値を表わす所定の評価関数の値が、所定のリソースの制約条件のもとで最大となるように通信サービスの品質を調整し、所定の通信サービスの品質の範囲を逸脱したときは、上記通信サービスの品質の調整を行って、調整後の通信サービスの品質を設定し、上記ストリームエージェントは、上記アプリケーションエージェントによって設定された通信サービスの品質とその制御基準に従って、当該通信ストリームの通信サービスの品質を制御して上記通信制御部手段に通知して設定することにより自律的に通信ストリームを制御し、上記制御基準は、（ａ）ＱｏＳの調整方法と、（ｂ）調整可能なＱｏＳの上限値、下限値及び平均値と、（ｃ）段階的にＱｏＳを調整する／しないの設定と、調整する場合の各ステップ幅と、（ｄ）通信ストリームの優先度と、ＱｏＳのパラメータ間の優先度と、（ｅ）複数のパラメータ集合とそれぞれの集合に対するユーザの満足度と、を含む。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００５７
【補正方法】変更
【補正内容】
【００５７】従って、本発明によれば、各エージェントが与えられた通信サービスの品質と制御ポリシーに従って自律的に通信サービスの品質を管理して制御することにより、動的な環境変化に対して迅速に対応できる。また、複雑な通信サービスの品質の制御を、簡単な装置構成で制御可能となる。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2009-218773
(43)Date of publication of application : 24.09.2009

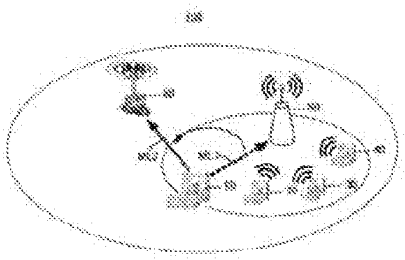
(51)Int.Cl. H04W 36/14 (2009.01)
H04B 1/40 (2006.01)
H04W 36/22 (2009.01)
H04W 36/36 (2009.01)
H04W 84/12 (2009.01)

(21)Application number : 2008-059128
(22)Date of filing : 10.03.2008

(71)Applicant : ADVANCED TELECOMMUNICATION RESEARCH INSTITUTE INTERNATIONAL
(72)Inventor : KIN SHOGYOKU
YAMAGUCHI AKIRA
OBANA SADAO

(54) RADIO APPARATUS, RADIO COMMUNICATION METHOD THEREIN, AND RADIO NETWORK WITH THE RADIO APPARATUS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a radio apparatus capable of switching a radio link while suppressing deterioration in communication characteristics and frequent switching of the radio link.
SOLUTION: The radio apparatus 10 measures a congestion degree Cind in performing a radio communication with an access point 50. When the measured congestion degree Cind becomes greater than a threshold Tf, the radio apparatus 10 switches a radio link with the access point 50 into a radio link with a base station 60 and transmits a packet to the base station 60. When the congestion degree Cind becomes smaller than a threshold Tr (<Tf), the radio apparatus 10 switches the radio link with the base station 60 into the radio link with the access point 50 and transmits a packet to the access point 50.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-218773
(P2009-218773A)
(43)公開日　平成21年9月24日(2009.9.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 36/14	(2009.01)	H04Q	7/00	309	5K011
H04B 1/40	(2006.01)	H04B	1/40		5K067
H04W 36/22	(2009.01)	H04Q	7/00	313	
H04W 36/36	(2009.01)	H04Q	7/00	331	
H04W 84/12	(2009.01)	H04Q	7/00	630	

審査請求 未請求　請求項の数 9　ＯＬ　（全 15 頁）

(21)出願番号　特願2008-59128(P2008-59128)
(22)出願日　平成20年3月10日(2008.3.10)

（出願人による申告）平成１９年度、支出負荷行為担当官、総務省大臣官房会計課企画官、研究テーマ「コグニティブ無線通信技術の研究開発」に関する委託研究、産業技術力強化法第１９条の適用を受ける特許出願

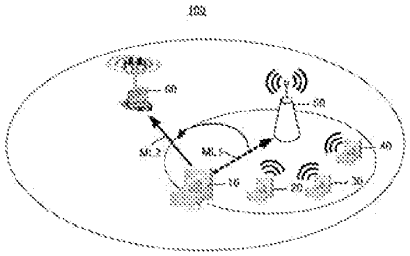
(71)出願人　393031586
株式会社国際電気通信基礎技術研究所
京都府相楽郡精華町光台二丁目２番地２
(74)代理人　100112715
弁理士　松山　隆夫
(72)発明者　金　鍾玉
京都府相楽郡精華町光台二丁目２番地２
株式会社国際電気通信基礎技術研究所内
(72)発明者　山口　明
京都府相楽郡精華町光台二丁目２番地２
株式会社国際電気通信基礎技術研究所内
(72)発明者　小花　貞夫
京都府相楽郡精華町光台二丁目２番地２
株式会社国際電気通信基礎技術研究所内

Ｆターム(参考)　5K011 CA01　JA02　KA13

最終頁に続く

(54)【発明の名称】無線装置、それにおける無線通信方法およびその無線装置を備えた無線ネットワーク

(57)【要約】
【課題】通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線装置を提供する。
【解決手段】無線装置１０は、アクセスポイント５０の間で無線通信を行なうときの混雑度C_{ind}を実測する。そして、無線装置１０は、その実測した混雑度C_{ind}がしきい値T_fよりも大きくなると、アクセスポイント５０との間の無線リンクを基地局６０との間の無線リンクに切換え、パケットを基地局６０へ送信する。また、無線装置１０は、混雑度C_{ind}がしきい値T_r（＜T_f）よりも小さくなると、基地局６０との間の無線リンクをアクセスポイント５０との間の無線リンクに切換え、パケットをアクセスポイント５０へ送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
無線通信空間のキャリアセンスを行ない、前記無線通信空間が空いているときに無線通信を行なう第１の無線通信システムを用いて第１の基地局との間で無線通信を行なう第１の無線モジュールと、
前記第１の無線通信システムと異なる第２の無線通信システムを用いて前記第１の基地局と異なる第２の基地局との間で無線通信を行なう第２の無線モジュールと、
前記第１の無線モジュールが前記第１の基地局との間で無線通信を行なうときの前記第１の基地局の通信範囲における通信状況を反映した混雑度を測定する測定手段と、
前記測定手段によって測定された混雑度が第１のしきい値よりも大きくなると、前記第１の無線モジュールへのパケットの分配を停止し、前記パケットを前記第２の無線モジュールに分配する分配手段とを備える無線装置。
【請求項２】
前記測定手段は、前記第１の無線モジュール用に設けられたキューから前記パケットを取り出した第１の時刻と、前記第１の基地局から確認応答を受信した第２の時刻との間の時間を前記混雑度として測定する、請求項１に記載の無線装置。
【請求項３】
前記分配手段は、前記測定手段によって測定された混雑度が前記第１のしきい値よりも小さい第２のしきい値よりも小さくなると、前記第２の無線モジュールへの前記パケットの分配を停止し、前記パケットを前記第１の無線モジュールに分配する、請求項１または請求項２に記載の無線装置。
【請求項４】
測定手段が、第１の無線モジュールが第１の無線通信システムを用いて第１の基地局との間で無線通信を行なうときの混雑度を測定する第１のステップと、
前記測定された混雑度が第１のしきい値よりも大きいか否かを判定する第２のステップと、
前記測定された混雑度が前記第１のしきい値よりも大きいと判定されたとき、前記第１の無線モジュールへのパケットの分配を停止し、前記第１の無線モジュールと異なる第２の無線モジュールへ前記パケットを分配する第３のステップと、
前記第２の無線モジュールが第１の無線通信システムと異なる第２の無線通信システムを用いて前記第１の基地局と異なる第２の基地局との間で無線通信を行なう第４のステップとを備える無線通信方法。
【請求項５】
前記第１のステップにおいて、前記測定手段は、前記第１の無線モジュール用に設けられたキューから前記パケットを取り出した第１の時刻と、前記第１の基地局から確認応答を受信した第２の時刻との間の時間を前記混雑度として測定する、請求項４に記載の無線通信方法。
【請求項６】
前記第４のステップが実行されているときに、前記測定された混雑度が前記第１のしきい値よりも小さい第２のしきい値よりも小さくなると、前記第２の無線モジュールへの前記パケットの分配を停止し、前記第１の無線モジュールへ前記パケットを分配する第５のステップと、
前記第１の無線モジュールが前記第１の無線通信システムを用いて前記第１の基地局との間で無線通信を行なう第６のステップとを更に備える、請求項４または請求項５に記載の無線通信方法。
【請求項７】
第１の基地局と、
前記第１の基地局と異なる第２の基地局と、
複数の無線装置とを備え、
前記複数の無線装置の各々は、

無線通信空間のキャリアセンスを行ない、前記無線通信空間が空いているときに無線通信を行なう第１の無線通信システムを用いて前記第１の基地局との間で無線通信を行なう第１の無線モジュールと、

前記第１の無線通信システムと異なる第２の無線通信システムを用いて前記第２の基地局との間で無線通信を行なう第２の無線モジュールと、

前記第１の無線モジュールが前記第１の基地局との間で無線通信を行なうときの混雑度を測定する測定手段と、

前記測定手段によって測定された混雑度が第１のしきい値よりも大きくなると、前記第１の無線モジュールへのパケットの分配を停止し、前記パケットを前記第２の無線モジュールに分配する分配手段とを含む、無線ネットワーク。

【請求項８】

前記測定手段は、前記第１の無線モジュール用に設けられたキューから前記パケットを取り出した第１の時刻と、前記第１の基地局から確認応答を受信した第２の時刻との間の時間を前記混雑度として測定する、請求項７に記載の無線ネットワーク。

【請求項９】

前記分配手段は、前記測定手段によって測定された混雑度が前記第１のしきい値よりも小さい第２のしきい値よりも小さくなると、前記第２の無線モジュールへの前記パケットの分配を停止し、前記パケットを前記第１の無線モジュールに分配する、請求項７または請求項８に記載の無線ネットワーク。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、無線装置、それにおける無線通信方法およびその無線装置を備えた無線ネットワークに関し、特に、無線通信の混雑度を用いて無線通信を制御する無線装置、それにおける無線通信方法およびその無線装置を備えた無線ネットワークに関するものである。

【背景技術】

【０００２】

従来、端末からアクセスポイントまでのＲＴＴ（Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）を測定し、その測定したＲＴＴをリンクの混雑度として用いて無線リンクを切換える無線通信方式が知られている。

【０００３】

また、受信信号強度ＲＳＳＩに基づいて無線リンクを切換える無線通信方式も知られている。そして、この無線通信方式においては、測定された受信信号強度ＲＳＳＩがしきい値よりも低いとき、他の無線リンクに切換えられる（非特許文献１）。

【非特許文献１】S. Hanaoka, M. Yano, and T. Hirata, “Testbed system of inter-radio system switching for cognitive radio”, IEICE Trans. on Communications, Vol. E91-B, no. 1, pp.14-21, Jan. 2008.

【発明の開示】

【発明が解決しようとする課題】

【０００４】

しかし、ＲＴＴは、数ｍｓから１ｓまで大きく揺らぐため、ＲＴＴを混雑度として用いて無線リンクを切換えると、無線リンクの切換が頻繁に発生し、ネットワークが安定しないという問題がある。

【０００５】

また、受信信号強度を用いて無線リンクを切換える無線通信方式では、測定した受信信号強度がしきい値よりも大きくても、ネットワークが混雑している場合、通信特性が低下するという問題が発生する。

【０００６】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、

通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線装置を提供することである。

【０００７】

また、この発明の別の目的は、通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線通信方法を提供することである。

【０００８】

さらに、この発明の別の目的は、通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線装置を備える無線ネットワークを提供することである。

【課題を解決するための手段】

【０００９】

この発明によれば、無線装置は、第１および第２の無線モジュールと、測定手段と、分配手段とを備える。第１の無線モジュールは、無線通信空間のキャリアセンスを行ない、無線通信空間が空いているときに無線通信を行なう第１の無線通信システムを用いて第１の基地局との間で無線通信を行なう。第２の無線モジュールは、第１の無線通信システムと異なる第２の無線通信システムを用いて第１の基地局と異なる第２の基地局との間で無線通信を行なう。測定手段は、第１の無線モジュールが第１の基地局との間で無線通信を行なうときの第１の基地局の通信範囲における通信状況を反映した混雑度を測定する。分配手段は、測定手段によって測定された混雑度が第１のしきい値よりも大きくなると、第１の無線モジュールへのパケットの分配を停止し、パケットを第２の無線モジュールに分配する。

【００１０】

好ましくは、測定手段は、第１の無線モジュール用に設けられたキューからパケットを取り出した第１の時刻と、第１の基地局から確認応答を受信した第２の時刻との間の時間を混雑度として測定する。

【００１１】

好ましくは、分配手段は、測定手段によって測定された混雑度が第１のしきい値よりも小さい第２のしきい値よりも小さくなると、第２の無線モジュールへのパケットの分配を停止し、パケットを第１の無線モジュールに分配する。

【００１２】

また、この発明によれば、無線通信方法は、測定手段が、第１の無線モジュールが第１の無線通信システムを用いて第１の基地局との間で無線通信を行なうときの混雑度を測定する第１のステップと、測定された混雑度が第１のしきい値よりも大きいか否かを判定する第２のステップと、測定された混雑度が第１のしきい値よりも大きいと判定されたとき、第１の無線モジュールへのパケットの分配を停止し、第１の無線モジュールと異なる第２の無線モジュールへパケットを分配する第３のステップと、第２の無線モジュールが第１の無線通信システムと異なる第２の無線通信システムを用いて第１の基地局と異なる第２の基地局との間で無線通信を行なう第４のステップとを備える。

【００１３】

好ましくは、第１のステップにおいて、測定手段は、第１の無線モジュール用に設けられたキューからパケットを取り出した第１の時刻と、第１の基地局から確認応答を受信した第２の時刻との間の時間を混雑度として測定する。

【００１４】

好ましくは、無線通信方法は、第４のステップが実行されているときに、測定された混雑度が第１のしきい値よりも小さい第２のしきい値よりも小さくなると、第２の無線モジュールへのパケットの分配を停止し、第１の無線モジュールへパケットを分配する第５のステップと、第１の無線モジュールが第１の無線通信システムを用いて第１の基地局との間で無線通信を行なう第６のステップとを更に備える。

【００１５】

更に、この発明によれば、無線ネットワークは、第１および第２の基地局と、複数の無線装置とを備える。第２の基地局は、第１の基地局と異なる。複数の無線装置の各々は、

第１および第２の無線モジュールと、測定手段と、分配手段とを含む。第１の無線モジュールは、無線通信空間のキャリアセンスを行ない、無線通信空間が空いているときに無線通信を行なう第１の無線通信システムを用いて第１の基地局との間で無線通信を行なう。第２の無線モジュールは、第１の無線通信システムと異なる第２の無線通信システムを用いて第２の基地局との間で無線通信を行なう。測定手段は、第１の無線モジュールが第１の基地局との間で無線通信を行なうときの混雑度を測定する。分配手段は、測定手段によって測定された混雑度が第１のしきい値よりも大きくなると、第１の無線モジュールへのパケットの分配を停止し、パケットを第２の無線モジュールに分配する。

【００１６】

好ましくは、測定手段は、第１の無線モジュール用に設けられたキューからパケットを取り出した第１の時刻と、第１の基地局から確認応答を受信した第２の時刻との間の時間を混雑度として測定する。

【００１７】

好ましくは、分配手段は、測定手段によって測定された混雑度が第１のしきい値よりも小さい第２のしきい値よりも小さくなると、第２の無線モジュールへのパケットの分配を停止し、パケットを第１の無線モジュールに分配する。

【発明の効果】

【００１８】

この発明においては、第１の基地局の通信範囲における無線通信の通信状況を反映した混雑度を実測し、その実測した混雑度が第１のしきい値を超えると、第１の基地局との無線リンクを第２の基地局との無線リンクに切換えて無線通信が行なわれる。その結果、スループットの低下が抑制される。そして、この実測された混雑度は、揺らぎが小さいものである。

【００１９】

従って、この発明によれば、通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換えることができる。

【発明を実施するための最良の形態】

【００２０】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２１】

図１は、この発明の実施の形態による無線ネットワークの概略図である。無線ネットワーク１００は、無線装置１０，２０，３０，４０と、アクセスポイント５０と、基地局６０とを備える。

【００２２】

無線装置１０，２０，３０，４０は、アクセスポイント５０の通信範囲と基地局６０の通信範囲との両方の重複範囲内に配置される。そして、無線装置１０，２０，３０，４０の各々は、アクセスポイント５０へアクセスすることも可能であり、基地局６０へアクセスすることも可能である。

【００２３】

無線装置１０，２０，３０，４０の各々は、後述する方法によって、アクセスポイント５０との間で無線通信を行なうときの混雑度C_{ind}を測定し、その測定した混雑度C_{ind}がしきい値T_fよりも大きいとき、無線リンクをアクセスポイント５０へアクセスする無線リンクＭＬ１から基地局６０へアクセスする無線リンクＭＬ２へ切換え、パケットを基地局６０へ送信する。

【００２４】

また、無線装置１０，２０，３０，４０の各々は、無線リンクを無線リンクＭＬ１から無線リンクＭＬ２へ切換えた後、アクセスポイント５０との間で無線通信を行なうときの混雑度C_{ind}を測定し、その測定した混雑度C_{ind}がしきい値T_r（＜T_f）よりも小さいとき、無線リンクを無線リンクＭＬ２から無線リンクＭＬ１へ切換え、パケットを

アクセスポイント５０へ送信する。

【００２５】

更に、無線装置１０，２０，３０，４０の各々は、混雑度C_{ind}が$T_r < C_{ind} < T_f$を満たすとき、現在の無線リンク（無線リンクＭＬ１または無線リンクＭＬ２）を維持する。

【００２６】

アクセスポイント５０は、例えば、ＷｉＦｉのアクセスポイントからなり、無線装置１０，２，３０，４０との間で無線通信を行なう。

【００２７】

基地局６０は、例えば、ＷｉＭＡＸの基地局からなり、無線装置１０，２，３０，４０との間で無線通信を行なう。

【００２８】

なお、アクセスポイント５０および基地局６０は、バックボーンネットワーク（図示せず）に接続されている。

【００２９】

図２は、図１に示す無線装置１０の構成を示す概略図である。無線装置１０は、キュー１と、分配手段２と、無線モジュール３，４とを含む。そして、無線モジュール３は、キュー５を含み、無線モジュール４は、キュー６および測定手段７を含む。

【００３０】

キュー１は、ＩＰ層からパケットＰＫＴを受け、その受けたパケットＰＫＴを一定時間保持した後、パケットＰＫＴを分配手段２へ出力する。

【００３１】

分配手段２は、キュー１からパケットＰＫＴを受け、測定手段７から混雑度C_{ind}を受ける。そして、分配手段２は、混雑度C_{ind}をしきい値T_fと比較し、混雑度C_{ind}がしきい値T_fよりも大きいとき、パケットＰＫＴのキュー６への分配を停止し、パケットＰＫＴをキュー５へ分配する。

【００３２】

また、分配手段２は、パケットＰＫＴをキュー５へ分配した後に、混雑度C_{ind}がしきい値T_rよりも小さくなると、パケットＰＫＴのキュー５への分配を停止し、パケットＰＫＴをキュー６へ分配する。

【００３３】

さらに、分配手段２は、混雑度C_{ind}が$T_r < C_{ind} < T_f$を満たすとき、キュー５（またはキュー６）へのパケットＰＫＴの分配を維持する。

【００３４】

無線モジュール３は、ＩＥＥＥ８０２．１６によって基地局６０へアクセスする無線モジュールである。即ち、無線モジュール３は、ＷｉＭＡＸによって無線通信を行なう無線モジュールである。そして、無線モジュール３は、キュー５に分配されたパケットＰＫＴを基地局６０へ送信するとともに、基地局６０からのパケットＰＫＴを受信してＩＰ層以上の上位層へ出力する。

【００３５】

無線モジュール４は、ＩＥＥＥ８０２．１１によってアクセスポイント５０へアクセスする無線モジュールである。即ち、無線モジュール４は、ＷｉＦｉによって無線通信を行なう無線モジュールである。そして、無線モジュール４は、キュー６に分配されたパケットＰＫＴをアクセスポイント５０へ送信するとともに、アクセスポイント５０からのパケットＰＫＴを受信してＩＰ層以上の上位層へ出力する

キュー５は、分配手段２から受けたパケットＰＫＴを保持するとともに、その保持したパケットＰＫＴを無線モジュール３へ出力する。

【００３６】

キュー６は、分配手段２から受けたパケットＰＫＴを保持するとともに、その保持したパケットＰＫＴを無線モジュール４へ出力する。

【００３７】
測定手段７は、後述する方法によって、無線モジュール４がアクセスポイント５０との間で無線通信を行なうときの混雑度C_{ind}を測定し、その測定した混雑度C_{ind}を分配手段２へ出力する。
【００３８】
なお、図１に示す無線装置２０，３０，４０の各々は、図２に示す無線装置１０と同じ構成からなる。
【００３９】
図３は、混雑度の測定方法を説明するための概念図である。無線装置１０の無線モジュール４は、タイミングｔ１でキュー６からパケットＰＫＴを取り出すと、ＤＩＦＳ（Ｄｉｓｔｒｉｂｕｔｅｄ ａｃｃｅｓｓ Ｉｎｔｅｒ Ｆｒａｍｅ Ｓｐａｃｅ）を設定し、ＤＩＦＳが経過すると、バックオフタイム（ＢＯ：Ｂａｃｋ Ｏｆｆ））を設定する。そして、無線装置１０の無線モジュール４は、バックオフタイムが経過するタイミングｔ２でパケットＰＫＴの送信を試みる。
【００４０】
しかし、無線装置２０の無線モジュール４がタイミングｔ２よりも前のタイミングｔ３でパケットＰＫＴの送信を開始しているので、無線装置１０の無線モジュール４は、無線装置２０の無線モジュール４がアクセスポイント５０から確認応答（ＡＣＫ）を受信し終わるタイミングｔ４まで待機する。
【００４１】
その後、無線装置１０の無線モジュール４は、再度、ＤＩＦＳを設定し、ＤＩＦＳが経過すると、バックオフタイムを設定し、バックオフタイムが経過するタイミングｔ５でパケットＰＫＴの送信を開始する。
【００４２】
そして、無線装置１０の無線モジュール４は、パケットＰＫＴの送信が完了し、更に、ＳＩＦＳ（Ｓｈｏｒｔ Ｉｎｔｅｒ Ｆｒａｍｅ Ｓｐａｃｅ）が経過すると、アクセスポイント５０から確認応答（ＡＣＫ）を受信し始め、タイミングｔ６で確認応答（ＡＣＫ）の受信を完了する。
【００４３】
これによって、無線装置１０の無線モジュール４は、パケットＰＫＴのアクセスポイント５０への送信が成功したことを検知する。
【００４４】
この発明においては、図３に示すタイミングｔ１からタイミングｔ６までの時間Ｔを無線モジュール４がアクセスポイント５０との間で無線通信を行なうときの混雑度C_{ind}と定義する。
【００４５】
この混雑度C_{ind}は、無線装置１０の無線モジュール４と、アクセスポイント５０との間の無線リンク$ML1_{10-50}$の混み具合を表す。そして、混雑度C_{ind}が大きければ、無線リンク$ML1_{10-50}$を用いた無線装置１０－アクセスポイント５０間のスループットが低下し、混雑度C_{ind}が小さければ、無線リンク$ML1_{10-50}$を用いた無線装置１０－アクセスポイント５０間のスループットが向上する。従って、この混雑度C_{ind}は、無線リンク$ML1_{10-50}$のリンクコストを表す。
【００４６】
また、混雑度C_{ind}は、無線モジュール４がアクセスポイント５０へのパケットＰＫＴの送信を開始した時刻から、確認応答（ＡＣＫ）をアクセスポイント５０から実際に受信するまでの時刻であるので、混雑度C_{ind}は、ＩＥＥＥ８０２．１１によるネットワークの通信状況を反映した値になる。つまり、混雑度C_{ind}は、アクセスポイント５０の通信範囲における無線通信の通信状況を反映した値になる。
【００４７】
例えば、無線装置１０，２０，３０，４０のうち、無線装置１０のみがアクセスポイン

ト５０へパケットＰＫＴを送信している場合、アクセスポイント５０は、無線装置１０からパケットＰＫＴを受信すると、直ちに、確認応答（ＡＣＫ）を無線装置１０へ送信する。

【００４８】

一方、無線装置１０，２０，３０，４０のうち、無線装置１０，２０がアクセスポイント５０へパケットＰＫＴを送信しており、無線装置２０の送信タイミングが無線装置１０の送信タイミングよりも早い場合、アクセスポイント５０は、無線装置１０からのパケットＰＫＴを受信し、かつ、確認応答（ＡＣＫ）を無線装置２０へ送信した後に、確認応答（ＡＣＫ）を無線装置１０へ送信する。即ち、アクセスポイント５０は、アクセスポイント５０における混み具合を反映したタイミングで確認応答（ＡＣＫ）を送信する。

【００４９】

従って、混雑度C_{ind}は、ＩＥＥＥ８０２．１１によるネットワークの混み具合を反映した値になる。

【００５０】

無線装置１０の測定手段７は、タイマー（図示せず）を内蔵しており、無線モジュール４がパケットＰＫＴをキュー６から取り出した時刻ｔ１から、無線モジュール４が確認応答（ＡＣＫ）をアクセスポイント５０から受信した時刻ｔ６までの時間Ｔをタイマーを用いて測定し、その測定した時間Ｔを混雑度C_{ind}として分配手段２へ出力する。

【００５１】

図４は、図１に示す無線ネットワーク１００における無線通信方法を説明するためのフローチャートである。なお、図４においては、無線装置１０が無線通信を行なう場合を例にして無線通信方法について説明する。

【００５２】

一連の動作が開始されると、無線装置１０の無線モジュール４は、キュー６からパケットＰＫＴを取り出し、他の無線装置２０，３０，４０がアクセスポイント５０へパケットＰＫＴを送信していないことを確認すると、その取り出したパケットＰＫＴをアクセスポイント５０へ送信する。そして、無線装置１０の無線モジュール４は、アクセスポイント５０から確認応答（ＡＣＫ）を受信する。

【００５３】

一方、無線装置１０の測定手段７は、無線モジュール４がパケットＰＫＴをキュー６から取り出した時刻から、確認応答（ＡＣＫ）をアクセスポイント５０から受信する時刻までの時間Ｔ-（＝混雑度$C_{ind}1$）を内蔵したタイマーによって測定する。即ち、無線装置１０の測定手段７は、無線モジュール４（＝第１の無線モジュール）がアクセスポイント５０（＝第１の基地局）との間で無線通信を行なうときの混雑度$C_{ind}1$を測定する（ステップＳ１）。

【００５４】

そして、無線装置１０の測定手段７は、その測定した混雑度$C_{ind}1$を分配手段２へ出力する。無線装置１０の分配手段２は、測定手段７から混雑度$C_{ind}1$を受け、その受けた混雑度$C_{ind}1$がしきい値T_fよりも大きいか否かを判定する（ステップＳ２）。

【００５５】

ステップＳ２において、混雑度$C_{ind}1$がしきい値T_f以下であると判定されたとき、無線装置１０の分配手段２は、無線モジュール４（＝第１の無線モジュール）へのパケットＰＫＴの分配を維持する（ステップＳ３）。その後、一連の動作は、ステップＳ１へ戻る。

【００５６】

一方、ステップＳ２において、混雑度$C_{ind}1$がしきい値T_fよりも大きいと判定されたとき、無線装置１０の分配手段２は、無線モジュール４（＝第１の無線モジュール）へのパケットＰＫＴの分配を停止し、無線モジュール３（＝第２の無線モジュール）へパケットＰＫＴを分配する（ステップＳ４）。

【００５７】
そして、無線装置１０の無線モジュール３は、キュー５からパケットＰＫＴを取り出し、その取り出したパケットＰＫＴを基地局６０（＝第２の基地局）へ送信する（ステップＳ５）。
【００５８】
その後、無線装置１０の測定手段７は、無線モジュール４（＝第１の無線モジュール）がアクセスポイント５０（＝第１の基地局）との間で無線通信を行なうときの混雑度$C_{ind}2$を上述した方法によって測定し（ステップＳ６）、その測定した混雑度$C_{ind}2$を分配手段２へ出力する。
【００５９】
そして、無線装置１０の分配手段２は、混雑度C_{ind}がしきい値T_rよりも小さいか否かを判定する（ステップＳ７）。ステップＳ７において、混雑度C_{ind}がしきい値T_r以上であると判定されたとき、無線装置１０の分配手段２は、無線モジュール３（＝第２の無線モジュール）へのパケットＰＫＴの分配を維持する（ステップＳ８）。その後、一連の動作は、ステップＳ６へ戻る。
【００６０】
一方、ステップＳ７において、混雑度C_{ind}がしきい値T_rよりも小さいと判定されたとき、無線装置１０の分配手段２は、無線モジュール３（＝第２の無線モジュール）へのパケットＰＫＴの分配を停止し、無線モジュール４（＝第１の無線モジュール）へパケットＰＫＴを分配する（ステップＳ９）。
【００６１】
そして、無線モジュール４（＝第１の無線モジュール）は、キュー６からパケットＰＫＴを取り出し、その取り出したパケットＰＫＴをアクセスポイント５０（＝第１の基地局）へ送信する（ステップＳ１０）。これによって、一連の動作が終了する。
【００６２】
なお、図１に示す無線装置２０，３０，４０の各々も、図４に示すフローチャートに従って無線通信を行なう。
【００６３】
上述したように、この発明においては、無線モジュール４がアクセスポイント５０との間で無線通信を行なうときの混雑度C_{ind}がしきい値T_fよりも大きくなると、無線装置１０は、無線モジュール４へのパケットＰＫＴの分配を停止し、パケットＰＫＴを無線モジュール３へ分配してパケットＰＫＴを基地局６０へ送信する（ステップＳ２の“ＹＥＳ”，Ｓ４，Ｓ５参照）。
【００６４】
従って、無線装置１０は、混雑している基地局（＝アクセスポイント５０）ではなく、空いている基地局６０へパケットＰＫＴを送信することができ、無線装置１０から基地局（＝アクセスポイント５０）への無線通信のスループットの低下を抑制して無線リンクを無線装置１０－アクセスポイント５０間の無線リンク$ML1_{10-50}$から無線装置１０－基地局６０間の無線リンク$ML1_{10-60}$に切換えることができる。
【００６５】
また、無線装置１０が無線リンクを無線リンク$ML1_{10-50}$から無線リンク$ML1_{10-60}$に切換えることによって、無線装置２０，３０，４０がアクセスポイント５０との間で無線通信を行なうときの混雑度C_{ind}が小さくなるので、無線装置２０，３０，４０がアクセスポイント５０へアクセスできる割合を大きくできる。
【００６６】
更に、一旦、無線リンク$ML1_{10-50}$から無線リンク$ML1_{10-60}$に切換えた後に、混雑度$C_{ind}2$がしきい値T_fよりも小さいしきい値T_rよりも小さくなったときに、無線リンク$ML1_{10-60}$から$ML1_{10-50}$に切換える（ステップＳ２の“ＹＥＳ”，Ｓ４～Ｓ６，Ｓ７の“ＹＥＳ”，Ｓ９，Ｓ１０参照）。従って、無線リンク$ML1_{10-50}$と無線リンク$ML1_{10-60}$との間の頻繁な切換を抑制して、無線リン

クを安定して切換えることができる。

【００６７】

図５は、混雑度の実測結果を示す図である。また、図６は、混雑度を用いたときのＷｉＦｉによる無線リンクへ分配されるパケットの割合を示す図である。図５において、縦軸は、混雑度（ｍｓ）を表し、横軸は、時間（ｓｅｃ）を表す。また、曲線ｋ１は、混雑度のタイミングチャートを示す。

【００６８】

図６において、縦軸は、ＷｉＦｉの重み、即ち、ＷｉＦｉによる無線リンクへ分配されるパケットの割合を表し、横軸は、時間（ｓｅｃ）を表す。また、曲線ｋ２は、混雑度を用いたときにＷｉＦｉによる無線リンクへ分配されるパケットの割合のタイミングチャートを示す。なお、図６に示す曲線ｋ２は、しきい値T_f＝５（ｍｓ）、しきい値T_r＝T_f／２＝２．５（ｍｓ）であるときに実測されたものである。

【００６９】

混雑度C_{ind}は、５０ｓｅｃ付近および７０ｓｅｃ付近で突発的に大きくなっているが、それ以外の領域では、比較的、安定している（図５参照）。

【００７０】

図５に示す混雑度C_{ind}を用いてＷｉＦｉによる無線リンクとＷｉＭＡＸによる無線リンクとの切換を行なった結果が図６に示す曲線ｋ２である。

【００７１】

図６において、ＷｉＦｉの重みが１．０であることは、パケットＰＫＴを無線モジュール４へ分配することを意味し、ＷｉＦｉの重みが０であることは、パケットＰＫＴを無線モジュール３へ分配することを意味する。

【００７２】

混雑度C_{ind}は、５０ｓｅｃまでは、しきい値T_fである５（ｍｓ）よりも小さいので、ＷｉＦｉの重みが“１．０”である。そして、混雑度C_{ind}が５０ｓｅｃ付近でしきい値T_fよりも大きくなると、ＷｉＦｉの重みが“０”となり、無線リンクが無線リンク$ML1_{10-50}$から無線リンク$ML1_{10-60}$に切換えられる。

【００７３】

その後、混雑度C_{ind}は、しきい値T_r＝T_f／２＝２．５（ｍｓ）よりも小さくなるので、ＷｉＦｉの重みが“１．０”になり、無線リンクが無線リンク$ML1_{10-60}$から無線リンク$ML1_{10-50}$に切換えられる。

【００７４】

更に、その後、混雑度C_{ind}は、７０ｓｅｃ付近で、再び、しきい値T_fを超えるので、ＷｉＦｉの重みが“０”になり、無線リンクが無線リンク$ML1_{10-50}$から無線リンク$ML1_{10-60}$に切換えられる。その後、混雑度C_{ind}は、約１３０ｓｅｃまでしきい値T_r＝T_f／２＝２．５（ｍｓ）よりも小さくならないので、ＷｉＦｉの重みは、“０”のままであり、混雑度C_{ind}が１３０ｓｅｃ以降になってしきい値T_r＝T_f／２＝２．５（ｍｓ）よりも小さくなると、ＷｉＦｉの重みは、“１．０”となり、無線リンクが無線リンク$ML1_{10-60}$から無線リンク$ML1_{10-50}$に切換えられる。

【００７５】

このように、実測された混雑度C_{ind}を用いることにより、無線リンク$ML1_{10-60}$と無線リンク$ML1_{10-50}$との頻繁な切換を抑制できることが実証された。混雑度C_{ind}は、アクセスポイント５０の通信範囲における無線通信の通信状況を反映したものであるので、図５に示すように、揺らぎが相対的に小さい。従って、混雑度C_{ind}を用いて無線リンクを切換えた場合、無線リンクの頻繁な切換を抑制できる。

【００７６】

図７は、ＲＴＴの実測結果を示す図である。また、図８は、ＲＴＴを用いたときのＷｉＦｉによる無線リンクへ分配されるパケットの割合を示す図である。

【００７７】

図７において、縦軸は、ＲＴＴ（ｍｓ）を表し、横軸は、時間（ｓｅｃ）を表す。また、曲線ｋ３は、ＲＴＴのタイミングチャートを示す。図８において、縦軸は、ＷｉＦｉの重み、即ち、ＷｉＦｉによる無線リンクへ分配されるパケットの割合を表し、横軸は、時間（ｓｅｃ）を表す。また、曲線ｋ４は、ＲＴＴを用いたときにＷｉＦｉによる無線リンクへ分配されるパケットの割合のタイミングチャートを示す。なお、図８に示す曲線ｋ４は、しきい値$Ｔ_{f}$＝３０（ｍｓ）、しきい値$Ｔ_{r}$＝$Ｔ_{f}$／２＝１５（ｍｓ）であるときに実測されたものである。

【００７８】

ＲＴＴは、５０ｓｅｃ付近から１１０ｓｅｃ付近までの期間、しきい値$Ｔ_{f}$（＝３０ｍｓ）よりも大きくなったり、しきい値$Ｔ_{r}$（＝１５ｍｓ）よりも小さくなったりし、大きく揺らいでいる（図７参照）。

【００７９】

その結果、ＷｉＦｉの重みは、５０ｓｅｃ付近から１１０ｓｅｃ付近までの期間、“１．０”と“０”との間で頻繁に切り換えられる（図８参照）。つまり、無線リンクは、５０ｓｅｃ付近から１１０ｓｅｃ付近までの期間、無線リンク$ＭＬ１_{10-60}$と無線リンク$ＭＬ１_{10-50}$との間で頻繁に切換えられる。

【００８０】

図９は、ＴＣＰスループットのタイミングチャートである。図９において、縦軸は、ＴＣＰスループット（Ｍｂｐｓ）を表し、横軸は、時間（ｓｅｃ）を表す。また、曲線ｋ５は、混雑度を用いた場合のＴＣＰスループットを示し、曲線ｋ６は、ＲＴＴを用いた場合のＴＣＰスループットを示す。

【００８１】

約５０ｓｅｃから７０ｓｅｃまでの期間、ＴＣＰスループットは、混雑度を用いた方がＲＴＴを用いるよりも大きくなる（曲線ｋ５，ｋ６参照）。これは、図６および図８に示すように、混雑度を用いる方が無線リンク$ＭＬ１_{10-60}$と無線リンク$ＭＬ１_{10-50}$との間での無線リンクの切換が抑制されるからである。

【００８２】

従って、上述した方法によって測定した混雑度を用いることによって、スループットの低下および無線リンクの頻繁な切換を抑制して無線リンクを切換えることができる。

【００８３】

なお、この発明においては、アクセスポイント５０は、「第１の基地局」を構成し、基地局６０は、「第２の基地局」を構成する。

【００８４】

また、無線モジュール４は、「第１の無線モジュール」を構成し、無線モジュール３は、「第２の無線モジュール」を構成する。

【００８５】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【産業上の利用可能性】

【００８６】

この発明は、通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線装置に適用される。また、この発明は、通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線通信方法に適用される。さらに、この発明は、通信特性の低下および無線リンクの頻繁な切換を抑制して無線リンクを切換可能な無線装置を備える無線ネットワークに適用される。

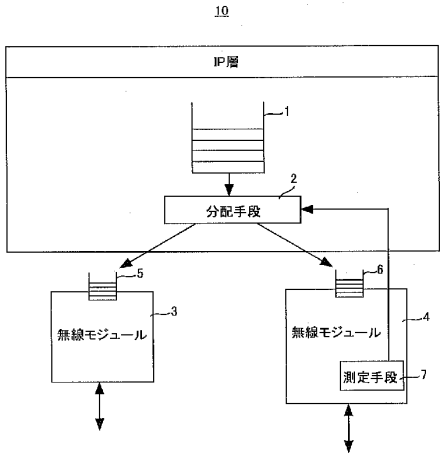
【図面の簡単な説明】

【００８７】

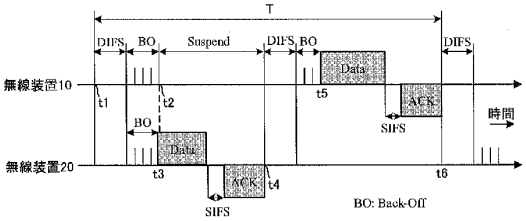
【図１】この発明の実施の形態による無線ネットワークの概略図である。

【図２】図１に示す無線装置の構成を示す概略図である。
【図３】混雑度の測定方法を説明するための概念図である。
【図４】図１に示す無線ネットワークにおける無線通信方法を説明するためのフローチャートである。
【図５】混雑度の実測結果を示す図である。
【図６】混雑度を用いたときのＷｉＦｉによる無線リンクへ分配されるパケットの割合を示す図である。
【図７】ＲＴＴの実測結果を示す図である。
【図８】ＲＴＴを用いたときのＷｉＦｉによる無線リンクへ分配されるパケットの割合を示す図である。
【図９】ＴＣＰスループットのタイミングチャートである。
【符号の説明】
【００８８】
１，５，６　キュー、２　分配手段、３，４　無線モジュール、７　測定手段、１０，２０，３０，４０　無線装置、５０　アクセスポイント、６０　基地局、１００　無線ネットワーク。

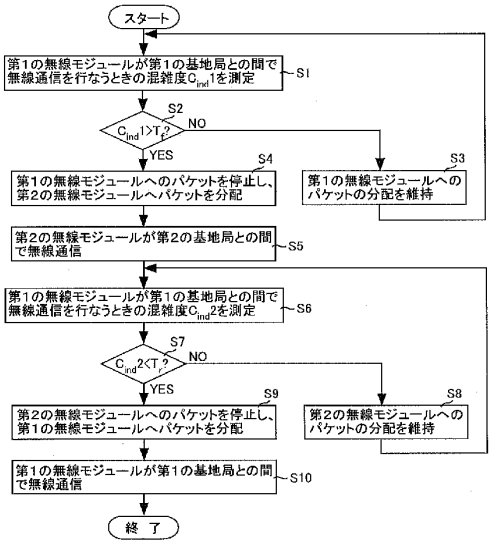
【図２】



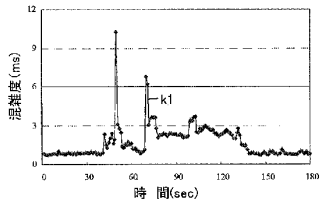
【図３】



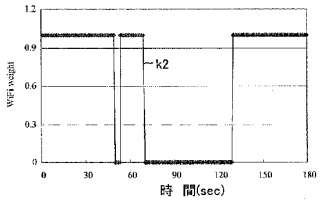
【図４】



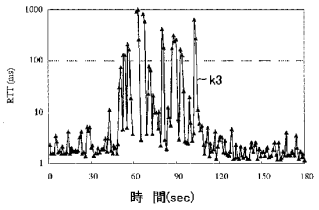
【図５】



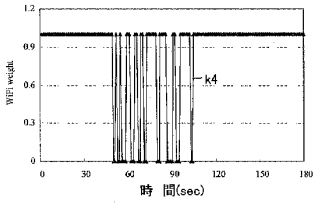
【図６】



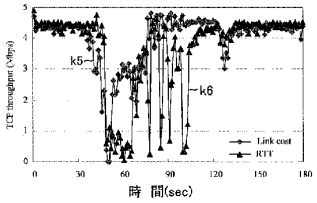
【図７】



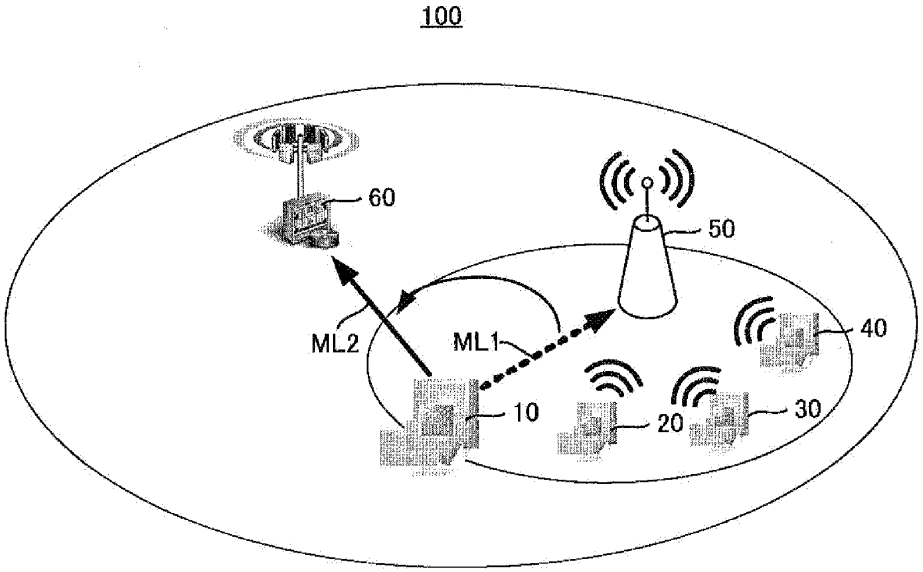
【図８】



【図９】



【図１】



フロントページの続き

Fターム(参考) 5K067 AA12 BB04 BB21 EE04 EE10 EE24 JJ39 JJ73

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 September 2006 (08.09.2006)

PCT

(10) International Publication Number
WO 2006/093961 A1

(51) International Patent Classification:
H04Q 7/38 (2006.01) *H04L 12/28* (2006.01)

(21) International Application Number:
PCT/US2006/007079

(22) International Filing Date:
27 February 2006 (27.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/070,583 1 March 2005 (01.03.2005) US

(71) Applicant *(for all designated States except US)*: **KYOCERA WIRELESS CORP.** [US/US]; 10300 Campus Point Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DUNN, Doug** [US/US]; c/o Kyocera Wireless Corp., 10300 Campus Point Drive, San Diego, California 92121 (US). **CHANG, Henry** [US/US]; c/o Kyocera Wireless Corp., 10300 Campus Point Drive, San Diego, California 92121 (US).

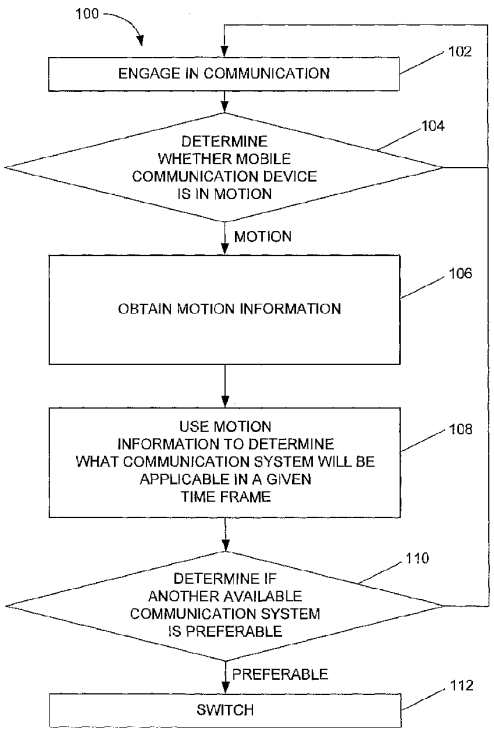
(74) Agents: **CONNELL, Kathleen, L.** et al.; Kyocera Wireless Corp., Attn: Intellectual Property Department, P.O. Box 928289, San Diego, California 92192-8289 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR MOTION SENSITIVE ROAMING IN A MOBILE COMMUNICATION DEVICE



(57) Abstract: A method for selecting a mobile communication service such as an air interface and/or communication system can include selecting the communication service based on motion and/or location. The selection of communication system can be made to optimize the user experience based on the type of service required and the environment the mobile station is in. Additionally, within an air interface, service can be chosen based on the type of call and the environment that mobile communication device is in.

WO 2006/093961 A1

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEMS AND METHODS FOR MOTION SENSITIVE ROAMING IN A MOBILE COMMUNICATION DEVICE

FIELD OF THE INVENTION

The field of the invention relates generally to mobile communication devices and more particularly to systems and methods for selecting service based on motion information related to a mobile communication device.

BACKGROUND OF THE INVENTION

Many mobile communication devices operate using only one type of wireless service, for example analog service. Mobile communication devices that operate using more than one type of wireless service are becoming more common. Different wireless services can use different air interfaces and/or different types of communication systems and protocols. Today, more and more air interfaces are emerging, including Global System for Mobile Communication (GSM), Code-Division Multiple Access (CDMA), CDMA2000, or Universal Terrestrial Radio Access (UTRA), to name just a few. Wireless data services are also generating new air interface standards including, High Rate Packet Data (HRPD), 802.11, 802.16, and 802.20, to name just a few. These wireless data systems could carry Voice Over Internet Protocol (VoIP.)

Often, these different systems will overlap. Ideally, a mobile communication device would be able to switch from system to system as required or to provide the best service for a particular function. The selection of a particular air interface, and/or communication system to use at a particular time will be a problem for a conventional mobile communication device that supports multiple air interfaces and/or communication systems, because there is no current mechanism to allow a mobile communication device to seamlessly determine the best system to use.

SUMMARY OF THE INVENTION

A method for selecting a mobile communication system using motion to assist in determining when it is appropriate to switch from one mobile communication system to

another. In one aspect, various motion-related information, such as direction and velocity, can be used to determine which communication system to use.

These and other features, aspects, and embodiments of the invention are described below in the section entitled "Detailed Description."

BRIEF DESCRIPTION OF THE DRAWINGS

Features, aspects, and embodiments of the inventions are described in conjunction with the attached drawings, in which:

Figure 1 is a flowchart illustrating an example method for using motion information to select a communication system in accordance with one embodiment;

Figure 2 is a diagram illustrating a mobile communication system configured to implement the method of figure 1; and

Figure 3 is a diagram illustrating an expanded preferred roaming list that can be used by the system of figure 2 to implement the method of figure 1.

DETAILED DESCRIPTION

It is becoming practical to produce mobile communication devices, such as mobile telephone handsets, capable of operating in multiple air interfaces and/or communication systems. Generally, each of the communication systems has certain advantages and disadvantages depending on the situation. For example, an air interface that is optimized for voice may not be the best choice for a user that wants data services. Blindly searching for a system to acquire and use because the mobile communication device supports that air interface can significantly delay switching to the most appropriate system for the environment in which the mobile is located. This delay can increase significantly depending on how many air interfaces are supported and what roaming agreements the providers have for each air interface. Accordingly, selection of a communication system can be made to optimize the user experience based on the type of service required and the environment in which the mobile station resides.

In one embodiment, for example, a communication system for a mobile communication device can be selected from a predetermined list of available air

interfaces and/or communication systems. Thus, the mobile communication device can select which system or systems to search for from the list based on the type of service employed by a user at a particular time; e.g., voice or high speed data services. Other factors can also contribute to the selection of a given system. For example, factors that can be used to select a system can include adequate radio link quality for the service in use, quality of service, cost of service, including taking into consideration any billing plans a subscriber might have, or the number of minutes a subscriber has on a particular service, whether the mobile communication device is plugged in or using battery power, how much battery power is left, or some combination thereof. How these criteria are applied and services selected can, depending on the embodiment, be modified by the user or service provider.

While these criteria are used to determine which system or systems the mobile communication device will attempt to acquire, and in some embodiments the order of those attempts, it may not be possible to acquire the system identified as optimum for a particular service for reasons beyond the control of the user and the mobile communication device, e.g., system is at capacity, or the system is temporarily shut down. In those cases where the optimum system cannot be acquired, acquisition of the next best system for that particular service should be attempted.

Before describing the figures, it should be noted that the examples presented are discussed generally in the context of a mobile device, specifically, a mobile telephone handset. It will be understood that the systems and methods described herein can be applied to any mobile communication device, including, but not limited to personal digital assistants (PDAs), pagers, etc.

Accordingly, Figure 1 is a flowchart illustrating an embodiment of a method for selecting a communication system in accordance with the systems and methods described herein. In step 102, a mobile communication device can engage in a communication. The communication device can be configured to use many different air interface standards, including, but not limited to Global System for Mobile Communication (GSM), Code-Division Multiple Access (CDMA), CDMA2000, or Universal Terrestrial Radio Access (UTRA) as well as data services such as High Rate Packet Data (HRPD),

802.11, 802.16, and 802.20. It will be understood that these data systems could carry Voice Over Internet Protocol (VoIP.) Moreover, mobile communication devices configured to implement the method of Figure 1 can use some or all of the above communication systems as well as other communication systems.

In step 104, the mobile communication device can determine whether the mobile communication device is in motion. In certain embodiments, determining whether the device is in motion can comprise using Global Positioning System (GPS) Satellites to determine position and/or location information for the mobile communication device. This information can then be used to determine whether the device is in fact in motion. In another embodiment the determination step 104 can be made using Differential GPS (DGPS.) A DGPS is a system designed to improve the accuracy of GPS position determination by measuring small changes in variables to provide satellite positioning corrections. The DGPS can, in another embodiment comprise a Wide Area Augmentation System (WAAS) GPS Receiver. WAAS is basically a DGPS implemented by the Federal Aviation Administration. Integration of GPS types of functionality into a mobile device is well known, and therefore will not be explained in detail here. Moreover, it will be understood that GPS based position and/or location services can, for example, be standalone, network assisted, or network based. It will also be understood that the systems and methods described herein can use any system or method that can provide information that can be used to determine motion of the mobile communication device.

Once it is determined that the mobile communication device is in fact in motion, then information related to that motion can be obtained by the mobile communication device in step 106. For example, the motion information can include position information and relative velocity. In other words, in order to determine, in step 104, that the device is in motion, several position measurements can be made within a certain time frame. If the position has changed, then the device is in motion. The time frame clearly needs to be selected so that it is sufficiently short to ensure that the device is in fact in motion if there is a change in position for the given time frame. The magnitude of the change in position combined with the time associated with the time frame can then be used to determine velocity. The direction of motion can also be determined, or at least estimated, based on

the change in position. All such information, and the like, can be considered motion information. Further, it will be understood that the motion information can be determined by the mobile communication device, by a system external to the mobile communication device, e.g., the network, or some combination thereof.

The motion information obtained in step 106 can then be used to determine what other communication systems will be available within a given time frame in step 108 based on information stored in the mobile, alternatively it could be provided by the network at that time. For example, based on the direction and relative velocity determined in step 106, it can be determined that a wireless hotspot, e.g., an 802.11 system, will be available in 5 minutes or that several wireless Wide Area Network (WAN) systems are currently available. In one embodiment, system locations and type can be provided via an expanded preferred roaming list stored in the mobile communication device. One example of an expanded preferred roaming list is described in more detail below. In another embodiment, the mobile communication device may be able to probe the pilot signal level for various systems and use the knowledge of the signal strength of the systems obtained to determine the preferred system using, e.g. signal level constraints.

In step 110, the mobile device can then determine which of the available or soon to be available systems would be preferable. For example, if a subscriber initiates a high data rate file transfer, the user's mobile communication device can determine which of the available, or soon to be available, systems is the best system to support the communication. The mobile device can then be configured to switch to the preferred system, if it can be acquired, in step 112 in order to make the high data rate transfer. Similarly, if a system with a higher available bandwidth is going to be available soon, as determined with the aid of the motion information, then the mobile communication device can be configured such that it waits until the higher bandwidth system is available.

Factors that can be used to determine which system is the best system for a particular communication can include the required data rate, but can also include how long that system will be available based on the direction and speed of travel. The term "system is available" can be used to describe a condition whereby the mobile

communication device can obtain a strong enough signal from the system such that the level of service is adequate for the type of service the system is intended for. In other words, the mobile communication device is within the coverage area of the system when the "system is available".

Other factors that can be used to determine the best system can include cost, e.g., one communication system can be preferable when a user of a mobile communication device has a contract with the provider, or the provider has a partnership with a provider that a user of the mobile communication device has a contract with. Cost consideration can also include, for example, whether a user has minutes left on one available service, but not on another available service.

The determination that a system is preferable can also be made based on geographic location indicators, such as distance from a base station, or a predetermined coverage area. Determination based on geographic location will be discussed further with respect to figure 2.

Motion based performance capabilities of a particular communication system can also be used to determine which system is preferable. For example, certain systems or certain air interfaces can be considered better suited to serving a mobile communication device when it is in motion, while other systems or air interfaces can be better when a mobile communication device is stationary. How fast the device is traveling can also effect the determination of which system is preferable.

The application a user would like to use can also be used to determine what system is preferable. In some cases a systems can be better for a desired applications. For example, if a user would like to use a voice service, it can be preferable to select a voice communication system that is available as opposed to a data communication system. As mentioned, the bandwidth of a system or supported data rate can also be important factors.

Also mentioned above, an expanded preferred roaming list can be used to determine what systems will or will not be available. In other embodiments, however, such a determination can be made without the use of an expanded preferred roaming list. For example, motion based performance capabilities can be known generally for different

types of communication systems. The determination can then be made based on a list of types of systems and the performance capabilities associated with the systems on the list. Thus, as certain systems are encountered or anticipated the list can be consulted to determine which is preferable. The list of motion based performance capabilities for different types of systems can also be included in, or with, an expanded preferred roaming list.

In certain embodiments, the mobile communication device can also include data regarding course and destination of the device. For example, some GPS based navigation systems include turn by turn directions from a starting location to an ending location. In one embodiment, a mobile communication device can use such data to determine what communication systems will be available and for how long. This information can then be used to determine what systems are preferable, e.g., based on cost, service requested, etc.

In another embodiment, knowledge of terrain can also be used to determine a preferable communication system. For example, a system that transmits line of sight may not be preferable in situations when, for example, a mountain is between the mobile communication device and a transmitter of the line of sight system.

In step 112, the mobile communication device can switch to the preferred communication system. In one embodiment, the switch of step 112 can be a soft handoff between the original communication system and the preferred system. In another embodiment, switch 112 can comprise a hard handoff. For example, if the communication device begins transmitting a large file, but then detects that a data service with higher bandwidth will be available shortly, then the device can be configured to stop the transmission, perform a hard handoff to the higher bandwidth system, and then reinitiate the transfer.

It should be noted that a trade off may need to be made, e.g., with respect to download speed and cost. For example, 802.11 can, in some cases be faster, but may not be the cheapest service available. The service selected can, thus, depend on the relative importance of price, download speed, file size, or length of the stream.

The switch of step 112 can, in some embodiments be over-ridden by the user. For example, generally, 802.11 may in some cases not be considered to be advantageous when a user is in motion, however, a user riding on a train that provides 802.11 service within the train may wish to override a determination that another service is preferable. Thus, the switch of step 112 can be automatic. Alternatively, the switch of step 112 can be displayed to a user, allowing the user to override the determination. Additionally, the selection of automatic switching or user override can, depending on the embodiment, be selected by the user. In another embodiment, the mobile communication device can detect and display the available systems for the user to select from. These systems can be displayed in a manner indicating their ranking based on the defined criteria.

Figure 2 is a diagram illustrating a mobile communication system 200 in accordance with the systems and methods described herein. Mobile communication device 202 typically includes a processor coupled to a memory and a transceiver (not shown). Mobile communication device 202 can be configured execute instructions stored in memory to perform the steps illustrated by figure 1. For example, mobile communication device 202 can engage in a communication with a first communication system 204 as described with respect to step 102 of figure 1. First communication system 204 can, e.g., comprise a GSM, CDMA, CDMA2000, or UTRA system. First communication system 204 can also comprise, e.g., a wireless data only system such as HRPD, 802.11, 802.16, or 802.20.

Mobile communication device 202 can be in motion, as indicated by arrow 210. When it is determined that mobile communication device 202 is in motion (step 104) the mobile communication device 202 can be configured to then determine if another communication system will become available that is preferable (step 106).

For example, in one embodiment, it can be preferable for the mobile communication device 202 to engage in communication with second communication system 206 if the mobile communication device 202 has crossed over the line 208. Line 208, can, e.g., be a boundary of an area serviced by second communication system 206. Information regarding communication system boundaries can be stored in an expanded preferred roaming list. Alternatively, line 208 can simply indicate that device 202 is now

closer to system 206. Expanded preferred roaming lists will be discussed further with respect to figure 3.

In the embodiment of figure 2, however, device 202 is configured to determine whether device 202 is in motion (step 104) and to then obtain motion information (step 106), such as velocity and direction. Using this information, device 202 can be configured to determine that at a certain time system 206 will be preferable due to its closer proximity. Stated another way, device 202 can be configured to determine that at a certain time device 202 will cross boundary 208 making system 206 preferable for at least certain types of communications.

The determination that mobile communication device 202 is in motion can be made using location determination system 212. The location determination system 212 can be a global positioning system. It will be understood that global positioning systems generally include multiple satellites and can additionally include ground based components. Alternatively, the location determination system 212 can also be a ground based system.

Figure 2 includes an example wherein a determination that another communication system is preferable can be made based on a boundary of an area serviced by second communication system 206. The determination that another communication system is preferable (step 106) can be based on other factors and combinations of factors as discussed with respect to figure 1.

Figure 3 is a diagram illustrating a simplified example of an expanded preferred roaming list 300 in accordance with an embodiment of the systems and methods described herein. Each entry 314, 316, and 318 in expanded preferred roaming list 300 can include system ID 302 and network ID 304.

Each entry 314, 316, and 318 can also include information related to geographic location indicators 306. The geographic location indicators can indicate a location within an area serviced by the communication system. In another embodiment, geographic indicators 306 can include information about the boundaries of an area serviced by a communication system.

Each entry 314, 316, and 318 can also include motion based performance capabilities 308. Different communication systems can, for example, have higher or lower performance based on velocity of a mobile communication device. Thus, in one embodiment, a mobile communication device can select a service based on velocity of the mobile communication device and an expected level of performance at that velocity.

Expanded preferred roaming list 300 can also include types of services available 310. In an embodiment the selection of a communication service can be made based on, for example, a predetermined list of services available for the location and/or velocity of the mobile communication device.

Expanded preferred roaming list 300 can also include applications that a particular communication system and/or air interface is suited for 312. The selection of a particular communication system can be made based on selecting a suitable system and/or air interface from a list that is available at a given location. When the mobile chooses a system based on geographic location, type of service, motion, etc. the mobile may still not have service available due to changes in service, network maintenance, or accuracy of the geographic location of the system, etc. Thus, in certain embodiments, the mobile will try to acquire the system based on the preferred roaming list 300 and will successively go down the preferred roaming list 300 until it finds a system suitable for its application with strong enough signal from the system.

When determining that a communication system is preferable based on the applications that the system is best suited for, the determination can take multiple factors into account. For example, assume that one system, System A is good for voice communications and not as good for data communications. Further, assume that System B is good for data communications but not as good for voice communications; however, System B performs well when a device using System B is in motion. If a device is in motion, it can, thus be preferable to choose System B, even for voice communications.

In one embodiment a point system can be used to rate the available services. For example, various characteristics of the system, such as voice communication capability, data communication capability, performance of the system while in motion, etc., can be rated, e.g., from 1 to 5 points, 5 points being better than 1 point. As an example, system

A can, e.g., be rated 5 for voice communication, 3 for data communication, and 1 for motion. System B can be rated 5 for data communication, 3 for voice communication, and 5 for motion. To choose a system, points can be added up and the system with the most points can be selected. In the present example, for voice communication while in motion, System A has 6 points, 5 points for voice communication and 1 point for motion. System B has 8 points, 3 points for voice communication and 5 points for motion. System B, in this example would thus be the preferable system.

Other factors that can be considered in determining a preferable system include, but are not limited to, cost of service, minutes remaining on the present service, and roaming partner agreements. For example, it may be desirable to select a lower cost service as apposed to a higher cost service. Another consideration that relates to cost is minutes remaining. In many cases customers buy service plans based on some number of minutes per month. The costs of using more than this allotment of minutes can be high relative to the cost for one month of service. It can be preferable to select a service that has minutes remaining as opposed to a service that does not have minutes remaining or a service that charges per minute. Another way that costs to the consumer can be managed is through roaming partner agreements. Roaming can occur when a mobile communication device uses another network. In some cases service providers may have agreements that can make it preferable, when roaming, to select a service with a roaming partner agreement.

It should be noted that other methodologies besides a point system can be used to rank systems in order to determine which service should be selected. For example, any methodology that uses some or all of the above characteristics and parameters to rank potential services can be implemented as part of the methods and systems described herein.

Generally a roaming list includes multiple entries 314, 316, 318. The number of entries may vary for different mobile devices. Further, each entry can be configured to include information that can allow a mobile communication device to make motion based decisions as described above.

While certain embodiments of the inventions have been described above, it will be understood that the embodiments described are by way of example only. Accordingly, the inventions should not be limited based on the described embodiments. Rather, the scope of the inventions described herein should only be limited in light of the claims that follow when taken in conjunction with the above description and accompanying drawings.

What is claimed is:

CLAIMS

1. A mobile communication device comprising:

a processor,

a memory coupled to the processor;

a transceiver coupled to the processor, the processor further configured to:

engage (102) in a communication using a first communication system;

determine (104) whether the mobile communication device is in motion;

when the device is in motion, determine (106) motion information for the device;

determine (110) if another communication system is preferable based on the motion information; and

when it is determined that another communication system is preferable, switch (112) to the other communication system.

2. The mobile communication device of claim 1, wherein the determination of motion step comprises using global positioning system signals to determine that the mobile communication device is in motion.

3. The mobile communication device of claim 2, wherein using global positioning system signals comprises processing the signals with assistance from a communication network.

4. The mobile communication device of claim 1, wherein the determination of motion step comprises using a plurality of position fixes to determine that the mobile communication device is in motion.

5. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises using an expanded preferred roaming list including geographical information.

6. The mobile communication device of claim 1, wherein the determination of motion comprises a determination of position, bearing, and velocity.

7. The mobile communication device of claim 1, wherein the processor is further configured to:

predict a future location; and

schedule the switching to another communication system step based on the predicted future location.

8. The mobile communication device of claim 1, wherein the switching step comprises a handoff.

9. The mobile communication device of claim 8, wherein the handoff is delayed based on a prediction of a future location of the mobile communication device.

10. The mobile communication device of claim 1, wherein the determine if another communication system is preferable step comprises determining if another communication system is preferable for one of a voice communication, a data communication, and for a voice over internet protocol communication.

11. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises determining if another communication system is preferable for Quality of Service (QoS).

12. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on available data rates on each of the first and second communication systems.

13. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on availability of the first and second communication systems.

14. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on access rights on each of the first and second communication systems.

15. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on cost of service.

16. The mobile communication device of claim 1, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on a roaming partner agreement.

17. A method for managing system access of a mobile communication device comprising, the method comprising:

engaging (102) in a communication using a first communication system;

determining (104) whether the mobile communication device is in motion;

when the device is in motion, determining (106) motion information for the device;

determining (110) if another communication system is preferable based on the motion information; and

when it is determined that another communication system is preferable, switching (112) to the other communication system.

18. The method of claim 17, wherein the determination of motion step comprises using a plurality of position fixes to determine that the mobile communication device is in motion.

19. The method of claim 17, wherein the determination that another communication system is preferable step comprises using an expanded preferred roaming list including geographical information.

20. The method of claim 17, wherein the determination of motion comprises a determination of position, bearing, and velocity.

21. The method of claim 17, further comprising:
predicting a future location; and
scheduling the switching to another communication system step based on the predicted future location.

22. The method of claim 17, wherein the determine if another communication system is preferable step comprises determining if another communication system is preferable for one of a voice communication, a data communication, and for a voice over internet protocol communication.

23. The method of claim 17, wherein the determination that another communication system is preferable step comprises determining if another communication system is preferable for Quality of Service (QoS).

24. The method of claim 17, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on available data rates on each of the first and second communication systems.

25. The method of claim 17, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on availability of the first and second communication systems.

26. The method of claim 17, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on access rights on each of the first and second communication systems.

27. The method of claim 17, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on cost of service.

28. The method of claim 17, wherein the determination that another communication system is preferable step comprises determining the preferable communication system based on a roaming partner agreement.

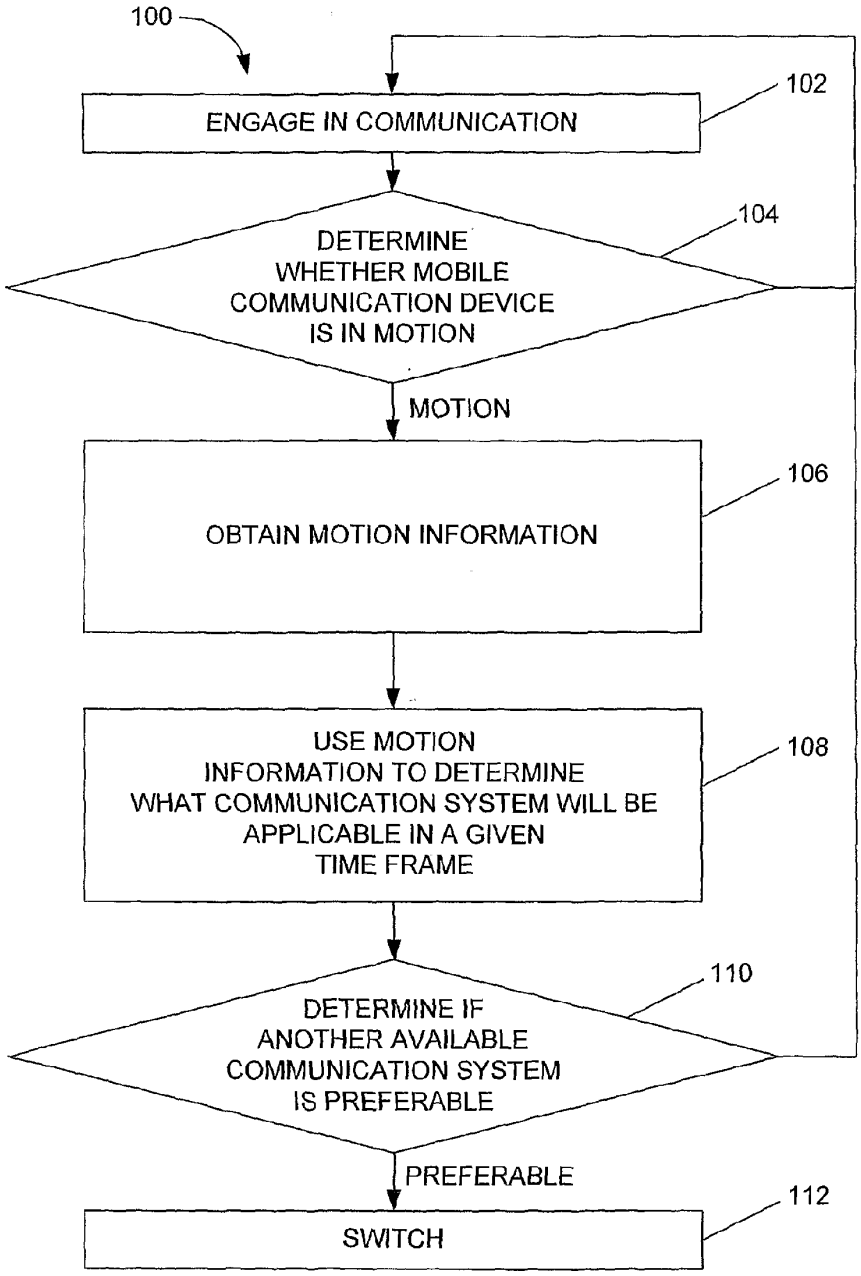

100
ENGAGE IN COMMUNICATION
102
DETERMINE WHETHER MOBILE COMMUNICATION DEVICE IS IN MOTION
104
MOTION
OBTAIN MOTION INFORMATION
106
USE MOTION INFORMATION TO DETERMINE WHAT COMMUNICATION SYSTEM WILL BE APPLICABLE IN A GIVEN TIME FRAME
108
DETERMINE IF ANOTHER AVAILABLE COMMUNICATION SYSTEM IS PREFERABLE
110
PREFERABLE
SWITCH
112

FIG. 1

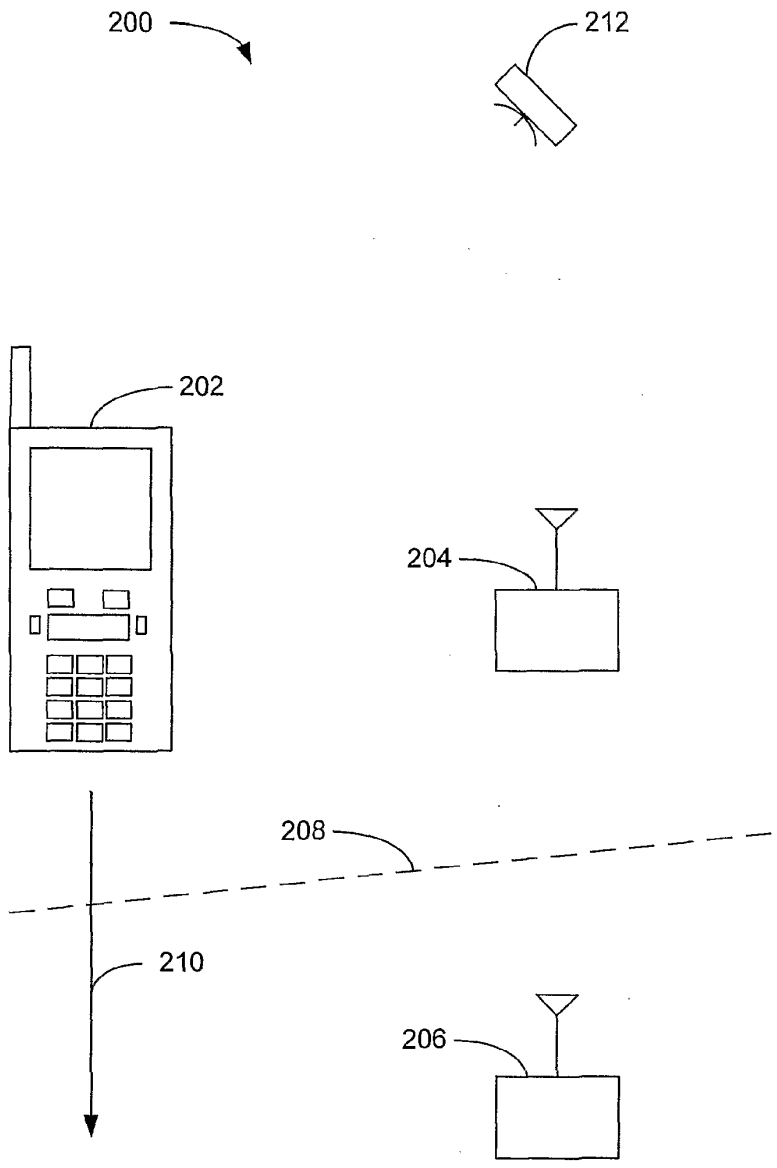


FIG. 2

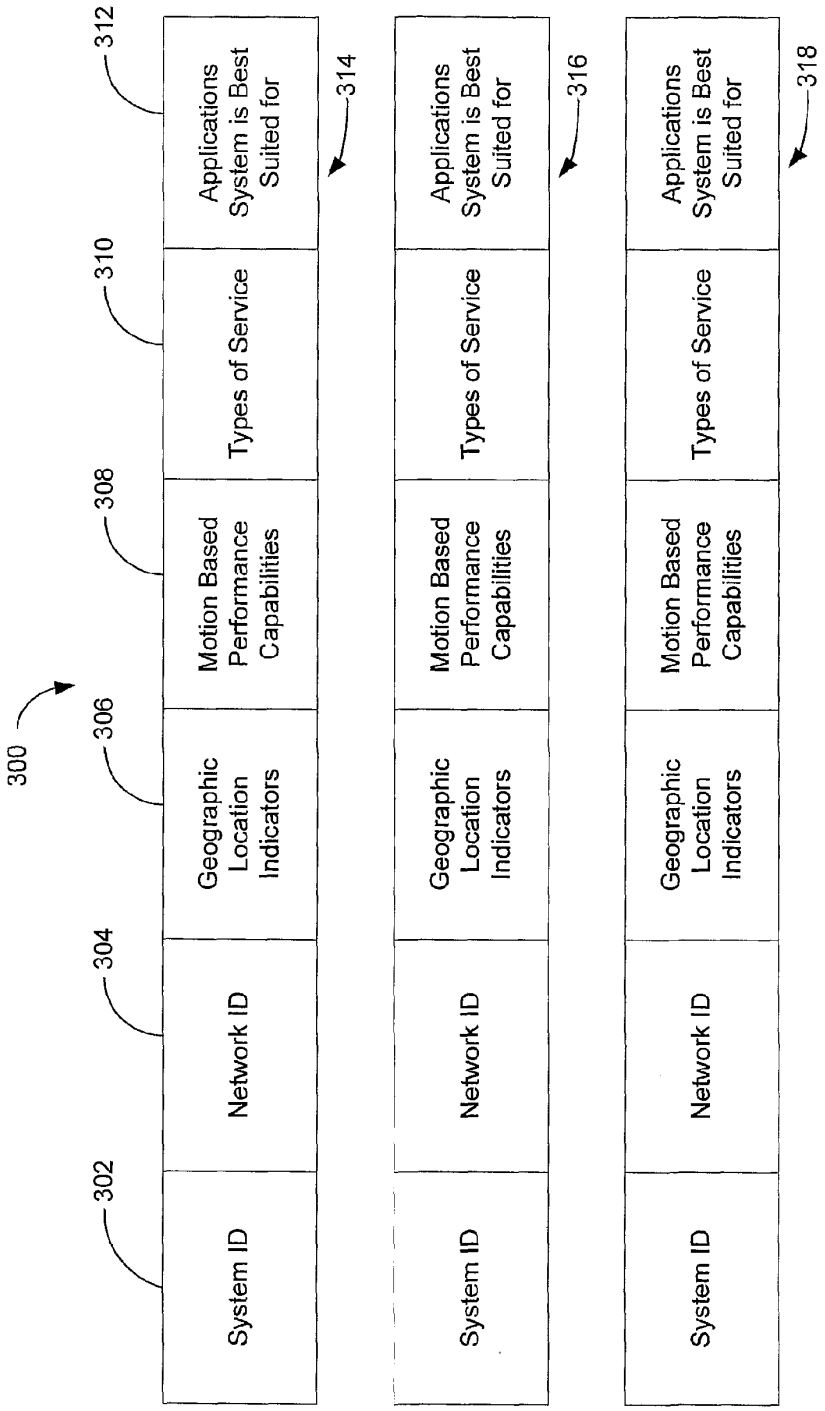

300
302
304
306
308
310
312
314
316
318
System ID
Network ID
Geographic Location Indicators
Motion Based Performance Capabilities
Types of Service
Applications System is Best Suited for
System ID
Network ID
Geographic Location Indicators
Motion Based Performance Capabilities
Types of Service
Applications System is Best Suited for
System ID
Network ID
Geographic Location Indicators
Motion Based Performance Capabilities
Types of Service
Applications System is Best Suited for

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/007079

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/38 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/072581 A1 (TAJIMA TAKESHI ET AL) 15 April 2004 (2004-04-15) figures 4,7 paragraphs [0042], [0044], [0046], [0057], [0064] - [0066], [0073], [0075], [0076], [0079], [0080], [0082], [0085] - [0089], [0097] - [0101]	1-28
X Y	WO 01/41488 A (ROBERT BOSCH GMBH; BRANDES, AXEL; KYNAST, ANDREAS; RUF, MICHAEL; POECH) 7 June 2001 (2001-06-07) page 4, lines 25-30 page 10, line 28 - page 12, line 32 page 14, lines 9-19 page 15, lines 20-23	1-6,8, 10-20, 22-28 7,9,21

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 July 2006	17/07/2006

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Chimet, D

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/007079

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 038 444 A (SCHIPPER ET AL) 14 March 2000 (2000-03-14)	1-6,8, 13, 16-20, 25,28
Y	figure 2 column 2, lines 53-60 column 3, line 50 - column 4, line 3 column 4, lines 34-41 column 5, line 48 - column 6, line 35 column 7, lines 25-45 column 8, lines 45-61 column 13, line 53 - column 14, line 15 column 15, line 20 - column 16, line 10	7,9,21

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/007079

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004072581 A1	15-04-2004	JP 2004140459 A	13-05-2004
WO 0141488 A	07-06-2001	DE 19957642 A1	07-06-2001
		EP 1238558 A2	11-09-2002
		JP 2003516064 T	07-05-2003
		US 6920327 B1	19-07-2005
US 6038444 A	14-03-2000	US 5669061 A	16-09-1997
		US 6198930 B1	06-03-2001

Form PCT/ISA/210 (patent family annex) (April 2005)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2007-318354
(43)Date of publication of application : 06.12.2007

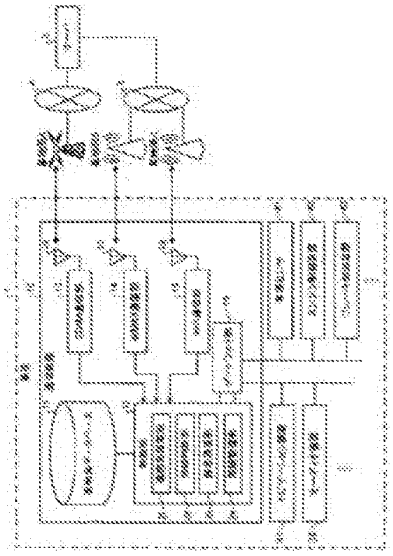
(51)Int.Cl. *H04Q 7/22 (2006.01)*
H04Q 7/38 (2006.01)
H04Q 7/34 (2006.01)

(21)Application number : 2006-144642
(22)Date of filing : 24.05.2006

(71)Applicant : FUJITSU TEN LTD
(72)Inventor : HAGIWARA MASAYUKI
SAWADA JUNICHI

(54) COMMUNICATION DEVICE FOR MOBILE AND COMMUNICATION METHOD FOR MOBILE

(57)Abstract:
PROBLEM TO BE SOLVED: To communicate with a plurality of base stations whose communication modes (communication methods) are different, and actualize smooth switching between communications.
SOLUTION: Communication devices 10 are provided with communication units corresponding to each communication system such as CDMA, WiMAX, WiFi, etc., and register information regarding the base stations in a base station database 11. A base station search unit 21 detects or predicts a base station which is possible to communicate referring the base station database 11, a connection discrimination unit 22 discriminates whether there is a merit to perform a communication connection or not based on the communication mode of the searched base station to determine propriety of connection, and an integrated communication unit 23 communicates with the base station which is discriminated to be possible to be connected.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-318354
(P2007-318354A)
(43)公開日　平成19年12月6日(2007.12.6)

(51)Int.Cl.			F I			テーマコード（参考）
H04Q	7/22	(2006.01)	H04B	7/26	107	5K067
H04Q	7/38	(2006.01)	H04B	7/26	109G	
H04Q	7/34	(2006.01)	H04B	7/26	106A	

審査請求 未請求　請求項の数 11　OL　（全 10 頁）

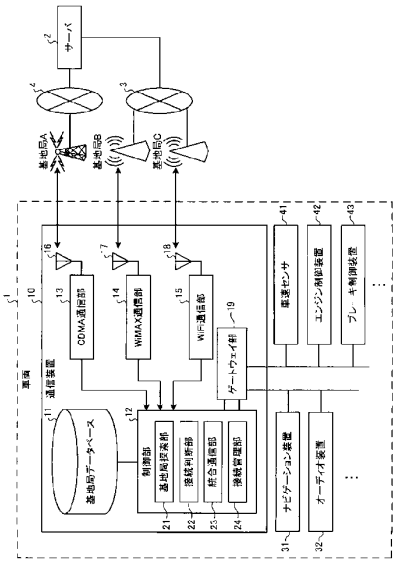
(21)出願番号　特願2006-144642 (P2006-144642)
(22)出願日　平成18年5月24日 (2006.5.24)

(71)出願人　000237592
富士通テン株式会社
兵庫県神戸市兵庫区御所通１丁目２番２８号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　萩原　正之
兵庫県神戸市兵庫区御所通１丁目２番２８号　富士通テン株式会社内
(72)発明者　澤田　純一
兵庫県神戸市兵庫区御所通１丁目２番２８号　富士通テン株式会社内

Fターム(参考)　5K067 BB03 BB04 BB36 DD43 DD44 EE04 EE10 EE24 FF03 FF04 FF05 HH22 HH23 JJ52 JJ56 JJ72

(54)【発明の名称】移動体用通信装置および移動体用通信方法

(57)【要約】
【課題】通信形態（接続方法）の異なる複数の基地局と通信し、通信間の円滑な切り替えを実現すること。
【解決手段】通信装置１０内部にＣＤＭＡ、ＷｉＭＡＸ、ＷｉＦｉなどの各通信方式に対応した通信部を備えるとともに、基地局に関する情報を基地局データベース１１に登録する。基地局探索部２１は、基地局データベース１１を参照して通信可能な基地局を検知もしくは予測し、接続判断部２２は探索した基地局の通信形態に基づき、通信接続するメリットがあるか否かによって接続可否を判断し、統合通信部２３は接続可と判断された基地局と通信する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
通信可能な基地局を探索する基地局探索手段と、
前記通信可能な基地局の通信形態に基づいて、当該基地局との通信接続が必要であるか否かを判断する接続判断手段と、
通信接続が必要であると判断した基地局との通信を行なう通信手段と、
を備えたことを特徴とする移動体用通信装置。
【請求項２】
前記接続判断手段は、前記通信形態として基地局の接続コスト、通信モード、通信方式、伝送速度、使用周波数帯、アクセス方式、通信可能エリア、接続可能な移動体の速度のうち少なくとも何れか一つを用いて前記通信接続の必要性を判断することを特徴とする請求項１に記載の移動体用通信装置。
【請求項３】
前記接続判断手段は、前記基地局の位置、自らの位置、移動経路、移動方向、移動速度、天候、時間帯のうち、少なくとも何れか一つをさらに用いて前記通信接続の必要性を判断することを特徴とする請求項１または２に記載の移動体用通信装置。
【請求項４】
前記接続判断手段は、新たに通信可能な基地局との通信が、既に通信中の基地局との通信に比してメリットが存在する場合に当該新たに通信可能な基地局との通信接続が必要であると判断することを特徴とする請求項１，２または３に記載の移動体用通信装置。
【請求項５】
前記基地局探索手段は、自らの移動方向前方の基地局を選択的に探索することを特徴とする請求項１～４のいずれか一つに記載の移動体用通信装置。
【請求項６】
前記基地局探索手段は、自らの移動経路もしくは移動方向に変更があった場合に前記通信可能な基地局の探索を再実行することを特徴とする請求項１～５のいずれか一つに記載の移動体用通信装置。
【請求項７】
前記基地局探索手段は、複数の基地局の間に設定された優先度に基づいて優先度の高い基地局を接続候補とすることを特徴とする請求項１～６のいずれか一つに記載の移動体用通信装置。
【請求項８】
前記基地局探索手段は、道路沿いの基地局を優先的に接続候補として選択することを特徴とする請求項１～７のいずれか一つに記載の移動体用通信装置。
【請求項９】
前記基地局探索手段は、基地局と建築物との位置関係に基づいて接続候補となる基地局を選択することを特徴とする請求項１～８のいずれか一つに記載の移動体用通信装置。
【請求項１０】
前記通信手段は、同一のサービスを提供する通信形態の異なる複数の基地局と接続中である場合に、前記複数の基地局を切り替えつつ前記サービスを受けることを特徴とする請求項１～９のいずれか一つに記載の移動体用通信装置。
【請求項１１】
通信可能な基地局を探索する基地局探索工程と、
前記通信可能な基地局の通信形態に基づいて、当該基地局との通信接続が必要であるか否かを判断する接続判断工程と、
通信接続が必要であると判断した基地局との通信を行なう通信工程と、
を含んだことを特徴とする移動体用通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】

この発明は、車両などの移動体用の通信装置およびその通信方法に関し、特に通信形態（接続方法）の異なる複数の基地局と通信する通信装置およびその通信方法に関する。

【背景技術】

【０００２】

近年、車両などの移動体に通信機能を持たせる技術が実用化されている。かかる移動体による通信では、その移動に伴って通信相手となる基地局が変化するため、基地局の切り替えを円滑に行うことが重要である。

【０００３】

そこで、例えば特許文献１は、車両にＶＰＮで通信する通信手段を備え、通信手段が基地局と通信するエリアを自車位置から予測し、予測した通信エリアに近づいた場合に予めＶＰＮの構築（ＩＰアドレスやドメインネームの設定など）を行なうことで、迅速に通信接続を行なう技術を開示している。

【０００４】

【特許文献１】特開２００４－３１２３５０号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

ところで、移動体の通信に使用可能な通信形態は、携帯電話網に用いられるＣＤＭＡをはじめとしてＷｉＦｉやＷｉＭＡＸ、ＤＳＲＣなど多岐にわたり、さらに今後増加することが予想される。

【０００６】

また、サービス提供者は、これら複数の通信形態を用いて同一のサービスを提供することが可能である。すなわち、車両側では任意の通信形態を用いた接続によって所望のサービスを受けることができる。

【０００７】

そこで、異なる通信形態を統合して利用する移動体用通信と、通信形態の異なる基地局間での円滑な切り替えの実現が重要な課題となっていた。

【０００８】

本発明は、上述した従来技術の課題を解決するためになされたものであって、特に通信形態の異なる複数の基地局と通信し、通信間の円滑な切り替えを実現する移動体用通信および移動体用通信方法を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するため、本発明に係る移動体用通信装置および移動体用通信方法は、通信可能な基地局を検知もしくは予測し、通信可能な基地局の通信形態に基づいて、当該基地局との通信接続が必要であるか否かを判断し、通信接続が必要であると判断した基地局との通信を行なう。

【発明の効果】

【００１０】

本発明によれば移動体用通信装置および移動体用通信方法は、通信形態の異なる基地局から接続先を選択する場合に、基地局との通信接続の必要性に基づいて選択を行なうので、通信形態の異なる複数の基地局と通信し、通信間の円滑な切り替えを実現する移動体用通信装置および移動体用通信方法を得ることができるという効果を奏する。

【発明を実施するための最良の形態】

【００１１】

以下に添付図面を参照して、この発明に係る移動体用通信装置および移動体用通信方法の好適な実施例について詳細に説明する。

【実施例】

【００１２】

図１は、本発明の実施例である車両用の通信装置１０の概要構成を示す概要構成図であ

る。同図に示すように、通信装置１０は、車両１に搭載され、ナビゲーション装置３１、オーディオ装置３２、車速センサ４１、エンジン制御装置４２、ブレーキ制御装置４３などと接続する。

【００１３】

ナビゲーション装置３１は、ＧＰＳ（Global Positioning System）人工衛星と通信して特定した自車両の位置と、予め記憶した地図データとを利用して走行経路の設定および誘導を行なう車載装置である。また、ナビゲーション装置３１は、通信装置１０に対して自車両の位置情報や周辺の地図情報、走行予定経路、時刻情報などを提供する。

【００１４】

車速センサ４１は、タイヤの回転速度などから車両１の走行速度を検知して、通信装置１０に出力する。また、エンジン制御装置４２はエンジンの動作制御を、ブレーキ制御装置４３はブレーキの動作制御を行なうＥＣＵであり、通信装置１０に対して自車両の動作状態を通知する。さらに、エンジン制御装置４２やブレーキ制御装置４３は、通信装置１０による外部との通信によってファームウェアの更新などを行なうことができる。

【００１５】

通信装置１０は、その内部に基地局データベース１１、制御部１２、ＣＤＭＡ通信部１３、ＷｉＭＡＸ通信部１４、ＷｉＦｉ通信部１５、アンテナ１６～１８およびゲートウェイ部１９を有する。

【００１６】

ゲートウェイ部１９は、制御部１２によって接続された各通信部（ＣＤＭＡ通信部１３、ＷｉＭＡＸ通信部１４、ＷｉＦｉ通信部１５）からのデータを、後段のエンジン制御装置４２、ブレーキ制御装置４３などの車載装置、あるいはナビゲーション装置３１へ各々伝送するための装置である。例えば、通信データが地図の更新であればゲートウェイ部１９を介してナビゲーション装置３１にデータ伝送し、エンジン制御のメンテナンスデータであればゲートウェイ部１９を介してエンジン制御部４２へ伝送する。

【００１７】

ＣＤＭＡ通信部１３は、アンテナ１６を用いて基地局ＡとＣＤＭＡ（Code Division Multiple Access）方式による通信を行なうことで、携帯電話回線網４に無線接続する。また、ＷｉＭＡＸ通信部１４は、アンテナ１７を用いて基地局ＢとＷｉＭＡＸに（world interoperability for microwave access）よる通信を行なうことで、インターネット３に無線接続する。同様に、ＷｉＦｉ通信部１５は、アンテナ１８を用いて基地局ＣとＷｉＦｉによる通信を行なうことで、インターネット３に無線接続する。

【００１８】

ここで、渋滞や天候などの情報提供、音楽のダウンロードによる提供などのサービスを行なうサーバ２は、携帯電話回線網４とインターネット３の双方に接続している。そのため、通信装置１０は任意の通信方式を用いて所望のサービスを受けることができる。

【００１９】

基地局データベース１１は、基地局に関する情報を記憶する記憶手段である。基地局データベース１１の構成例を図２に示す。同図において基地局データベース１１は、各基地局の位置、接続重み、接続コスト、通信モード（インフラストラクチャ、アドホック、メッシュなど）、通信方式、伝送速度、周波数帯、アクセス方式、通信可能エリア、移動速度、契約状況、接続先アドレスやパスワードを記憶している。

【００２０】

基地局の位置は、緯度経度の指定によって特定される。また、接続重みは、その基地局との接続に対する優先度を示す値であり、接続コストは接続に要するコスト、例えば通信装置１０にかかる処理負荷や料金などを示す値である。また、通信モードや通信方式、アクセス方式は、その基地局の通信形態を特定する情報である。

【００２１】

伝送速度はその基地局との通信における通信速度であり、周波数帯は、通信に使用する周波数を示す。さらに、通信可能エリアはその基地局と通信可能な距離を示し、移動速度

はその基地局と通信する際における移動速度（車両の走行速度）の上限を示す情報である。

【００２２】

契約状況は、その基地局と通信する際に予め必要な契約がなされているか否かを示す情報であり、接続先アドレスやパスワードはその基地局と通信する際に使用する接続準備情報である。

【００２３】

制御部１２は、ＣＰＵから成るマイコンなどによって実現され、各通信部１１～１３に対する接続、切断、監視を行なうネットワーク制御を行なう処理部であり、その内部に基地局探索部２１、接続判断部２２、統合通信部２３、接続管理部２４を有する。

【００２４】

基地局探索部２１は、基地局データベース１１が記憶する基地局の情報や、通信装置１０の外部から取得した各種情報を用いて、通信可能な基地局を検知もしくは予測する処理を行なう。

【００２５】

具体的には、基地局データベース１１が記憶する基地局の位置と通信エリアから各基地局と通信可能なエリアを特定する。そして、自車両の位置や進行方向、移動速度、予定経路から自車両と通信可能な基地局を検知し、また通信可能となる基地局を予測する。

【００２６】

接続判断部２２は、基地局探索部２１が探索した基地局との通信接続が必要であるか否かを判断する。具体的には、接続判断部２２は、新たに通信可能な基地局との通信が、既に通信中の基地局との通信に比してメリットが存在する場合に新たに通信可能な基地局との通信接続が必要であると判断する。

【００２７】

例えば、新たに通信可能な基地局の伝送速度が高い場合や、接続コストが小さい場合には、メリットが存在するので通信接続が必要であると判断する。また、通信エリアの大きさや位置、移動速度の上限と、自車両の位置、走行予定経路、移動方向、移動速度から安定して長時間通信できる可能性がある場合にも、メリットが存在するので通信接続が必要であると判断する。

【００２８】

さらに、同一の周波数を使用する通信接続を複数並行して実行すると電波状態が不安定となるので、それまでの通信とは異なる周波数帯を使用する基地局についてもメリットがあると判断する。

【００２９】

また、天候や時間帯をさらに使用することもできる。例えば、電波状態が良好になる晴天時には安定性よりも通信速度を重視してメリットの判断を行ない、利用者の数が多く、通信トラフィックの増大が予測される時間帯については通信速度よりも安定性を重視してメリットの判断を行なえばよい。なお、天候の情報は例えばサーバ２から取得することができ、時間情報はナビゲーション装置３１から取得することができる。

【００３０】

統合通信部２３は、接続が必要であると判断された基地局の接続準備情報を用い、通信処理を行なう処理部である。ここで、同一のサービスを提供する通信形態の異なる複数の基地局と接続中である場合、統合通信部２３は、複数の基地局を切り替えつつ目的のサービスを受けることができる。

【００３１】

接続管理部２４は、基地局との接続結果や接続予定の管理を行なう処理部である。例えば、接続した基地局の履歴を走行した道路に対応付けて記憶し、同じ道路を走行する場合に過去に接続した基地局の履歴に沿って接続を行うことができる。

【００３２】

また、基地局の情報をサーバ２などから取得して基地局データベース１１を更新する、

基地局データベース１１を参照して接続を試みた結果、撤去されていたり、停止している基地局があったなど基地局データベース１１と差異があった場合にはサーバ２などへ通知したり、基地局データベース１１を更新する、などの処理を行なうこともできる。

【００３３】

さらに、自車両の目的地までの経路をナビゲーション装置３１が設定している場合には、予め接続すべき基地局の順番を決めておき、この順番に従って基地局との接続を行うこともできる。

【００３４】

また、目的地までの経路上で使用した基地局の履歴をサーバ２などに送信して他のユーザが利用できるようにしたり、目的地までの経路上で他のユーザが使用した基地局の履歴をサーバ２などから取得して使用することもできる。

【００３５】

つぎに、通信装置１０の動作例について図３を参照して説明する。同図において、車両１は、位置１ａから位置１ｂ、位置１ｃ、位置１ｄの順に移動している。位置１ａでは、通信装置１０は携帯電話回線網４と接続する基地局Ａのみと通信し、サーバ２から交通情報などのセンタコンテンツを受信している。

【００３６】

その後、車両１が位置１ｂに移動すると、通信装置１０は基地局ＢとＷｉＭＡＸ通信を行ない、ＷｉＭＡＸ通信によって地域情報を取得するとともに、音楽のダウンロードを行なっている。

【００３７】

さらに、車両１が位置１ｃに至ると基地局Ｃと通信可能となる。基地局ＣとのＷｉＦｉ通信は、既に接続しているＷｉＭＡＸ通信に比して通信速度でのメリットがあるため、通信装置１０は基地局Ｃとの通信を開始する。

【００３８】

この位置１ｃにおいては、通信装置１０は、ＷｉＭＡＸ通信による地域情報の取得を継続するとともに、ＷｉＦｉ通信によって地域情報よりもさらに狭い範囲の情報である周辺情報を取得する。

【００３９】

また、音楽のダウンロードはＷｉＭＡＸ通信でもＷｉＦｉ通信でも実行可能であるので、通信装置１０は音楽ダウンロードをより高速なＷｉＦｉ通信に切り替えて継続する。

【００４０】

その後、車両１が位置１ｄに至って基地局ＣとＷｉＦｉ通信が不可能となると、通信装置１０は基地局Ｂと同様にＷｉＭＡＸ通信を提供する基地局Ｄとの通信を行なう。

【００４１】

この位置１ｄにおいて通信装置１０は、ＷｉＭＡＸ通信による地域情報の取得を継続するとともに、ＷｉＦｉ通信を利用して行なっていた音楽ダウンロードを、再びＷｉＭＡＸ通信に切り替えて継続している。

【００４２】

つづいて、制御部１２の処理動作について、図４のフローチャートを参照して説明する。同図に示す処理動作は、制御部１２のメインルーチン、もしくはその一部として繰り返し実行される処理である。

【００４３】

同時に示すように、まず制御部１２内部の基地局探索部２１は、車両の現在位置情報、道路情報、車両の進行方向、車速情報を読み出す（ステップＳ１０１）。さらに、現在位置から所定範囲にある基地局の情報を基地局データベース１１から読み出して（ステップＳ１０２）、新たな基地局に接近しているか否かを判定する（ステップＳ１０３）。

【００４４】

その結果、新たな基地局に接近していなければ（ステップＳ１０３，Ｎｏ）そのまま処理を終了し、新たな基地局に接近している場合に（ステップＳ１０３，Ｙｅｓ）、接続判

断部２２が新たな基地局との通信接続にメリットがあるかを判断する（ステップＳ１０４）。

【００４５】

そして、新たな基地局との通信接続にメリットが無ければ（ステップＳ１０４，Ｎｏ）そのまま処理を終了し、メリットがあるならば（ステップＳ１０４，Ｙｅｓ）、統合通信部２３が基地局データベース１１から接続準備情報を読み出して接続準備を行なう（ステップＳ１０５）。

【００４６】

その後、接続準備を行なった基地局の電波強度が閾値以上となったならば（ステップＳ１０６，Ｙｅｓ）、読み出した接続準備情報を用いて基地局に接続し（ステップＳ１０７）、処理を終了する。

【００４７】

つづいて、基地局探索部２１による基地局探索についてさらに説明する。基地局探索部２１は、車両１の移動方向や走行予定経路に基づいて、前方に存在する基地局を選択的に探索する。例えば図５に示すように、車両１が位置１ｅを走行中である場合、後方領域６に位置する基地局ｃ１１および基地局ｃ１２は除外して基地局の探索を行なう。

【００４８】

また、車両１の進行方向や走行予定経路に変更があった場合、走行予定経路を外れた場合には基地局の探索を再実行する。

【００４９】

例えば、図５において車両１が位置１ｅを走行し、基地局ｃ１３と通信中である場合、車両１が直進する予定ならば基地局ｃ１３の後に接続すべき基地局の候補（接続候補）として前方領域５に位置する基地局ｃ１４および基地局ｃ１５を選択する。

【００５０】

その後、車両１が右折して位置１ｆを走行したならば、基地局探索部２１は、基地局の探索を再実行し、基地局ｃ１６，ｃ１７，ｃ１８を接続候補とする。

【００５１】

ここで、基地局ｃ１７と基地局ｃ１８のように、基地局から道路までの距離に差がある場合には、基地局探索部２１は、道路に近い（道路沿いの）基地局を優先的に接続候補とすることで、通信時の電波状態が安定し、かつ長時間通信できる可能性のある基地局を選択する。そのため、図５においては、基地局ｃ１７に対して基地局ｃ１８を優先することとなる。同様に、道路と基地局との間に遮蔽物となる建物が存在する場合には、そのような遮蔽物のない基地局を優先的に接続候補とする。

【００５２】

また、複数の基地局の間には、優先度（接続重み）を設定しておくことが好ましい。基地局間の優先度の設定例を図６に示す。同図において車両１は、基地局ｃ２１と通信中であり、次につながる可能性のある基地局は基地局ｃ２２および基地局ｃ２３である。

【００５３】

ここで、基地局間の距離、接続可否、周辺環境（道路からの近さや建物の有無）などに基づいて、基地局ｃ２１と基地局ｃ２２の間は優先度１に設定され、基地局ｃ２１と基地局ｃ２３との間は優先度４に設定されている。この優先度は、次につながる可能性の高さを示し、値が小さいほど次につながる可能性が高い。

【００５４】

そのため、車両１が基地局ｃ２１の次に接続する可能性の高いのは基地局ｃ２３となり、車両１は基地局ｃ２３に優先的につなげるよう接続準備を行ない、基地局ｃ２２を第二候補とする。

【００５５】

同様に、基地局ｃ２３の次につながる可能性のある基地局は基地局ｃ２４と基地局ｃ２５であるが、基地局ｃ２４が接続できない状態であるため、基地局ｃ２３から基地局ｃ２４への優先度は１０に設定されている。一方、基地局ｃ２３から基地局ｃ２５への優先度

は２に設定されているので、基地局ｃ２３の次には基地局ｃ２５に接続する可能性が高い。

【００５６】

上述してきたように、本実施例にかかる通信装置１０は、基地局データベース１１を参照して通信可能な基地局を検知もしくは予測し、その基地局との通信接続にメリットがあるか否かによって接続可否を判断するので、通信形態の異なる複数の基地局との通信を統合して制御し、通信間の円滑な切り替えを行うことができる。

【００５７】

なお、本発明はかかる実施例によって限定されるものではなく、適宜変更して実施することができる。例えば、通信によって取得する情報の種類によって優先的に選択する通信方式を変更するようにしてもよい。具体的には、車両の動作制御に関わるＥＣＵのファームウェアを変更するデータを受信する場合には、セキュリティ強度に優れた通信を優先的に使用することが望ましい。

【００５８】

また、例えば基地局への接続が失敗した場合には、その基地局の優先度を下げて次回以降は他の基地局を優先的に使用するようにしてもよい。

【００５９】

さらに、検知もしくは予測した基地局の情報を地図表示などに重ね合わせて表示し、ユーザ（車両乗員）が手動で接続先を指定できるようにしても良い。

【産業上の利用可能性】

【００６０】

以上のように、本発明にかかる移動体用通信装置及び移動体用通信方法は、車両などの移動体用における通信に有用であり、特に通信形態の異なる複数の基地局との通信に適している。

【図面の簡単な説明】

【００６１】

【図１】本発明の実施例にかかる通信装置の概要構成を示す概要構成図である。

【図２】図１に示した基地局データベースの構成例を説明する説明図である。

【図３】図１に示した通信装置１０の動作例を説明する説明図である。

【図４】図１に示した通信装置１０の処理動作について説明するフローチャートである。

【図５】基地局の探索動作について説明する説明図である。

【図６】基地局間の優先度設定について説明する説明図である。

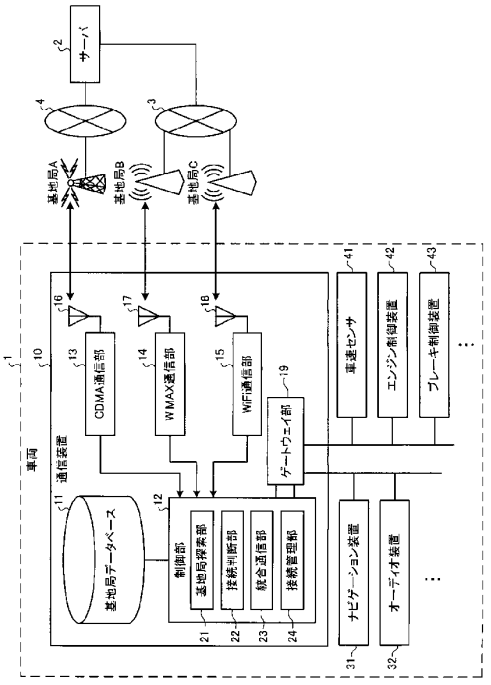
【符号の説明】

【００６２】

１　車両
２　サーバ
３　インターネット
４　携帯電話回線網
５　前方領域
６　後方領域
１０　通信装置
１１　基地局データベース
１２　制御部
１３　ＣＤＭＡ通信部
１４　ＷｉＭＡＸ通信部
１５　ＷｉＦｉ通信部
１６～１８　アンテナ
１９　ゲートウェイ部
２１　基地局探索部
２２　接続判断部

２３　　統合通信部
２４　　接続管理部
３１　　ナビゲーション装置
３２　　オーディオ装置
４１　　車速センサ
４２　　エンジン制御装置
４３　　ブレーキ制御装置

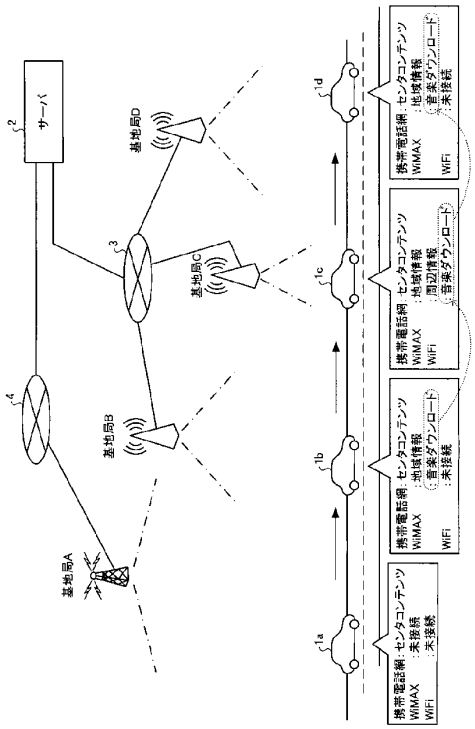
【図１】



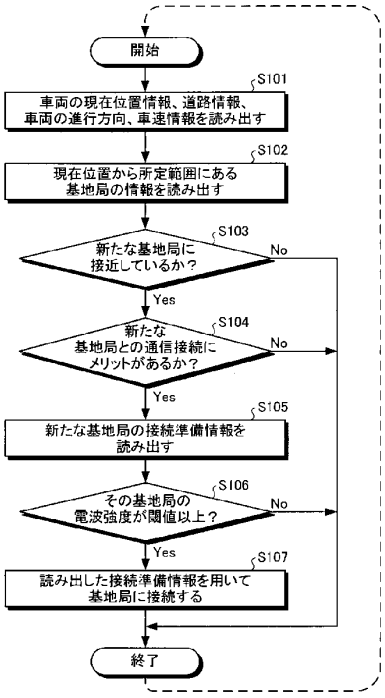
【図２】

基地局	位置（中心）	接続度み	接続コスト	通信モード	通信方式	伝送速度	周波数帯	アクセス方式	通信可能エリア	移動速度	契約	接続先ランク
A	経度x1緯度y1	1	10	インフラストラクチャ	CDMA	○○Mbit/s	○○GHz	CDMA	10km	○○km/h	○	AAA
B	緯度x2経度y2	10	20	インフラストラクチャ	WiMAX	□□Mbit/s	□□GHz	OFDMA	2km	□□km/h	○	BBB
C	緯度x3経度y3	2	50	インフラストラクチャ	WiFi	△△Mbit/s	△△GHz	CSMA	100m	△△km/h	○	CCC
D	緯度x4経度y4	10	20	メッシュ	WiMAX	□□Mbit/s	□□GHz	OFDMA	2km	□□km/h	○	BBB
E	緯度x5経度y5	1	10	インフラストラクチャ	CDMA	○○Mbit/s	○○GHz	CDMA	10km	○○km/h	－	－

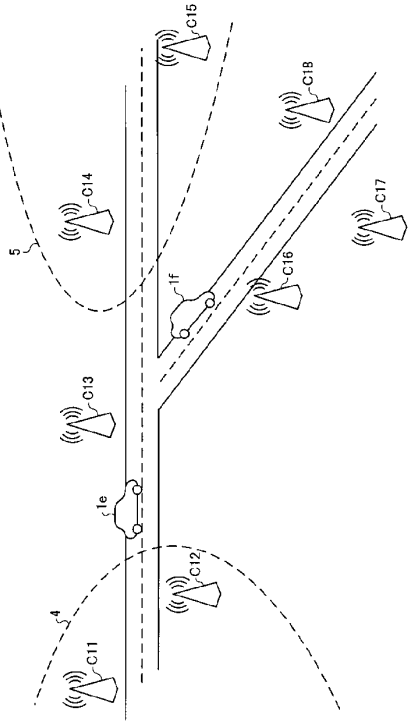
【図３】


サーバ
2
基地局D
基地局C
基地局B
基地局A
3
4
1a
1b
1c
1d
携帯電話網：センタコンテンツ
WiMAX：未接続
WiFi：未接続
携帯電話網：センタコンテンツ
WiMAX：地域情報
WiFi：周辺情報
音楽ダウンロード
携帯電話網：センタコンテンツ
WiMAX：地域情報
WiFi：音楽ダウンロード
未接続
携帯電話網：センタコンテンツ
WiMAX：地域情報
WiFi：音楽ダウンロード
未接続

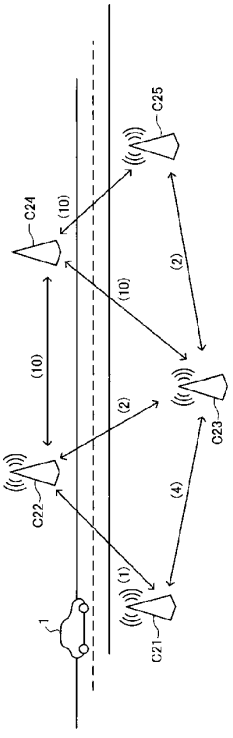
【図４】


開始
S101
車両の現在位置情報、道路情報、
車両の進行方向、車速情報を読み出す
S102
現在位置から所定範囲にある
基地局の情報を読み出す
S103
新たな基地局に
接近しているか？
No
Yes
S104
新たな
基地局との通信接続に
メリットがあるか？
No
Yes
S105
新たな基地局の接続準備情報を
読み出す
S106
その基地局の
電波強度が閾値以上？
No
Yes
S107
読み出した接続準備情報を用いて
基地局に接続する
終了

【図５】


C15
C18
C14
C17
5
1f
C16
C13
1e
C12
4
C11

【図６】


C25
C24
(10)
(2)
(10)
(10)
(2)
C23
C22
(4)
(1)
C21
1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 November 2007 (08.11.2007)

PCT

(10) International Publication Number
WO 2007/126352 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04Q 7/38* (2006.01)

(21) International Application Number:
PCT/SE2006/050538

(22) International Filing Date:
5 December 2006 (05.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0600965-8 2 May 2006 (02.05.2006) SE

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KAZMI, Muhammad, Ali** [PK/SE]; Svartviksslingan 110, 3 Tr, S-167 39 Bromma (SE). **FODOR, Gabor** [SE/SE]; Astrakangatan 124, S-165 52 Hässelby (SE).

(74) Agent: **HASSELGREN, Joakim**; Ericsson AB, Patent Unit LTE, S-164 80 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

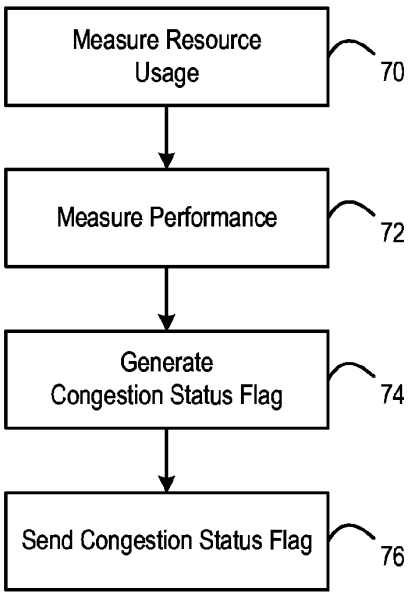
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

[Continued on next page]

(54) Title: A METHOD FOR GENERATING A CONGESTION FLAG BASED ON MEASURED SYSTEM LOAD



(57) Abstract: A radio base station generates a congestion status flag, based on measured resource usage in its cell, and based on performance of sessions in the cell. The flag may be a one bit, or a small number of bits, indicating whether the base station is congested. The flag can be sent to neighbouring radio base stations, for use in determining whether to perform handovers to that radio base station. The flag generated in a radio base station, and the flags generated in neighbouring radio base stations, can also be sent to user equipment in a cell.

WO 2007/126352 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD FOR GENERATING A CONGESTION FLAG BASED ON MEASURED SYSTEM LOAD

FIELD OF THE INVENTION

The present invention relates to methods and arrangements in cellular mobile communication systems, in particular to efficient radio resource management in an evolved UMTS Terrestrial Radio Access (E-UTRA) Network.

BACKGROUND AND SUMMARY

In order to meet high target bit rate requirement in an evolved UMTS Terrestrial Radio Access (E-UTRA) Network, efficient radio resource management (RRM) techniques are required. The realization of efficient RRM methods requires exchange of measurements across different network nodes. The measurement reports indicate the resource usage in a certain network node such as average transmission power level. Generally these measurements are needed before the execution of an RRM function. Since there are different types of resources, there are several kinds of measurement reports that are to be communicated between the network nodes, notably between NodeBs, in order to efficiently perform the RRM operation. Although measurement reports are critically important, excessive or unnecessary measurement reporting should be avoided in order to minimize the signaling overheads. Our key observation is that there are a multitude of radio resource measurements that need to be communicated between radio network nodes for efficient radio resource management.

In cellular systems the RRM techniques, namely admission control and handover control, play a key role in achieving the desired grade and quality of service (GoS/QoS) targets

(see also the documents 3GPP TR 25.922 "Radio Resource Management Strategies" and 3GPP TS 25.331 "Radio Resource Protocol Specifications" issued by the 3rd Generation Partnership Project). The main purpose of the admission control is to ensure that the QoS of the new session can be fulfilled. Secondly, it should also ensure that the admission of a new user should not adversely affect the performance of the ongoing sessions.

In UTRA the admission control functionality is located in the radio network controller (RNC), where the radio resource control (RRC) protocol is also terminated. The admission control process in UTRA should take into account several types of resources such as downlink transmitted power, downlink channelization code usage and uplink received total wideband power (RTWP). In UTRA, similarly to admission control, the handover is also carried out by the RNC, which is aware of the resource situation of the target cells, as discussed in the document 3GPP TR 25.922 "Radio Resource Management Strategies".

When a new call or a handover is required, it will be denied if the required respources are not available in the target cell of the target Node B.

Figure 1 illustrates a handover attempt failure due to insufficient cell resources. That is, Figure 1 illustrates a serving Node B sending a handover request to a target Node B. The handover request is denied by the target Node B since uplink resource blocks are either fully utilized or their usage is above a certain threshold. The handover failure can however be prevented to some extent by inquiring the resource usage at the target Node B prior to handover attempt.

Figure 2 therefore illustrates another scenario, where the serving Node B first requests the target Node B to report its measurements, for all type of resources, in order to prevent any handover failure due to the cell resource bottleneck. Only after receiving the measurement reports does the serving Node B determine whether that possible target Node B should be the target Node B for a handover attempt. It is clear that, in this type of situation where the target Node B cannot serve a new call due to lack of resources, the complete set of measurement reporting is wasteful of bandwidth and leads to unnecessary handover latency. In case of a failure of the handover attempt, the serving Node B typically repeats the above mentioned procedures with the second best target Node B and so on.

Hence, in an existing system the situation may arise in which several handover attempts may be needed before the handover is successfully executed. Secondly this would lead to considerable signaling overheads. The above mentioned problems have been identified and realized already from the past experiences in UTRA. The current WCDMA network utilizes try/fail/adjust/reattempt way of handling resource congestions problems.

It has thus been observed to be a problem that admission control and handover control cannot be efficiently used due to an inefficient use of radio resources. It is thus an objective to reduce unnecessary measurement reports in E-UTRA and a need to specify simple mechanisms of exchanging measurement reports between the Node Bs. There is also a need for devising mechanisms whereby the congestion situation in network could be communicated between the Node Bs in simple manner. For instance, it has been proposed to multicast congestion status in the form of single level of congestion such as available free capacity. In the current

proposal the congestion status does not consider the aggregation of all different types of radio, transport network and hardware resources. In addition the congestion status does not include the measured performance such as ongoing grade of service performance. However, a situation can arise in which the system is not fully congested but still the requested QoS requirements cannot be met.

According to an aspect of the present invention, a network node generates a congestion flag, indicative of measured resource usage and measured performance, and this can then be used as a basis for determining whether to attempt to access that node.

In preferred embodiments, the invention can therefore provide some of the following advantages, namely:

A simple way to indicate congestion status to the neighbour base stations and to the UEs.

Minimizing of handover failure and handover attempt failure, thereby improving grade of service. Particular advantage in distributed systems where handover is located in Node B.

Reduction of measurement reports when they are not needed. Particular advantage in distributed systems where excessive reports can overwhelm signalling links between the base stations.

Allowing the serving Node B to update the neighbour cell list. This will allow UE to do measurement on cells, which can accommodate new links. This will also reduce the number of UE measurements.

New call blocking can be reduced. Particular advantage in distributed systems where admission control is located in Node B.

Realization of multi-cell RRM in distributed architecture where there is no centralized controller with radio related information.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a handover attempt failure due to insufficient cell resources.

Figure 2 illustrates measurements required to prevent handover failures, in accordance with the prior art.

Figure 3 illustrates a radio access network architecture of E-UTRA.

Figure 4 illustrates an example of the resource situation in a target Node B.

Figure 5 illustrates an example for a flag generation at a Node B.

Figure 6 illustrates a 4-level congestion status diagram realized by single bit using state transition method.

Figure 7 is a flow chat, illustrating a process for generating a congestion status flag.

Figure 8 is a flow chart, illustrating a process for initiating a handover using a congestion status flag.

Figure 9 is a flow chart, illustrating the transmission of the updated neighbour cell list to a user equipment.

Figure 10 illustrates a part of a telecommunication network including a radio base station and a user equipment for which the present invention is applied.

DESCRIPTION

The present invention is particularly applicable to a cellular wireless communications system, for example as shown in Figure 3. In the example network shown in Figure 3, the network 10 is an evolved UMTS Terrestrial Radio Access (E-UTRA) network, although it will be apparent that the invention is similar applicable to other types of network.

Figure 1 shows a part of the network, containing four radio base stations, or Node Bs, although it will be apparent that the network will contain many more than this number. In E-UTRA, the RRC terminates in the Node B. As shown in Figure 3, the Node Bs each have respective connections 12, 14, etc, to an access gateway (aGW) 16, which performs only user plane switching but is not aware of any radio related information such as cell load etc. In order to carry out admission control and handovers, the serving network node should be aware of the load at the target node. Thus in E-UTRA both admission control and handovers are placed in the Node B. Each of the direct interfaces 18, 20, etc between the Node Bs (the X2 interfaces) is simply a control plane that can transport measurement reports, handover related commands etc.

E-UTRA is designed to achieve a significantly higher data rate compared to UTRA. Secondly, in E-UTRA the latency requirements of certain functions such as handover, is considerably more stringent than in WCDMA. This means that admission control and handover failures should be minimized because otherwise latency will increase. Thus, in E-UTRA,

efficient admission control and handover execution may require the Node B to monitor various types of measurements such as transmitted power, RTWP, resource block usage, transport network channel usage etc. By using more comprehensive resource information at the Node B, the admission and handover decisions can be made more predictable.

In E-UTRA there are several types of radio and network resources that are assigned to a session by the serving Node B. Some important resources that are to be used in E-UTRA are: the Downlink transmit power; the Uplink received total Interference; the Downlink resource blocks (DL RB); the Uplink resource blocks (UL RB); the Uplink transport network resources (UL TrNetCh); the Downlink transport network resources (DL TrNetCh); and the Hardware resources.

It should be noted that a new call or a handover request can be denied due to the lack of availability of any one of the cell resources listed above. This is illustrated in Figure 4, which shows certain average usage levels of different types of cell resources in a target cell of the target Node B. Figure 4 illustrates an example situation, where only one of the cell resources (that is, the uplink resource blocks) is fully occupied, but other resources are still available.

It is the basic idea of the current invention that each Node B generates a congestion status flag based on resource usage and measured performance to indicate whether or not a new connection can be served. The flag can be sent to neighbour Node Bs to prevent handover failures or it can be broadcasted in its own cell to facilitate admission control. The congestion status flag can also be used by the serving Node B to dynamically set the neighbour cell list, which is used by the UE to do downlink measurements.

Figure 5 illustrates the generation of the flag in the Node B. Two sets of measurements are fed into the flag generating algorithm as shown in figure 5. The first set of measurements relate to usage of resources at the Node B such as the downlink transmitted power (X_1), the downlink resource block usage (X_2), the uplink transport network channel usage (X_N), etc. The second set of measurements relate to the measured performance, which may include the fraction of unsatisfied users (Y_1), the new session blocking probability or P_b (Y_2), the ongoing session dropping probability or P_d (Y_M), the mean user bit rate etc. The measurements can be done over a certain time period. Different resource and performance metrics types may have different measurement periods.

As shown in Figure 5, each measurement is compared with a certain threshold. Specifically, as indicated in the figure, X_i and γ_i represent measured cell resource *i* and the corresponding threshold, respectively. Similarly, Y_i and β_i represent measured performance *i* and the corresponding threshold, respectively. In this example, any of the input measurements exceeding its respective threshold would generate a flag=1, indicating congestion in the network. The algorithm that generates the flag in the Node B is implementation dependent (involving the setting of threshold levels, defining the flag generation logic, etc). However, the main idea is the generation of congestion flag based on two sets of measurements: resource usage and measurement performance.

In Figure 5 the flag generation logic is exemplified by a simple OR operation. Other flag generation mechanisms assigning weights to different resources and hysteresis values are also possible.

In its simplest form, the flag may comprise a single bit of information as depicted in the table below, where Flag = 1 and Flag =0 manifest congestion and no congestion situations respectively in a cell.

Table 1: Preventive flag

Flag	Meaning
1	Congestion
0	NO Congestion

Different services typically require different amounts of resources. Thus, it is advantageous to have multilevel signalling, i.e. some intermediate levels between congestion and no congestion states. For example, multilevel congestion status can be realized either by using more bits (e.g. 2 bits for 4-levels); or by using multiple states and state transitions with the same number of bits (e.g. 1 bit for 4-levels).

As an example, we can consider the 4-level case, where the congestion status, in addition to the two extreme situations, can also indicate if the target cell can accept low or medium bit rate services. The table below depicts as examples two 4-level congestion status signalling mechanisms, using 2-bits and using a single bit to indicate state transitions, respectively.

Congestion Flag		Meaning
Method 1: 2-bits	Method 2: State transition (states)	
00	1	NO congestion
01	2	Accept medium bit rate
10	3	Accept low bit rate
11	4	Congestion

The state transition based signalling mechanism for 4-level congestion status is also illustrated by the 4-state transition diagram in Figure 6. The state transition method, i.e. method 2 in the table, governs the transitions between congestion states rather than indicating the congestion level itself. Thereby multiple congestion levels are maintained but the signalled information between network nodes is 1 bit at a time. However the obvious drawback is that only adjacent congestion states can be reported using 1 bit. On the other hand, in the first method, whereby each state is explicitly represented by 2-bits, a congestion status report can be completely independent of the previous report. An M-level congestion status flag generation algorithm in the Node B can be realized by having M-1 thresholds for both sets of input parameters: resource usage and measurement performance. Thus, a 4-level congestion status would require 3 thresholds for each type of measurement.

The E-UTRA system shall also support inter-RAT handovers, which means handovers to other access technologies such as UTRA and GERAN. In case Node Bs or base stations belonging to different radio access technologies are co-sited (e.g. UTRA/E-UTRA Node Bs at same location), a multi-RAT flag can also be sent to the neighbour Node Bs of these other RATs. This will provide E-UTRA Node Bs with an overall status of the resource situation in cells belonging to other technologies. The multi-RAT flag can depict 2-level or multilevel congestion status as described above. The table below illustrates an example, where 2-level congestion status indicates the congestion in different technologies. In this example both E-UTRA Node B (eNode B) and GSM base station are congested.