Amendments

☐ Cancel in this application original claims _____ of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

					Small Entity			Large Entity	
					Rate	Fee		Rate	Fee
Filing Fees					x $165 = $		OR	x $330 = $	330
Search Fees					x $270 = $		OR	x $540 = $	540
Examination Fees					x $110 = $		OR	x $220 = $	220
CLAIMS	Filed.		Extra						
Total	32	Less 20	12		x $26 = $		OR	x $52 = $	624
Independent	4	Less 3	1		x $110 = $		OR	x $220 = $	220
Multiple Dependent Claims			-0-		x $195 = $		OR	x $390 = $	
Declaration and Surcharge Fee					X $65 = $		OR	X $130 = $	130
Excess Page Fee									1350
					TOTAL FILING FEE $			TOTAL FILING FEE $	**3414.00**

☐ Applicants petition for an extension of time to respond under 37 CFR § 1.136(a) as follows:

	SMALL ENTITY			LARGE ENTITY	
	Rate	Add'l Fee		Rate	Add'l Fee
☐ Extension for Response within FIRST month	x $65 = $		OR	x $130 = $	
☐ Extension for Response within SECOND month	x $245 = $		OR	x $490 = $	
☐ Extension for Response within THIRD month	x $555 = $		OR	x $1110 = $	
☐ Extension for Response within FOURTH month	x $865 = $		OR	x $1730= $	
☐ Extension for Response within FIFTH month	x $1175 = $		OR	x $2350 = $	

☒ Check No. 4772 for $3414.00 is enclosed.

General Authorizations

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed to Deposit Account No. 50-0685 (Order No. RALEP018).

☒ The Commissioner is given general authorization to charge any fees or to credit any overpayment during the pendency of this application to Deposit Account No. 50-0685 (Order No. RALEP018).

☒ Please send correspondence to the following address:

Customer No. 21912
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd.
Suite 200
Cupertino, CA 95014

Date: 5-26-2009

Michael J. Schallop
Reg. No. 44,319

JUN 01 2009
PATENT & TRADEMARK OFFICE

JFW

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/380,773	03/02/2009	Gregory G. Raleigh	RALEP018

RECEIVED
MAR 31 2009

CONFIRMATION NO. 5719

FORMALITIES LETTER

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

OC000000035088689

Date Mailed: 03/25/2009

06/02/2009 SSITHIB1 00000001 12380773

01 FC:1011 330.00 OP
02 FC:1111 540.00 OP
03 FC:1311 220.00 OP
04 FC:1201 220.00 OP
05 FC:1202 624.00 OP
06 FC:1051 130.00 OP
07 FC:1081 1350.00 OP

VAN PELT, YI & JAMES
Van Pelt, Yi & James LLP
APR 03 2009
DOCKETED

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  *Applicant must submit $**330** to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) 1-15, 22-23, 26A, 29-41, 46, 48-55, 57, 59, 61-64.
  - Numbers, letters, and reference characters on the drawings must measure at least 0.32 cm (1/8 inch) in height. See Figure(s) 22-23, 26A-29, 23,26A-30, 33-45,.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **$844** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of **$130** for a non-small entity, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$3414** for a non-small entity
- **$330** Statutory basic filing fee.
- **$130** Surcharge.
- The application search fee has not been paid. Applicant must submit **$540** to complete the search fee.
- The application examination fee has not been paid. Applicant must submit **$220** to complete the examination fee for a non-small entity.
- The specification and drawings contain more than 100 pages. Applicant owes **$1350** for **231** pages in excess of **100** pages for a non-small entity.
- Total additional claim fee(s) for this application is **$844**
  - **$220** for **1** independent claims over 3.
  - **$624** for **12** total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/mkanno/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. 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 12/380,773	Filing Date 03/02/2009	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	06/01/2009	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 32	Minus	** 32	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

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

Legal Instrument Examiner:
/DIANE WILLIAMS/

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.

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/380,773	03/02/2009	2416	3414	RALEP018	32	4

CONFIRMATION NO. 5719

UPDATED FILING RECEIPT

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

OC00000036387246

Date Mailed: 06/16/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;

Assignment For Published Patent Application

Gregory G. Raleigh

Power of Attorney: The patent practitioners associated with Customer Number 21912

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009

Foreign Applications

If Required, Foreign Filing License Granted: 03/19/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/380,773**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No

Title

Verifiable service policy inplementation for intermediate networking devices

Preliminary Class

370

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

OIPE MPB
JUL 27 2009
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Gregory G. Raleigh	Examiner:	Not Assigned
Application No.:	12/380,773	Art Unit:	2445
Filed:	March 2, 2009	Docket No.	RALEP018
Title:	VERIFIABLE SERVICE POLICY IMPLEMENTATION FOR INTERMEDIATE NETWORKING DEVICES		

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in a prepaid envelope addressed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

July 22, 2009.

Monique Huang

REQUEST FOR A CORRECTED FILING RECEIPT

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

Sir:

Enclosed is a copy of the Official Filing Receipt we received for the above-identified patent application. Please make the following corrections and reprint an updated Filing Receipt for the above-identified patent application and forward it to the undersigned at the address set out below.

The Domestic Priority data is claimed by applicant is missing provisional application 61/207,739 filed on February 13, 2009.

If any additional fees are due in connection with this request, the Commissioner is hereby authorized to charge such fees to Deposit Account No. 50-0685 (Order No. RALEP018).

Respectfully submitted,

Dated: July 22, 2009

/Michael J. Schallop/
Michael J. Schallop
Registration No. 44,319
V 408-207-4762
F 408-973-2595

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

Attorney Docket No. RALEP018

OIPE
JUL 27 2009
PATENT & TRADEMARK OFFICE

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/380,773	03/02/2009	2416	3414	RALEP018	32	4

CONFIRMATION NO. 5719

UPDATED FILING RECEIPT

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

RECEIVED
JUN 19 2009
VAN PELT, YI & JAMES
Van Pelt
JUN 19 2009
DOCKETED

OC000000036387246

Date Mailed: 06/16/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;

Assignment For Published Patent Application

Gregory G. Raleigh

Power of Attorney: The patent practitioners associated with Customer Number 21912

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

Foreign Applications

If Required, Foreign Filing License Granted: 03/19/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/380,773**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No

Title

Verifiable service policy inplementation for intermediate networking devices

Preliminary Class

370

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

OIPE
JUL 27 2009
PATENT & TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY FOR ORIGINAL U.S. PATENT APPLICATION

Attorney's Docket No. RALEP018

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **VERIFIABLE SERVICE POLICY IMPLEMENTATION FOR INTERMEDIATE NETWORKING DEVICES**, the specification of which,

(check one)

1. ☐ is attached hereto.

2. ☒ was filed on March 2, 2009 as U.S. Application No. 12/380,773 and was amended on _____.

3. ☐ was filed on _____ as International PCT Application No. _____ and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

For Assigned Inventions: I understand that the purpose of making this appointment is to permit prosecution of patent applications for the above-identified invention for the benefit of my assignee, and that this appointment does not create an attorney-client relationship between me and these appointees.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under Title 35, United States code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s) Priority Benefits Claimed?

(Appl. No.)	(Country)	(Filing Date)	☐Yes ☐No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

Prior Provisional Application(s)

61/206,354 (Application No.)	1/28/2009 (Filing Date)
61/206,944 (Application No.)	2/4/2009 (Filing Date)

61/207,393 (Application No.)	2/10/2009 (Filing Date)
61/207,739 (Application No.)	2/13/2009 (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Application(s)

(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)

And I hereby appoint the attorneys and/or agents associated with Customer No. **21912** as my principal attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Please Direct all Correspondence To: **Customer No. 21912**
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

Direct Telephone Calls To: **Michael J. Schallop at telephone number (408) 207-4762**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Full name of sole or first inventor	Gregory G. Raleigh				
Signature of sole or first inventor				Date:	March 24, 2009
Residence: City	Woodside	State:	CA	Citizenship:	United States
Mailing Address	131 Fox Hollow Rd., Woodside, CA 94062				

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/380,773	03/02/2009	2445	3414	RALEP018	32	4

CONFIRMATION NO. 5719

CORRECTED FILING RECEIPT

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

OC000000037210931

Date Mailed: 08/07/2009

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;

Assignment For Published Patent Application

Gregory G. Raleigh

Power of Attorney: The patent practitioners associated with Customer Number 21912

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

Foreign Applications

If Required, Foreign Filing License Granted: 03/19/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/380,773**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No

Title

Verifiable service policy inplementation for intermediate networking devices

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

OPAP IAP4 FEB 16 2010 PATENT & TRADEMARK OFFICE

IPW

PTO/SB/36 (01-08)
Approved for use through 01/31/2008. 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.

RESCISSION OF PREVIOUS NONPUBLICATION REQUEST
(35 U.S.C. 122(b)(2)(B)(ii))
AND, IF APPLICABLE,
NOTICE OF FOREIGN FILING
(35 U.S.C. 122(b)(2)(B)(iii))

Send completed form to:
Mail Stop PG Pub
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
FAX: (571) 273-8300

Application Number	12/380,773
Filing Date	March 2, 2009
First Named Inventor	Greg G. Raleigh
Title	VERIFIABLE SERVICE POLICY IMPLEMENTATION FOR INTERMEDIATE NETWORKING DEVICES
Atty Docket Number	RALEP018
Art Unit	2416
Examiner	Unknown

A request that the above-identified application not be published under 35 U.S.C. 122(b) (nonpublication request) was included with the above-identified application on filing pursuant to 35 U.S.C. 122(b)(2)(B)(i).
I hereby **rescind** the previous nonpublication request.

If a notice of foreign or international filing is or will be required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c), I hereby provide such notice. This notice is being provided no later than forty-five (**45**) days after the date of such foreign or international filing.

*If a notice of subsequent foreign or international filing required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c) was not filed within forty-five (**45**) days after the date of filing of the foreign or international application, the application is ABANDONED, and a petition to revive under 37 CFR 1.137(b) is required. See 37 CFR 1.137(f).*

Michael J. Schallop — Signature
2-11-10 — Date

Michael J. Schallop — Typed or printed name
44,319 — Registration Number, if applicable

408-207-4762 — Telephone Number

This request must be signed in compliance with 37 CFR 1.33(b).

If information or assistance is needed in completing this form, please contact the Pre-Grant Publication Division at (703)605-4283 or by e-mail at PGPub@USPTO.gov.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop PG Pub, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature: Jennifer C. Gross

Name (Print/Type): Jennifer C. Gross — Date: 2/11/2010

This collection of information is required by 37 CFR 1.213(b). 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 PG Pub, 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.

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/380,773	03/02/2009	Gregory G. Raleigh	RALEP018

CONFIRMATION NO. 5719

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

NONPUBLICATION RESCISSION LETTER

OC000000040344077

Date Mailed: 03/02/2010

Communication Regarding Rescission Of Nonpublication Request and/or Notice of Foreign Filing

Applicant's rescission of the previously-filed nonpublication request and/or notice of foreign filing is acknowledged. The paper has been reflected in the Patent and Trademark Office's (USPTO's) computer records so that the earliest possible projected publication date can be assigned.

The projected publication date is 07/29/2010.

If applicant rescinded the nonpublication request before or on the date of "foreign filing,"[1] then no notice of foreign filing is required.

If applicant foreign filed the application after filing the above application and before filing the rescission, and the rescission did not also include a notice of foreign filing, then a notice of foreign filing (not merely a rescission) is required to be filed within 45 days of the date of foreign filing. See 35 U.S.C. § 122(b)(2)(B)(iii), and Clarification of the United States Patent and Trademark Office's Interpretation of the Provisions of 35 U.S.C. § 122(b)(2)(B)(ii)-(iv), 1272 Off. Gaz. Pat. Office 22 (July 1, 2003).

If a notice of foreign filing is required and is not filed within 45 days of the date of foreign filing, then the application becomes abandoned pursuant to 35 U.S.C. § 122(b)(2)(B)(iii). In this situation, applicant should either file a petition to revive or notify the Office that the application is abandoned. See 37 CFR 1.137(f). Any such petition to revive will be forwarded to the Office of Petitions for a decision. Note that the filing of the petition will not operate to stay any period of reply that may be running against the application.

Questions regarding petitions to revive should be directed to the Office of Petitions at (571) 272-3282.

[1] Note, for purpose of this notice, that "foreign filing" means "filing an application directed to the same invention in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing".

/hsarwari/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	12/380,773
				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	1	of	4	Atty Docket No.	RALEP018

U.S. Patent Documents					
Examiner Initials	CiteNo.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A.	US 2006/0048223	03-02-2006	LEE et al.	
	B.	US 6,965,667	11-15-2005	TRABANDT et al.	
	C.	US 2008/0268813	10-13-2008	Stephane H. Maes	
	D.	US 2007/0255848	11-01-2007	SEWALL et al.	
	E.	US 2008/0039102	02-14-2008	SEWALL et al.	
	F.	US 2006/0233108	10-19-2006	Murali R. Krishnan	
	G.	US 5,892,900	04-06-1999	GINTER et al.	
	H.	US 7,403,763	07-22-2008	Stephane H. Maes	
	I.	US 7,317,699	01-08-2008	GODFREY et al.	
	J.	US 7,353,533	04-1-2008	WRIGHT et al.	
	K.	US 7,322,044	01-22-2008	Scott E. Hrastar	
	L.	US 7,058,968	06-06-2006	ROWLAND et al.	
	M.	US 7,042,988	05-09-2006	JUITT et al.	
	N.	US 7,418,253	08-26-2008	Alan Kavanah	
	O.	US 7,242,920	04-10-2007	Robert P. Morris	
	P.	US 6,148,336	11-14-2000	THOMAS et al.	
	Q.	US 7,317,699	01-08-2008	GODFREY et al.	
	R.	US 7,325,037	01-29-2008	Karen L. Lawson	
	S.	US 6,141,686	10-31-2000	JACKOWSKI et al.	
	T.	US 2004/0044623	03-04-2004	WAKE et al.	
	U.	US 2006/0040642	02-23-2006	BORIS et al.	
	V.	US 2008/0229388	09-18-2008	Stephane H. Maes	
	W.	US 2008/0120688	05-22-2008	QIU et al.	
	X.	US 2003/0236745	12-25-2003	HARTSELL et al.	
	Y.	US 2008/0052387	02-28-2008	HEINZ et al.	
	Z.	US 2004/0019539	01-29-2004	RAMAN et al.	
	AA.	US 2004/0236547	11-25-2004	RAPPAPORT et al.	
	BB.	US 2002/0199001	12-26-2002	WENOCUR et al.	
	CC.	US 2004/0073672	04-15-2004	Fascenda	
	DD.	US 2006/0143098	06-29-2006	Lazaridis	
	EE.	US 6,098,878	08-08-2000	DENT et al.	
	FF.	US 2004/0198331	10-07-2004	COWARD et al.	
	GG.	US 2003/0004937	01-02-2003	SALMENKAITA et al.	
	HH.	US 2005/0107091	05-19-2005	VANNITHAMBY et al.	
	II.	US 2003/0224781	12-04-2003	MILFORD et al.	
	JJ.	US 2008/0189760	08-07-2008	ROSENBERG et al.	
	KK.	US 2005/0246282	11-03-2005	NASLUND et al.	
	LL.	US 2008/0316923	12-25-2008	FEDDERS et al.	
	MM.	US 2006/0026679	02-02-2006	Zakas	
	NN.	US 2008/0082643	04-03-2008	STORRIE et al.	

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	12/380,773
				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	2	of	4	Atty Docket No.	RALEP018

	OO.	US 2007/0140275	06-21-2007	BOWMAN et al.	
	PP.	US 2003/0182435	09-25-2003	REDLICH et al.	
	QQ.	US 6,263,055	07-17-2001	GARLAND et al.	
	RR.	US 5,940,472	08-17-1999	NEWMAN et al.	
	SS.	US 2008/0318550	12-25-2008	Deatley	
	TT.	US 2008/0298230	12-01-2008	LUFT et al.	
	UU.	US 2007/0220251	09-20-2007	ROSENBERG et al.	
	VV.	US 2007/0100981	05-03-2007	ADAMCZYK et al.	
	WW.	US 2007/0022289	01-25-2007	ALT et al.	
	XX.	US 2008/0095339	04-24-2008	ELLIOTT et al.	
	YY.	US 2006/0233166	10-19-2006	BOU-DIAB et al.	
	ZZ.	US 2008/0168523	07-10-2008	ANSARI et al.	
	AAA.	US 2006/0183462	08-17-2006	KOLEHAINEN et al.	
	BBB.	US 2006/0165060	07-27-2006	Dua	
	CCC.	US 2008/0177998	07-24-2008	APSANGI et al.	
	DDD.	US 2008/0064367	03-13-2008	NATH et al.	
	EEE.	US 2004/0168052	08-26-2004	CLISHAM et al.	
	FFF.	US 2005/0198377	09-08-2005	FERGUSON et al.	
	GGG.	US 2005/0216421	09-29-2005	BARRY et al.	
	HHH.	US 2006/0218395	09-28-2006	Maes	
	III.	US 2005/0055309	03-10-2005	WILLIAMS et al.	
	JJJ.	US 2003/0050837	03-13-2003	Kim	
	KKK.	US 2005/0266825	12-01-2005	Clayton	
	LLL.	US 2006/0178917	08-10-2006	Mikurak	
	MMM.	US 2007/0055694	03-08-2007	RUGE et al.	
	NNN.	US 2005/0097516	05-05-2005	DONNELLY et al.	
	OOO.	US 7,356,337	04-08-2008	Florence	
	PPP.	US 2007/0019670	01-25-2007	Falardeau	
	QQQ.	US 2004/0127200	07-01-2004	SHAW et al.	
	RRR.	US 2005/0166043	07-28-2005	ZHANG et al.	
	SSS.	US 7,349,695	03-25-2008	OOMMEN et al.	
	TTT.	US 2004/0098715	05-20-2004	AGHERA et al.	
	UUU.	US 2006/0072646	04-06-2006	FEHER et al.	
	VVV.	US 2006/0206904	09-14-2006	WATKINS et al.	
	WWW.	US 2005/0060266	03-17-2005	DEMELLO et al.	
	XXX.	US 6,047,268	04-04-2000	BARTOLI et al.	
	YYY.	US 6,639,975	10-28-2003	O'NEAL et al.	
	ZZZ.	US 6,539,082	03-25-2003	LOWE et al.	
	AAAA.	US 2008/0134330	06-05-2008	KAPOOR et al.	
	BBBB.	US 2004/0047358	03-11-2004	CHEN et al.	
	CCCC.	US 2007/0274327	11-29-2007	KAARELA et al.	
	DDDD.	US 2003/0161265	08-28-2003	CAO et al.	

Substitute for form 1449/PTO				Complete if Known	
				Application No.:	12/380,773
Information Disclosure Statement By Applicant				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
(Use as many sheets as necessary)				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	3	of	4	Atty Docket No.	RALEP018

	EEEE.	US 2008/0305793	12-11-2008	GALLAGHER et al.	
	FFFF.	US 2008/0083013	04-03-2008	SOLIMAN et al.	
	GGGG.	US 2004/0030705	02-12-2004	BOWMAN-AMUAH et al.	
	HHHH.	US 6,574,321	06-03-2003	COX et al.	
	IIII.	US 2006/0291477	12-28-2006	CROAK et al.	
	JJJJ.	US 2005/0266880	12-01-2005	Gupta	
	KKKK.	US 2003/0229900	12-11-2003	Reisman	
	LLLL.	US 2007/0198656	08-23-2007	MAZZAFERRI et al.	
	MMMM.	US 2003/0182420	09-25-2003	JONES et al.	
	NNNN.	US 2008/0225748	09-18-2008	KHEMANI et al.	
	OOOO.	US 2005/0250508	11-10-2005	GUO et al.	
	PPPP.	US 2008/0127304	05-29-2008	GINTER et al.	
	QQQQ.	US 7,289,489	10-30-2007	KUNG et al.	
	RRRR.	US 2003/0050070	03-13-2003	MASHINSKY et al.	
	SSSS.	US 6,996,076	02-07-2006	FORBES et al.	
	TTTT.	US 2008/0183	07-31-2008	PAUL et al.	
	UUUU.	US 2007/0226225	09-27-2007	YIU et al.	
	VVVV.	US 2007/0130315	06-07-2007	FRIEND et al.	
	WWWW.	US 2008/0059743	03-06-2008	BYCHKOV et al.	
	XXXX.	US 2008/0132268	06-05-2008	CHOI-GROGAN et al.	
	YYYY.	US 2003/0133408	07-17-2003	CHENG et al.	
	ZZZZ.	US 2005/0128967	06-16-2005	Scobbie	
	AAAAA.	US 2007/0140113	06-21-2007	Gemelos	
	BBBBB.	US 2002/0138601	09-26-2002	PIPONIUS et al.	
	CCCCC.	US 2002/0176377	11-28-2002	Hamilton	
	DDDDD.	US 2006/0034256	02-16-2006	ADDAGATLA et al.	
	EEEEE.	US 2005/0228985	10-13-2005	YLIKOSKI et al.	
	FFFFF.	US 2007/0036312	02-15-2007	CAI et al.	
	GGGGG.	US 2004/0082346	04-29-2004	SKYTT et al.	
	HHHHH.	US 7,142,876	11-28-2006	TROSSEN et al.	
	IIIII.	US 2008/0005561	01-03-2008	BROWN et al.	
	JJJJJ.	US 2007/0101426	05-03-2007	LEE et al.	
	KKKKK.	US 2008/0222692	09-11-2008	ANDERSSON et al.	
	LLLLL.	US 2008/0160958	04-03-2008	ABICHANDANI et al.	
	MMMMM	US 2006/0048223	03-02-2006	LEE et al.	
	NNNNN.	US 2007/0104126	5-10-2007	CALHOUN et al.	
	OOOOO.	US 2007/0243862	10-18-2007	COSKUN et al.	
	PPPPP.	US 2008/0109679	05-08-2008	WRIGHT et al.	
	QQQQQ.	US 2006/0242685	10-26-2006	HEARD et al.	
	RRRRR.	US 2008/0130656	06-05-2008	KIM et al.	
	SSSSS.	US 2005/0021995	01-27-2005	LAL et al.	
	TTTTT.	US 2008/0162704	04-03-2008	POPLETT et al.	

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	12/380,773
				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	4	of	4	Atty Docket No.	RALEP018

	UUUUU.	US 2008/0229385	09-18-2008	FEDER et al.	
	VVVVV.	US 2008/0098062	04-24-2008	Balia	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code–Number–Kind Code *(known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1A	WO 2006/130960	12-14-2006	Mobidia, Inc.	
	1B	EP 1772988A1	04-11-2007	Huawei Technologies, Co., LTD.	
	1C	EP 1978772A1	10-08-2008	British Telecommunications	
	1D	WO 2007/053848	05-10-2007	Mobile Armor, LLC	
	1E	WO 2006/073837	07-13-2006	Symbol Technologies, Inc.	
	1F	WO 2004/028070	04-01-2004	Credant Technologies, Inc.	
	1G	WO 2004/095753	11-04-2004	Motorola Inc.	
	1H	WO 2003/014891	02-20-2003	The Boeing Company	
	1I	WO 2007/107701	09-27-2007	British Telecommunications	
	1J	EP 1463238	09-29-2004	Alcatel	
	1K	WO 2008/080430	07-10-2008	Telecom Italia S.P.A	
	1L	WO 2008/017837	02-14-2008	Symbian Software	
	1M	WO 2008/099802	08-21-2008	NEC Corporation	
	1N	WO 2007/001833	01-04-2007	Symbol Technologies	
	1O	EP 1739518	06-29-2005	Research In Motion	
	1P	WO 2007/069245	06-21-2007	Yoggie Security	
	1Q	WO 2008/066419	06-05-2008	Telefonaktiebolaget LM Ericsson	
	1R	WO 2006/050758	05-18-2006	Telefonaktiebolaget LM Ericsson	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T^2 = Applicant is to place a check mark here if English language Translation is attached

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
14 December 2006 (14.12.2006)

(10) International Publication Number
WO 2006/130960 A1

(51) International Patent Classification:
H04L 29/02 (2006.01) *H04Q 7/20* (2006.01)
H04L 29/04 (2006.01)

(21) International Application Number:
PCT/CA2006/000901

(22) International Filing Date: 6 June 2006 (06.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/687,339 6 June 2005 (06.06.2005) US

(71) Applicant *(for all designated States except US)*: **MOBIDIA, INC.** [CA/CA]; 10451 Shellbridge Way, Suite 230, Richmond, British Columbia V6X 2W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SHARIF-AHMADI, Dr. Seyed M.** [US/CA]; #313 - 5880 Dover Cres., Richmond, British Columbia V7C 5P5 (CA). **ARJOMANDI, Fay** [CA/CA]; #312 - 5500 Cooney Rd., Richmond, British Columbia V6X 3E5 (CA).

(74) Agent: **INGALLS, Doran**; c/o Fasken Martineau DuMoulin LLP, 2100 - 1075 West Georgia Street, Vancouver, British Columbia V6E 3G2 (CA).

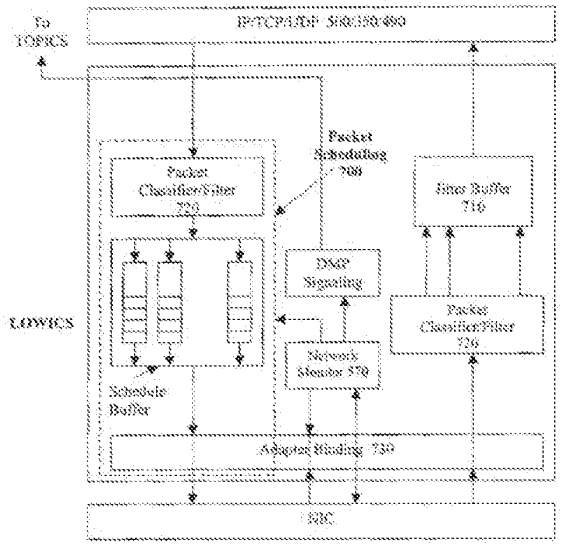
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, 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, 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*

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 AND METHOD OF CONTROLLING A MOBILE DEVICE USING A NETWORK POLICY



(57) Abstract: A method of controlling a mobile device based on a network policy, wherein the network policy is stored on the mobile device when a server or access point is accessed. When a packet is transmitted, it is sent only if it meets the policy parameters as established by the network policy. Parameters may include the type of service or packet, the time of day of the usage, or the maximum tolerable delay permitted.

WO 2006/130960 A1

SYSTEM AND METHOD OF CONTROLLING A MOBILE DEVICE USING A NETWORK POLICY

This application claims the benefit of U.S. provisional application no. 60/687,339, filed on June 6, 2005.

FIELD OF THE INVENTION

This invention relates to systems and methods of managing data traffic over networks, and more particularly to systems and methods for addressing the diverse requirements of different data types and their behaviour over different types of wired and wireless networks, each such network having different characteristics and changing network status.

BACKGROUND OF THE INVENTION

Wireless networks generally have very different properties when compared to traditional wired networks. For example, the "backbone" of a wired network is more homogeneous than a wireless network, and a wired network is typically, a mesh of intelligent sub networks connected through routers and switches that control data traffic. In wired networks, users are generally stationary and therefore movement of users has little impact on network service. The key influence on user service in a wired network is the data traffic congestion on the network. This congestion problem is dealt with by using the Transmission Control Protocol/Internet Protocol (TCP/IP), a communications protocol that most network applications use.

Wireless network characteristics and implementations are quite different from wired networks, for example, in the following ways:

1. The network infrastructure of a wireless network is simpler, with respect to the number of nodes between a mobile networked device and a first wired link in the network.

2. The status of a wireless network changes frequently, due to several factors, including: environmental conditions (e.g. downtown urban area vs. suburban area with different signal

attenuation and propagation); mobile device location (e.g. close to a large power supply field vs. in a large open area); network traffic at a given time, adjacent user usage of the network; and the base station backbone (e.g. fiber vs. copper backbone).

3. Software applications are generally not designed for wireless network environments that include frequent status variation. Therefore, operating such applications over a wireless network may worsen the network status by adding additional traffic, and thereby increasing the overall delay and latency of the network, which, in turn, may impact the experiences of other mobile device users.

Two parallel changes occurring in wireless network technologies are: i) the introduction of new wireless network types, so that the overall wireless network infrastructure is changing from being a single type network, for example a General Packet Radio Service (GPRS) network only, to an infrastructure comprising multiple network types, such as GPRS, Wi-Fi, Worldwide Interoperability for Microwave Access (WiMAX) and Universal Mobile Telecommunications System (UMTS); and, ii) wireless network users are no longer only using "background class" type of applications such as email, short message services (SMS) and downloads, but are now using more interactive applications such as web browsing, network gaming, and database access; streaming applications such as multimedia applications, video on demand, and webcasting; and conversational applications such as Voice over Internet Protocol (VoIP), video telephony, and video gaming. Service providers, or carriers, are driving to increase the usage of these applications over wireless networks as to increase "average revenue per user" and subscription rates. The service providers also differentiate themselves from competitors through the services offered along with Quality of Service (QoS) for their own "certified" applications as compared to third party applications. However, use of these different types of applications results in different data traffic types traversing the network, each data type having different delivery (time) requirements and different error tolerances (in time sensitive vs. error sensitive spectrums of applications). For example, a VoIP packet is very time sensitive and has a short time to live, whereas a data packet is very error sensitive. TCP and UDP/IP protocols (widely used by many software applications) are both network and application agnostic. TCP does provide congestion control features which occur on wired networks but the protocol doesn't distinguish a wired network from a wireless network. Also

neither of these protocols are application aware (they are not sensitive to the type of applications and time vs. error sensitivity). TCP/IP has been designed specifically to overcome the congestion problems in wired networks by detecting the congestion on the network and controlling the traffic between the two communicating parties. However, use of TCP/IP over wireless networks may be problematic. For example, delays in the wireless network may be caused by signal attenuation (not by congestion), causing TCP/IP to actually reduce performance of a wireless network.

Therefore, what is lacking in the prior art is the awareness and involvement of the networked (for example, mobile) device in the network by enabling the networked device to act as an intelligent and integrated element (similar to a router/switch) within the network. In the prior art, the networked device, particularly mobile devices, lack the ability to make decisions based on the types of wired or wireless network(s) available to it and the types of data it is communicating to other networked devices (given the differences between wireless and wired networks, data communications should be treated differently over the two network types).

The prior art fails to address the following problems:

1. TCP/IP inefficiency over wireless networks;

2. the lack of knowledge of wireless networks within the protocol layer of networked devices;

3. VoIP and the standard streaming video control protocol, known as the Real-Time Transport Control Protocol (RTCP) inefficiency over wireless networks;

4. the inability to dynamically distinguish between the different types of data and meet their real-time requirements in a mixed network, without relying on IP header information;

5. the inability of a mobile device in a mixed network to be aware of the types of the available networks and the status of each network at any given time and to feedback status information to the network as part of the data protocol delivery without requiring any extra transaction;

6. the inability of a mobile device in a mixed network to predict the signal to noise ratio (SNR), outside the physical layer and below the IP layer, of the wireless network and to make decisions for appropriate traffic types, such as forwarding/redirecting traffic through different networks, or using two types of networks simultaneously based on their conditions and network policy;

7. the inability to provide local jitter handling within a mobile device in the layer below IP; and

8. the inability to provide mobile data traffic prioritization, queuing and scheduling within a mobile device, based on the network condition and policy, or through either DNA/fingerprints set by a catalogue ID or determining the application type.

There have been attempts to solve one of the issues listed above, specifically TCP/IP inefficiency over wireless networks. These solutions include using TCP/IP spoofing and tunnelling techniques that are inefficient and often cause yet more unnecessary data to be sent over the wireless networks, and produce extra processing overhead for the network device.

TCP/IP is a protocol designed for wired networks and is well suited for problems in that environment, which are usually congestion related. If a node in a network using TCP/IP does not receive an acknowledgment, the node concludes there is congestion in the network and tries to help the network by slowing down transmissions and providing flow control. In a wireless network, the failure to receive an acknowledgment within a given time is usually not due to congestion but due to instant network delays, signal strength drop, or latency variation. In such situations a TCP/IP node will slow down the transmission and take some time before returning to its normal speed of operation. During this time the throughput over the same bandwidth will be reduced because of the unnecessarily slowed transmission.

Another problem caused by TCP/IP is that it was designed for the low bit error rate link environment of a wired network and therefore if one packet within a stream of packets is lost then

all packets are resent. For example, if a single packet is lost within a 20 packet stream the network node will resend all packets in the stream, even if most were successfully received.

Some application level protocols such as HyperText Transfer Protocol (HTTP) use TCP/IP in a manner that is not wireless network friendly. For example, when a HTTP browser, such as Microsoft Explorer, makes a communications request, the HTTP browser performs two or three simultaneous TCP/IP calls. Each TCP/IP call requires three-way handshaking (three requests and responses) to establish the link. Over wireless links (that normally have a higher latency than wired links), if a response does not arrive on time this will be interpreted as a need for a new TCP/IP request. If one TCP/IP link is delayed the browser will request another TCP/IP link with another three-way handshake. All of these communications create extra overhead and add delay to a wireless network.

To solve these problems there have been several inefficient solutions, which focus on a single type of data, using applications such as Internet Explorer. Following are the approaches taken to overcome TCP/IP inefficiency over the wireless networks:

1. Compression of data (content) which reduces the amount of data going over the network;

2. Domain Name System ("DNS") caching within a mobile device; and

3. User Datagram ("UDP") tunnelling of compressed TCP/IP packets, and TCP/IP spoofing.

To date, none of these approaches have been entirely adequate. The shortcomings of each of these approaches are as follows:

1. Content compression

Content compression is typically applied only to "background" applications and to some interactive applications, such as Internet Explorer requesting a website which includes both text and picture

objects. This method compresses content based on the classification of the data as lossy or lossless, e.g. Joint Photographic Expert Group ("JPEG") and text ("txt") file formats. These classifications allow for compression in different ways and ratios. Although this method reduces the amount of data travelling over the network, which indirectly results in greater use of bandwidth, it does not eliminate TCP/IP inefficiencies over wireless networks, as it is the wireless delay variations that cause the strange behaviour of TCP/IP.

2. DNS caching within a mobile device

DNS caching within a mobile device is used to reduce the time required for DNS searches. This technique requires software within the mobile device to cache the results from the DNS for each DNS query. The next time the same query is requested the DNS cache is used to provide the result instead of transmitting the request over the network and waiting for the response. This technique reduces the need for transferring frequently requested queries but it does not address TCP/IP inefficiency directly.

3. Tunnelling

Tunnelling includes UDP tunnelling of either compressed or uncompressed TCP/IP data. Tunnelling requires software within both the mobile device and the server communicating to capture the TCP/IP data and tunnel the entire TCP packet through UDP. The disadvantages of this technique include:

(i) Process consumption. As TCP data has already been created and passed to a lower layer, the network node should pass the data back to a higher layer, user-mode, proxy type application, which sends the TCP packet back to the protocol layer, in kernel-mode, but requests a UDP packet this time (called a UDP tunnel). If the network node is using IP Security (IPSec) Virtual Private Network (VPN) encryption security the tunnelled TCP data will go through yet another IPSec tunnel. This means that more processing time will be required for a small mobile device and further delays will be caused by the tunnelling technique. Also, if the compression or

encryption happened in the layer 4 (above TCP and UDP layers and below the application layer) then the proxy-type may not be able to distinguish the type of application.

(ii) Increased network traffic. Tunnelling within tunnelling (as described above) increases traffic over the network. This "solution" does not solve the TCP inefficiency issues created by the wireless network's latency variation, as TCP data has already been created but is wrapped around a different protocol for transmission. The main reason to tunnel TCP data is to compress the data, so therefore the data is wrapped around another protocol for transmission. However, if the network has high latency, TCP would still result in strange behaviour due to lack of receiving responses in a timely fashion.

In order to overcome TCP problems over wireless and mixed networks some solutions involve transferring extra packets, such as ping or extra acknowledgments to maintain proper TCP behaviour over the wireless link and to keep the link "alive" for the software application. This approach also increases the traffic over the wireless network by adding unnecessary data and also changes the mechanism of new packet switched networks to that of the old legacy circuit switch networks. The philosophy of a packet switched network is to allocate the link to a mobile user only when there is data available to transmit. During the time the user is waiting for a response the uplink will be allocated to another mobile user. This results in higher network capacity and enables use of the existing network for larger numbers of network users. Circuit switched networks have the link allocated to the mobile device user for a certain period of the time, whether or not the mobile user has any data available to transmit. During this time other mobile device users wait for the link to be de-allocated from that mobile device user and re-allocated to them by the network. This results in a lower network capacity and inefficient use of the network.

Roaming

Roaming is the process of moving from one access point ("AP") to another over a wireless link, for example, a mobile device user moving in an airport. For connection-oriented applications (for example, those that are TCP/IP based) the latency to transfer the communications and connection from one AP to another could result in the retransmission of data and reestablishment of TCP after

receiving a new IP from a new domain (in case of an intra domain move). For time-sensitive applications, this results in additional delay caused by the movement from one AP or domain to another.

There are two current preferred methods of dealing with this issue:

1. Pre-emptive AP discovery, in which the mobile device scans the networks available, to check for the strengths of available APs, before a decision to roam is made; and roam-time AP discovery, in which the mobile device makes a decision to roam and then scans the area to find an alternative AP. This method is vendor specific and is not based on any particular standard.

2. The client may initiate roam, which is well defined in various standards and thereby the client resumes the application session.

A problem in the art is in resuming an application session and this has not been specified in any standard. It has been suggested that the Mobile IP standard within a network could solve the problem, but the amount of signalling traffic within Mobile IP creates too much unnecessary traffic.

BRIEF SUMMARY OF THE INVENTION

The system and method according to the invention comprises a software platform that provides mixed mobile data traffic management over wired, wireless, or mixed networks. The system and method addresses the diverse requirements of different data types and their behaviour over different wireless networks, each network having different characteristics and changing network status. A mobile device is incorporated as part of the overall network instead of treated as an independent entity outside the network. In the prior art, the mobile node (i.e. the mobile device) is an independent entity, disjoint from the network, blind to the types of network(s) available, and blind to the different types of data it is communicating with other networked devices. The present invention provides a comprehensive software solution that incorporates the mobile node as part of

the network, enabling it to be an active participant within the network, and enabling it to manage and negotiate specific data needs with the network components.

The system and method according to the invention makes the mobile device aware of the network situation and application types and therefore their requirements; and also is aware of network policies at any given time, and therefore can make efficient decisions. The necessary "intelligence" is available so that there is no need to alter "any" application, the mobile device's Operating System (OS) code structure, or hardware. The solution is such that the network works with or without the system according to the invention (but the network is more efficient with such system) and other mobile devices not using the system can operate within the network. This is accomplished by adding the capability to the mobile device's OS to intercept system calls and alter the calls without initiator and destination involvement.

To implement these capability two layers are inserted within the mobile device's kernel OS to intercept the application path. A first layer receives the application calls, identifies the types of application and data; builds a protocol; and redirects to the UDP (if it was for TCP). The second layer controls the physical layer, so that the second layer monitors the status of the networks, predicts the status of the networks in the near future, schedules the outgoing traffic types based on this information, provides local jitter handling for received packets for conversational class of applications, and provides the collected status to the other layers. The second layer also provides packet redirection and forwarding between the multiple types of networks available.

Thereby, the system according to the invention:

i) delivers greater bandwidth efficiency and network capacity by managing all data types over single and mixed networks by taking a protocol approach, thereby reducing the overhead created by extra connections established by applications in the wireless network (only one connection is required) and reducing the overhead of data being transmitted by reducing the required acknowledgements, sending only non-expired data and filtering out others, and not using inefficient TCP/IP spoofing and tunnelling techniques;

ii) increases overall quality of service by using an efficient protocol designed specifically for wireless networks and able to work with all data types (not just "background" data types). By tying

directly into the TCP/IP command structure in the upper layer on a mobile device (or other networked device) a protocol is created; and by providing efficient prioritization, queuing, and scheduling of different data types a superior experience for applications such as VoIP, interactive gaming and streaming video is provided, along with email and corporate applications; and

iii) provides better network reporting and an integration strategy for carriers supporting multiple networks (mixed networks). As there is a client component within the system, a carrier can now observe their network end-to-end, treating the mobile device like a network element, enabling the carrier to support stronger Service Level Agreements (SLAs) and service quality assurance. Furthermore, the information about network and application status and performance is included as part of the same protocol which delivers the data and therefore obviates the need for extra transactions or scheduled tests to determine the status and performance of the network. Also, the carrier can observe what is on the client's device, including software and mobile device configurations, thereby allowing the carrier to address service issues in a timely fashion, reducing both costs and customer frustration. As the network information is transmitted to a server component, as part of the data protocol delivery, the carrier can receive extensive reports on network status, bringing full visibility of the network to the carrier. The lower layer component of the system, according to the invention, on the mobile device enables seamless switching or simultaneous use of multiple network technologies (e.g. between cellular 2.5G/3G/4G, Wi-Fi and WiMAX) which could be based on usage policy, application type, and/or network policy. This allows the carrier to provide their customers multiple network choices, using the choice that best satisfies their user's requirements without having to concern themselves on how to use the networks, or when to switch to the networks without interrupting the user or the application. This also provides greater network efficiency for the carrier by allowing the carriers to use faster networks for backhaul transport, e.g. Wi-Fi for music downloads, and the more expensive cellular networks for email and other data applications.

A method of controlling a mobile device based on a network policy, is provided, comprising the steps of: storing said policy on a database on an advance server; sending said policy to said mobile device when said mobile requests registration with said server; when an application on said mobile device attempts to access a network via said server, checking said policy; and providing access to said network for said application when said policy permits.

If said policy changes at the database, said changed policy is pushed to said mobile device. Preferably, the network policy includes a plurality of parameters, including parameters base on the type of service provided by said application, the maximum tolerable delay and the time of usage of said application.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram, showing a mixed network;

Figure 2 is a block diagram, showing a vertical view of a mixed wireless network;

Figure 3 is a schematic diagram of a mobile device, according to the invention;

Figure 4 is a block diagram, showing a client layer overview in a system according to the invention;

Figure 5 is a block diagram thereof, showing the client position with respect to other protocols;

Figure 6 is a flow diagram thereof, showing the management of incoming traffic to the application;

Figure 7 is a schematic diagram thereof, showing the lower client architecture;

Figure 8 is a schematic diagram thereof, showing the scheduler;

Figure 9 is a schematic diagram thereof, showing the SNR teller;

Figure 10 is a flow chart thereof, showing the pre-registration and discovery process; and

Figures 11 is a table showing the DMP signalling structure;

Figure 12 is a table showing a preferred embodiment of a DMP session; and

Figure 13 is a tree showing the structure of a DMP packet.

DETAILED DESCRIPTION OF THE INVENTION

Definitions

In this document, the following terms will have the following meanings:

"advance server" means a server in communication with ICS, through which ICS accesses the network;

"far-host" means a destination networked device, such as a mobile device, a server, or a software application, in communication with a network which is the destination of a transmission;

"mixed network" means network using different communication protocols for different network nodes and network devices, and may include mobile devices, and may employ more than one type of wireless protocol for communication;

"network device" means a device capable of communicating with other network devices that forms part of a wired, wireless, or mixed network; and

"wireless device" or "mobile device" means a device for communicating with wired or wireless devices over a wireless or mixed network.

The system according to the invention is designed for use with mixed networks, examples of which are seen in Figures 1 and 2. While the illustrative example of the system and method according to the invention are described in terms of mixed networks, the invention could be used in a network in which only a single communication protocol is used.

Figure 1 displays a representative mixed network environment 1, in which several networks communicate with each other, the Internet 10 and mobile devices 30. Elements of mixed network environment 1 include: mobile switching center (MSC) 40, base transceiver station (BTS) 50, base controller station (BCS) 60, network node 70, radio network controller (RNC) 80, public switch telephone network (PSTN) 90, Short Message Service - Global System for Mobile Communications center (SMS-GSMC) 100, Home Location Register/Authentication center (HLR/AuC) 110, Signaling System #7 (SS7) network 120, Equipment Identity Register (EIR) 155 using Mobile Application Part-Proxy (MAP-P), General Packet Radio Service (GPRS) network 130, Gateway

GPRS Support Node 140, Breakout Gateway (BG) 145, Gateway GPRS Support Node (GGSN) 150, public land mobile network (PLMN) 160, and a inter-PLMN backbone network 170.

Mixed network environment 1 may have a wide variety of components and communication protocols used within. Figure 1 shows a typical, but not representative network.

Figure 2 displays an alternative viewpoint of a mixed wireless network environment 1 from a vertical view. Satellite network 200 provides the broadest coverage, and within satellite network 200 is wireless wide area network 210, in this case a GSM/3G network 220. Within wireless wide area network 210 is a wireless metropolitan area network 230, in this case a WiMAX network 240. Wireless local area networks 250 are within wireless metropolitan network 260, in this case WiFi network access points 270. Finally, within the wireless local area networks are wireless personal area networks 280 comprised of a plurality of network devices 30 using protocols to communicate such as Bluetooth and ultra wideband (UWB).

Figures 3 and 4 show schematics of a mobile device 30 incorporating the system according to the invention. Figure 3 displays an overview of such a mobile device 30, and Figure 4 displays the details of the kernal layer 300 and the relationship between the intelligent client system according to the invention and the operating system (OS) of the mobile device.

The traffic management system is stored on the mobile device as a series of drivers interfacing with standard OS libraries and function calls, as seen in Figures 3 and 4. The traffic management system is an intelligent client system ("ICS") 310, which is comprised of three main components:

1. an upper layer, TOPICS 320;
2. a Dynamic Multimedia Protocol ("DMP") 330 used as a transport layer protocol; and
3. a lower layer, LOWICS 340.

The client ICS 310 is at the same level as TCP 350 but extends to the data link layer (miniport drivers 315), as shown in Figure 5. Figure 5 illustrates the relationship between LOWICS 310 and the other protocols in the OS. LOWICS 310 resides as a protocol within the OS, but no other

application or layers except for TOPICS 320 call LOWICS 310 yet LOWICS 310 intercepts the calls that arrive for other protocols e.g. TCP/IP 350. The protocols are related to each other in a chain format with respect to their hierarchy within the OS. Each protocol points to its next protocol in the chain and binds itself to the available network drivers, referred to as miniport drivers 315. LOWICS 310 therefore is loaded after all other protocols have been loaded and then points to the first protocol entry in chain, TCP/IP 350, and registers and binds to the available network drivers, miniport driver 315. In this fashion LOWICS 310 is capable of intercepting any packet leaving the IP layer to the MAC layer and therefore applies policy and scheduling to the packet in LOWICS layer 310.

Other components of mobile device 30, as seen in Figure 3, include libraries 370, system call interface 380, TCP/IP.sys file 390, file subsystem 400, buffer cache 410, device drivers 420, character 430, block 440, hardware control 450, and hardware/NIC 460 at hardware level 470. The kernal level 300 also includes process control subsystem 510, which includes scheduler 700, memory manager 530 and inter-process communicator 540.

TOPICS Layer 320

The TOPICS layer 320's main responsibility is to interface with calls from applications 360. TOPICS 320 maintains all application (requester) information, including socket information, device and file object information, and their interface including expected maximum transmission unit (MTU), buffer size, receive interface, expected receive message format, timeout, etc. TOPICS layer 320 maintains records regarding the application 360's predicted behaviour. As seen in Figure 4, other components of mobile device 30's OS include: Network Driver Interface Specification (NDIS) interface 480, UDP interface 490, IP interface 500, and ARP interface 510. Transport driver interface 550 is between TOPICS 320 and applications 360.

TOPICS layer 320 also communicates with lower layer, LOWICS 340, to inform LOWICS 340 of the types of outgoing traffic, referred to herein as "Pre-Channel Transmission". LOWICS layer 320 then passes the requester's message to DMP 330. TOPICS 320 includes TOPICS-DMP assembly

worker (not shown), for assembling packets; and TOPICS interface for communicating with applications 360.

Outgoing Traffic

The following is the transaction sequence for outgoing packets sent by an application 360 by the mobile device 30 through ICS 310 to a far-host:

1. The application 360's protocol is identified by TOPICS 320; by using the application name, the communication port, and/or scanning the header information of the first two user application buffers which requested the connection. The extracted information is verified by TOPICS 320 by comparing the extracted information against the application ID and/or signature and/or application catalogue ID, stored on the device. TOPICS also examines and determines the type of the transport layer protocol that application 360 has requested;

2. A response to the requester (application 360) is sent by TOPICS 320 to the application 360 for the related task, depending on whether the request (e.g. a request for creating a TCP socket and/or connecting to certain host), was successful or failed;

3. TOPICS 320 then creates and maintains an application book-keeping data structure about the application 360 and socket information, which is used for forwarding the response from the far-host to appropriate application 360;

4. LOWICS 340 is notified by TOPICS 320 of the appropriate outgoing traffic type;

5. TOPICS then passes the application 360 data to the DMP sub-module to build the corresponding DMP request protocol, based on the type of application, and the DMP packet is built (as described below);

6. The DMP packet is passed to UDP 190 and then to IP 500 layer;

7. LOWICS 340 receives the IP/UDP/DMP packet from IP 500 layer; and

8. The IP/UDP/DMP packet is scheduled and passed to the appropriate network interface card (NIC) 460, to be transmitted to far-host through an advance server.

Incoming Traffic

The process by which ICS 310 receives packets for mobile device 30 is shown in Figure 6, and is as follows:

1. a DMP packet is received by a NIC 460;

2. LOWICS 340 separates the IP header from the DMP packet;

3. the type of DMP is identified through the DMP header and by LOWICS 340 receiver module to determine if local jitter handling is needed;

4. if the DMP contains data of any type other than real-time, the DMP packet is passed through a direct call to TOPICS DMP assembly worker (not shown), which is a component within the DMP module, (so the packet does not need to go through the IP layer 500);

5. the TOPICS-DMP assembly worker module assembles the packet to build a message, and when the message is complete it is passed to the TOPICS-Interface 530;

6. the TOPICS-Interface 530 determines, through its application book-keeping data structure, the appropriate application 360 which should be the message recipient; and

7. the TOPICS-Interface passes the message to the application 360 through a standard OS call.

DMP (Dynamic Multimedia Protocol):

DMP 330 is a protocol capable of carrying any type of data. DMP 330 dynamically adapts itself as necessary, for example for varying acknowledgment requirements and best packet sizes. DMP 330 shares some of the characteristics of UDP and also some of the characteristics of TCP, however, DMP carries any type of data while meeting each data type's requirements over any type of wireless link through its dynamic header bits, as shown in Figures 11, 12 and 13. DMP 330 uses UDP/IP layer 500 as the transport and network layer protocol. DMP 330 preferably works with both IPv4 and IPv6, and provides the standard interface for applications and a standard interface to UDP/IP layer 500. Figure 13 illustrates the branching of DMP. As shown in Figure 13 there are three levels in DMP that are distinguished by header bits.

1. DMP Layer 1: contains "DMP Internals" and "DMP Communication" (DMP COM). DMP Internals: Used for internal communications among components within single sub-system, e.g. communications between TOPICS 320 and LOWICS 340.

2. DMP Layer 2 is a branch off DMP COM and it carries three types of messages, Signalling, Control and Session. DMP Signalling: Used for communication between two sub-systems, namely:

    a. DMP Control:

        Activities between LOWICS←→software in an AP, and software in an AP←→server for control proposes. For example, the server notifies ICS to change its packet size, or ICS provides the server with network status information or logs. Also DMP Control is used for sending control message to ICS to control the functionality of ICS.

3. DMP Layer 3, is a branch off DMP Signalling and DMP Session (each branch to two)

    a. DMPComSignaling Request: Carries a signalling request such as Registration, Re-Registration, Un-Register and acknowledgments between TOPICS 320 ←→Advance Server

b. DMPComSignaling Response: Carries a response to the requested signal

c. DMPComSession Message: Carries the actual application data

d. DMPComSession Control: Carries application connection requests, such as socket connect, and/or control feedback information such as RTCP

Figures 11 and 12 illustrate details of and embodiment of a DMP structure for both DMP Signalling and DMP Session according to the three layer structure, described above. Other embodiments of a DMP protocol may be used, including a subset of the features described herein and in the Figures.

LOWICS Layer:

The LOWICS layer 340 includes four main sub-modules, each discussed below. The LOWICS layer 340 resides in the OS of mobile device 30 in three different formats as a layer, hooking (a method of inserting a layer into the operating system) and as a protocol. Figure 7 illustrates the overview of LOWICS 340 with respect to the OS and its internal components. As shown in Figure 7, the modules include:

1. Scheduler system 700;

2. Network Monitor 570;

   (a) Neighbourhood Discovery;

   (b) Signal to Noise Ratio Teller;

   (c) Packet forwarding;

3. Local Jitter Buffer 710; and

4. Packet Classifier 720.

LOWICS – Scheduler:

The system according to the invention has the capability of distinguishing between different types of data received or sent by mobile device 30 (or other networked device) and can identify a mobile traffic model for such data. Each different data type has its own requirements, including end-to-end transmission control, and latency sensitive real-time requirements. An objective of the system according to the invention is to meet as many requirements as possible for these different data types. Therefore, the system differentiates the data and handles the packets with the objectives of: controlling traffic over the wireless link, maintaining loads, increasing the capacity of the network, and providing bandwidth improvements.

In order to identify the data type requirements three parameters are identified and considered:

i) The maximum error rate: interpreted as the acceptable value used to identify the type of error detection for the physical channel as well as transport layer protocol.

ii) The minimum throughput: interpreted as the priority of delivery, as different types of packets have different time requirements for delivery. For some types of data (voice, streaming video, etc.), transmission of the packet after time expiration simply becomes part of network overhead, so data of such types that have expired with respect to time are not delivered.

iii) The maximum delay: interpreted as the maximum number of retransmission attempts for that data type and the time between retransmission attempts.

To manage the diverse traffic types, the system calculates a "life time". This life time is the period of time in which a decision is made for all packets of a particular application. For example, a group of packets could belong to a message application. A "session" is a life time in which the packets belong to and exist in that life time of a single application. A life time can be a deterministic type or a random distribution inter-arrival type. Different classes of services, namely background, interactive, streaming and conversational are used to narrow the traffic classes to categories of:

Voice, Video, Audio and Data, so that the characteristics and requirements of each data type can be outlined and a mobile traffic model identified as in following Tables 1 and 2.

Traffic Type	Latency	Error	Inter-Arrival Generation Rate	Packet Size	Traffic Model	Equation
Voice	Highly Sensitive	Low Sensitivity	Fix	Fix	Pareto Distribution	$F(p) = 1 - (\frac{S}{p})^{\alpha}, p \geq S$
Data	Low Sensitivity	Highly Sensitivity	Highly Variable	Highly Variable	Exponential Distribution	$F(t) = 1 - e^{-\frac{t}{T}}, t \geq 0$
Video	Highly Sensitive	Low Sensitivity	Fix	Highly Variable (depending on codec)		
Audio	Highly Sensitive	Low Sensitivity	Fix	Highly Variable (depending on codec)		

Table -- 1: Traffic type and sensitivity

F(P): Pareto distribution Function, S: minimum packet size, P: Packet Size
F(T): Random distribution Function, t: time, T: expected value of the inter-arrival time t

As an example, Voice over IP (VoIP) is highly sensitive to the latency while it is not sensitive to error, as a user can always ask for the other party to repeat. However, the data's rate of arrival to TOPICS 320 is fixed and its packet size is fixed. Looking at the traffic that VoIP generates, it follows the model of Pareto Distribution. Data, however, such as Internet Explorer typically communicates, is very low sensitive for latency while highly sensitive to error, e.g. receiving corrupted banking information. The arrival rate of the packets (or its generation rate) for Data is variable and unpredictable, as it is generated and arrives in bursts, and the traffic type that it generates follows the exponential distribution. This information of the type of traffic model allows scheduler system 700 to make scheduling decisions based on the type of traffic model expected and whether the available networks have the capability of delivering the traffic or not. For example, in a mixed network, where the mobile user is on 2.5Generation network, such as GPRS, using VoIP application is not appropriate since this type of network doesn't have the capability of delivering the type of traffic.

Service Class	Priority	Bit Error Rate (BER)	#of Transmission	Value of T, S and α
Voice	6	10^{-3}	3	T = 0.001 s S = 256 bits
Data	2	10^{-7}	8	T = 0.01 s S= 8000 bits, α = 1.03
Media (Video/Audio)	4	10^{-5}	3	T = 0.005 s S= 1280 bits, α = 1.03

Table – 2: Service Class description

As illustrated in table 2 and based on table 1; the type of traffic is classified with respect to their priority in which they have to be serviced, delivered and transferred to the network, and tolerated Bit Error Rate (BER) such that if the error in packet was less than the BER, then there is no need to request for retransmitting the data and also determine how many times the data can be retransmitted before the data expires (based on its time to live). For example a VoIP packet can be retransmitted (if un-arrived) three times using fast retransmission before the packet's time to live expires, which is 250 milliseconds end-to-end (as set in VoIP standards). Using this method the values of T (the expected value of inter-arrival time t), S (the minimum packet size), and α (a constant value) can be inserted into either the Pareto or Exponential Distribution function shown in Table 1 for scheduler system 700 to make a decision for packet scheduling.

The different classes of service, include the Interactive class of service, which refers to the type of application/traffic which is a request/response oriented and it requires users interaction. An example of this application is Internet Explorer where the request sent and a response received. The Background class of service, refers to the type of applications that it runs in background and does a burst type of transaction. Email is an example of this type of application, as there is no need for the user interaction the email runs in the background and receives the information. A Streaming class of service, refers to the type of application where there is a request for receiving a media, not

necessary in real-time, similar to video or audio. Real-time class of service, also referred to as conversational, are the class of services that are very time-sensitive. They typically have a fixed time to live set by industry. As an example a voice over IP packet has only a 250 millisecond acceptable delay, if it received after that the packet will not be processed by the receiver. Examples of this type of application/service are Voice Over IP (VOIP), and video telephony.

Scheduler system 700 completes three main tasks, namely: queue managing; scheduling; and the channel SNR teller.

As seen in Figure 8, queue manager 800 in scheduler system 700 includes packet classifier 810, multiple queues 820 dedicated to different types of data, and queue tracker 830 (a queue scanner and analyzer) that reports on the traffic stored within each queue and the number of expired packets and delayed packets within each queue. Scheduler 840 acts as the decision maker between queue manager 800 and data link layer 850. Scheduler 840 examines the contents of queue manager 800 and data link 850 and makes decisions. Scheduler 840 also manages data traffic between the network layer and the data link layer 850. This process isolates the high-layer application or the network layer from direct interaction with the lower layer. However, these layers are mutually aware of each other.

In practice, IP layer 500 passes packets to packet classifier 810; packet classifier 810 examines the type of packet and associates an appropriate time for the packet, based on the type of packet, and then inserts that packet into appropriate queue 820. In a preferred embodiment of the system, the queues are for four distinct data types as previously described, namely: voice, video, audio and data. As a wireless network grows other types of data with different characteristics may be included. A challenge posed by queue 820 is the need for a module to monitor the queue, which normally adds delay to transmission scheduling. For this reason, each packet inserted in the buffer of queue 820 is an active record, resulting in the creation of packets of type timer. The expiration period of these packets varies for each timer as the timer packets are also typed (as voice, video, audio, or data timer). If the packet does not arrive at scheduler 840 before expiry of the timer the packet exits queue 820 and notifies queue tracker 830 of its expiry. Queue tracker 830 reports to scheduler 840 the number of expired packets, thereby notifying the scheduler 840 of the traffic congestion at each queue 820. Scheduler 840 makes a judgment as to which queue 820 should receive service first

based on the time sensitivity of the data type within the queue 820. Scheduler 840 may also be deployed on a server to schedule downlink data traffic to multiple mobile devices and different data traffic within a mobile device.

LOWICS – Network Status Monitor:

The SNR teller 900, as seen in Figure 9, is part of the network status monitor module. SNR teller predicts the near future Signal to Noise Ratio, in a time frame between the present (0) to the next 10 ms. The objective of this component is to be able to detect the expected signal-to-interference-plus-noise-ratio (SINR) value. Generally speaking SINR is the ratio of Signal Strength to the background noise ratio. The link rate depends on the SINR at the user's location. SINR can vary significantly within a cell. This variation is an inherent characteristic of all wireless systems and occurs primarily because of variations in RF propagation loss, building penetration loss, fading effects, and co-channel interference. As a result, the link rate experienced by a user may depend on his/her position within a cell, just as in the case of DSL.

Based on the support from Network Monitor 520, SNR values will be monitored. The objective of SNR teller system is to receive the monitored SNR value and by looking at these values in the past 5ms to present being able to calculate and estimate the expected value of the SNR value is in the next 5 to 10 millisecond. This resulted expected value will be used by the network monitor status module to make decision of when to switch the network, from one type to another (e.g. WiFi to cellular) and also used by the scheduler system to take this parameter into consideration for its scheduling decision making.

LOWICS – Neighbourhood Discovery

Neighbourhood discovery is a method, according to the invention, that reduces the time required when moving from one access point ("AP") to another over a wireless link (known as "roaming"), for example, a mobile device user moving in an airport. There are several different areas of research in eliminating this delay especially in the RF layer (Layer 1). In a preferred embodiment a RF level latency reduction layer 3.5 solution is used. For connection-oriented applications (for example, those that are TCP/IP based) the latency to transfer the communications and connection

from one AP to another could result in the retransmission of data and reestablishment of TCP after receiving a new IP from a new domain (in case of an intra domain move). For time-sensitive applications, this results in additional delay caused by the movement from one AP or domain to another.

In a preferred embodiment, a Layer 3.5 solution is used, which is a superset of Layer 2 roaming. In this embodiment, a layer above the Media Access Control (MAC) Layer and below the IP layer 500 monitors the AP(s) and domains, handles the packet forwarding between different AP's, while also shielding the higher layer of any changes. This solution requires Layer 2 roaming first but eliminates the extra delay of authentication and roaming applications to the new AP.

To achieve a preferred method of roaming, three main areas are considered:

a) Neighbourhood discovery;

b) Pre-registration; and

c) Packet forwarding.

In a preferred embodiment, a network status data module 570 located within LOWICS 340 provides network status data and neighbourhood discovery. In this embodiment LOWICS 340 has a single virtual adapter interface to the IP layer 500 but may bind itself to as many NIC 460 as are available. Network status monitor 570 monitors the collected AP information from a Wi-Fi card, including the AP name, MAC, Signal Strength, Noise Strength, and Signal to Noise Ratio. Network status monitor detects the next closest AP by receiving information from SNR Teller 900, which calculates the SNR for a period of time starting from past to future within a small time frame. SNR Teller 900 then sends pre-registration information to network status monitor 570 with the "Backup AP" that it has decided to be moved to. Therefore, the AP is located before a decision is made to roam.

In a preferred embodiment, the AP contains updateable firmware. Usually the AP firmware contains an IP layer protocol structure, including a routing table, a MAC address update table, DNS,

and other functionality. This firmware may be updated by adding a pre-register table. After identifying the AP the network status data module then sends a pre-registration request to the AP. The AP forwards the request to an advance server ("AS") and asks for authentication for the mobile device 30. The AS will check the authentication of the mobile device 30 against its database and send the authorization to the AP. The AP then records the MAC address of mobile device 30 in the AP's pre-register table. The AP also sends its own MAC address, network address and a time-to-live to the mobile device 30. When the network status data module 570 receives this information it stores for use for the next roam. The time-to-live tells the network status monitor 570 of the period of time the AP will keep the information in its pre-register table. If this time expires the network status monitor 570 should look for another round of pre-registration request. In the meantime, the network status monitor 570 will continuously look at the SNR to determine if the backup AP is the appropriate AP to roam to next.

In case the backup AP SNR degrades then the network monitor looks at finding and pre-registering with a new AP. The network status data module 570 in LOWICS 340 continuously monitors the network status and SNR. It is important that balance be maintained between fast roaming times and client stability. As an example, it is normal for an AP's signal strength to reduce as a function of its environment and frequency, therefore, such an occurrence should not be considered for a roam, or "handoff", as it could be an instant occurrence of the AP signal strength, and not the normal signal strength for such AP. To accomplish this, a timeframe threshold is created for the stability of the signal before roaming to that AP. A preferred threshold should be between 5 and 10 ms, but longer or shorter periods could be used.

The SNR should decrease in an active AP and increase in the back up AP before roaming occurs. To move from one AP or domain to another, network status monitor 570 first sends an update registration (Re-Registration) to the AS through the backup AP. As the backup AP already has the information in its pre-registered table, it just pushes the request to the AS immediately. This notifies the AS of the change of IP so the AS will start redirecting downlink traffic to the mobile device 30 through the new destination IP of the mobile device. After the mobile device 30 receives the confirmation from the AS, mobile device 30 redirects the uplink traffic. During this time mobile device 30 does not send any uplink traffic to the AS until it receives the confirmation. This method reduces the packet loss during the roaming, reduces the roaming duration as the information

already exists in the pre-registered table at the AP, and the change to the mobile device IP is completely transparent to the applications on both the mobile device and the far-end host application on the Internet. The latter sees the AS as the mobile device.

Figure 10 displays an overview sequence of events in pre-registration and neighbourhood discovery.

LOWICS – Local Jitter Handling:

The LOWICS 340 local jitter handler 710 handles received real-time data types. Its main responsibility is to handle the jitter on VoIP and real-time video based on the network status and information received. This eliminates the need for using RTCP, which creates high network overhead. To achieve this, a buffer agent examines the Type of Content (ToC) within DMP and decides whether to deliver the DMP to a higher layer or keep it in the buffer module. Each data packet inserted into a buffer is attached to a timer. As the timer expires the data packet will exit the buffer queue in the higher layer. This makes the individual rows of the buffer an active agent that "watch" the buffer's state. This reduces a need for an agent to track what has to be removed from the buffer and what does not and therefore reduces the buffer delay. The jitter buffer is in the lower layer as decisions are made based on real-time network information instead of on the feedback mechanism provided by RTCP. The feedback mechanism is not very efficient, as the frequency of incoming feedback cannot be adjusted for efficiency for wireless traffic while also providing sufficient and timely information to reduce jitter. Using the above described process, jitter may be reduced by 20-30%.

Network Policy

The method and system according to the invention can also control a network device based on the requirements of the network policy. In such a case, the network policy must be created, and transmitted to the network device for storage, such as a mobile device, when the network device requests registration.

When an application is attempting to access the network, the network policy usage will be checked, and TOPICS and LOWICS will provide network access to the application according to the policy. During the transactions between the network device and network server, at any time if the network

policy is changed at the database in the advance server the change will be pushed to the network device in a form of "Policy Push" command.

The two tables below describe, in a preferred embodiment, the policy parameters that will be pushed to the networked device at the registration time. Table 3 describes the policy parameters; Table 4 describes a "Class of Service" data structure.

TABLE 3:

PARAMETER	DESCRIPTION
User Class	Identifies the priority of users in using network. This parameter is usually refer to as Gold, Silver and Bronze.
Class of Service	Identifies the type of service, Background, Interactive, Streaming, Conversational
Priority of Service	This can be High, Medium and Low variable or a numerical value of 0 to 10; where 10 is the highest priority. Note that up & downlink bandwidth could still differentiate services sharing the same priority.
Uplink Bandwidth	The Bandwidth used for the specific class of service in Uplink channel
Uplink Data Rate	Average and Peak Data Rate for the Uplink channel
Delay	Maximum tolerable delay, this is only enforceable within the QoS scheduling of LOWICS for maximum delay that packet can stay in Queue before being delivered to the MAC layer
Downlink Data Rate	The policy used in Downlink (from MAG to ICS) for transferring data for this class of service. This will help ICS estimate the expected delay of arrival of the packets from MAG
Uplink Total Data Transmission	A parameter used to keep track of the total data transmission per month for that class of service in Uplink channel. The time will be reset and pushed to the ICS from MAG side. This could be calculated to exclude the duplicate/lost packets and even headers from the customer's actual payload data
Offset time	The time that total data transmission will be reset for usage and accounting purposes. This is offset time will block user to send data over the uplink when they reach maximum transmission on uplink
Network Type	Identifies the type of network (Preferred type, or the only type) that can be used for that service
Time of Use	Whether this person can use this service at all the time or only certain time (e.g. slow hours or peak hours or always)

TABLE 4:

PARAMETER	DESCRIPTION

User Class	Identifies the priority of users in using network. This parameter is usually refer to as Gold, Silver and Bronze.
Application Name	Name of application using network
Destination IP	The IP of the far host
Destination URL	Far-host URL (it could be exchangeable with Destination IP)
Access	A Union that contains Access information similar to class of Service structure. If the Uplink & Downlink Bandwidth value is zero then this means no access.
Uplink Bandwidth	The Bandwidth used for the specific class of service in Uplink channel
Uplink Data Rate	Average and Peak Data Rate for the Uplink channel
Delay	Maximum tolerable delay, this is only enforceable within the QoS scheduling of LOWICS for maximum delay that packet can stay in Queue before being delivered to the MAC layer
Downlink Data Rate	The policy used in Downlink (from MAG to ICS) for transferring data for this class of service. This will help ICS estimate the expected delay of arrival of the packets from MAG
Uplink Total Data Transmission	A parameter used to keep track of the total data transmission per month for that class of service in Uplink channel. The time will be reset and pushed to the ICS from MAG side. This could be calculated to exclude the duplicate/lost packets and even headers from the customer's actual payload data
Offset time	The time that total data transmission will be reset for usage and accounting purposes. This is offset time will block user to send data over the uplink when they reach maximum transmission on uplink
Network Type	Identifies the type of network (Preferred type, or the only type) that can be used for that service
Time of Use	Whether this person can use this service at all the time or only certain time (e.g. slow hours or peak hours or always)

Network Performance

The method and system according to the invention can provide service performance and status information to a carrier for any application over any types of network and without a need for creating extra transactions over the network. To do this, the network device stores an acceptable performance threshold parameter per application on the device. As the application data is carried to the advance server, the network device stores information about the type of network used per packet, the signal to noise ratio parameter on each packet, packets lost, duplicate, retransmissions and the total time needed to deliver application message and receive response information. This information is stored within a database in network status monitor 520. If any of the parameters

exceed the threshold set in either the database, local in the network device, or calculated based on certain rules (such as the network policy), the an alert is generated and sent to the advance server.

Determining type of application data

The system and method according to the invention can be used to determine the type of application data on a client device, such as a mobile device, without changing the application. This is done when ICS receives an application request by intercepting the call. ICS then identifies the application name, and/or the port used to send the message, and/or the header information (which is part of the first two application message buffer sent for the request for connection). This extracted information, such as VoIP, Video, email, Internet explorer; is used to create a corresponding tag such as Real-time, Streaming, Background, Interactive, and the packet is accordingly tagged.

The above described system and method can be implemented as a series of instructions stored on computer readable memory within a networked device, such as within RAM, or on computer readable storage medium. The method and system may be expressed as a series of instructions present in a carrier wave embodying a computer data signal to communicate the instructions to a networked device or server, which when executed by a processor within the mobile device or server, carry out the method.

The above method and system, while described in the context of a wireless or mixed network would also have application in wired networks, in cases where the wired network device is "smart" and able to identify and process incoming packets.

Although the particular preferred embodiments of the invention have been disclosed in detail for illustrative purposes, it will be recognized that variations or modifications of the disclosed apparatus lie within the scope of the present invention.

CLAIMS

The invention claimed is:

1. A method of controlling a mobile device based on a network policy, comprising the steps of:

(a) storing said policy on a database on an advance server;

(b) sending said policy to said mobile device when said mobile requests registration with said server;

(c) when an application on said mobile device attempts to access a network via said server, checking said policy; and

(d) providing access to said network for said application when said policy permits.

2. The method of claim 1 wherein, if said policy changes at the database, said changed policy is pushed to said mobile device.

3. The method of claim 2 wherein said network policy includes a plurality of parameters.

4. The method of claim 3, wherein said policy parameters, include a first parameter based on the type of service provided by said application.

5. The method of claim 4 wherein said policy parameters include a second parameter based on the maximum tolerable delay.

6. The method of claim 5 wherein said policy parameters include a third parameter based on the time of usage of said application.

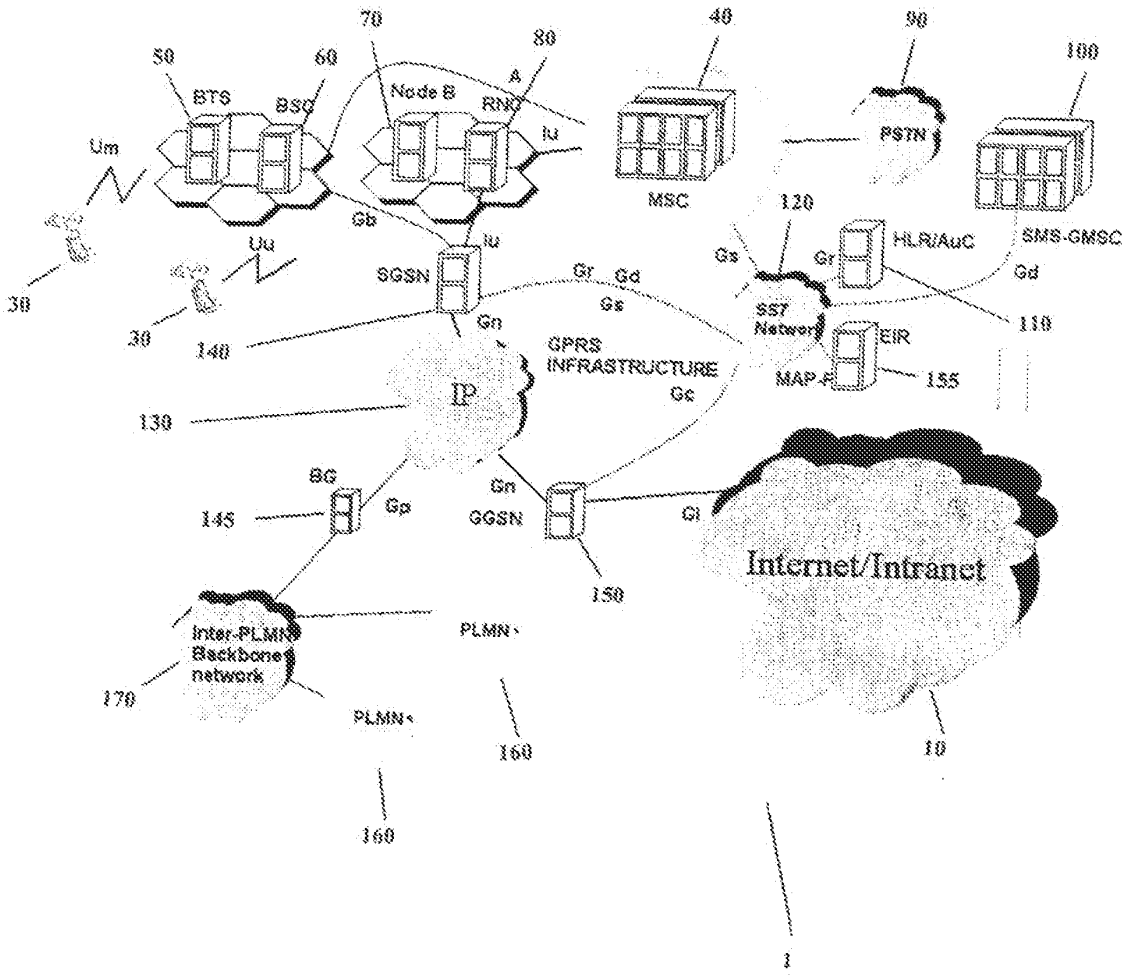

70
80
40
90
100
50
60
BTS
BSC
Node B
RNC
A
Iu
Um
MSC
PSTN
120
HLR/AuC
SMS-GMSC
Gb
Iu
Gs
Gr
Gd
Uu
SGSN
Gr
Gd
Gs
SS7 Network
EIR
110
30
38
140
Gn
GPRS INFRASTRUCTURE
MAP-F
155
IP
Gc
130
BG
Gn
145
Gp
GGSN
Gi
Internet/Intranet
150
Inter-PLMN Backbone network
PLMN
170
PLMN
160
10
160
1

FIGURE 1

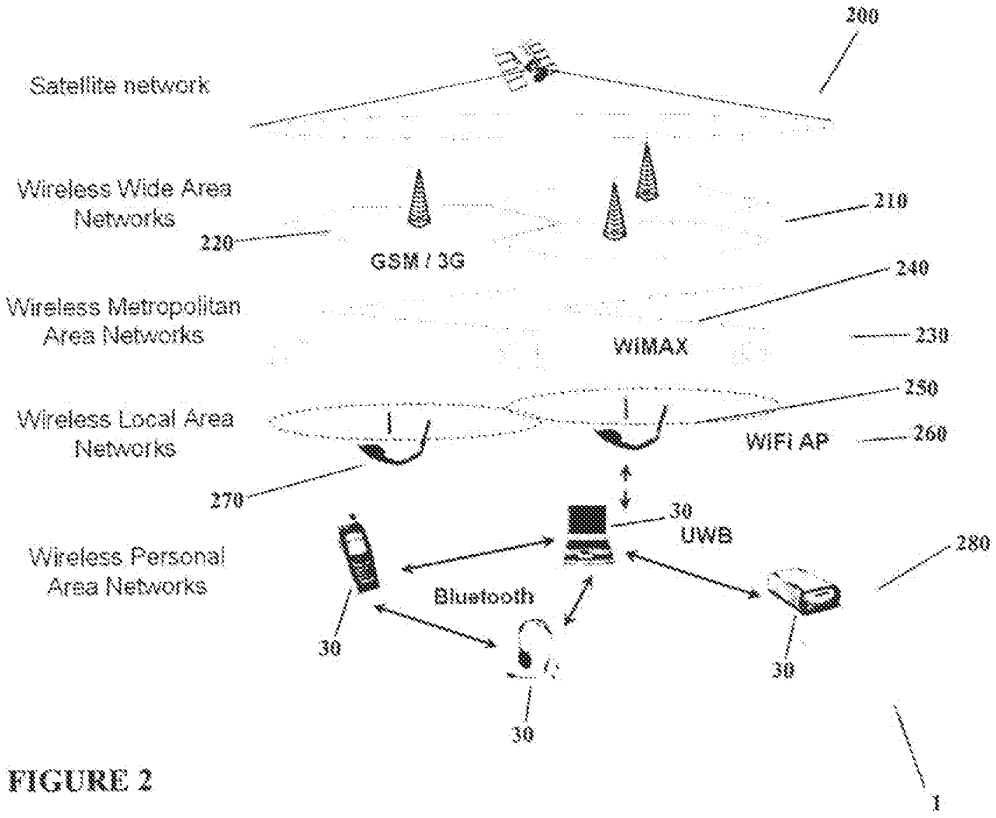

200
Satellite network
Wireless Wide Area Networks
210
220
GSM / 3G
240
Wireless Metropolitan Area Networks
WiMAX
230
250
Wireless Local Area Networks
WiFi AP
260
270
30
UWB
280
Wireless Personal Area Networks
Bluetooth
30
30
30
1

FIGURE 2

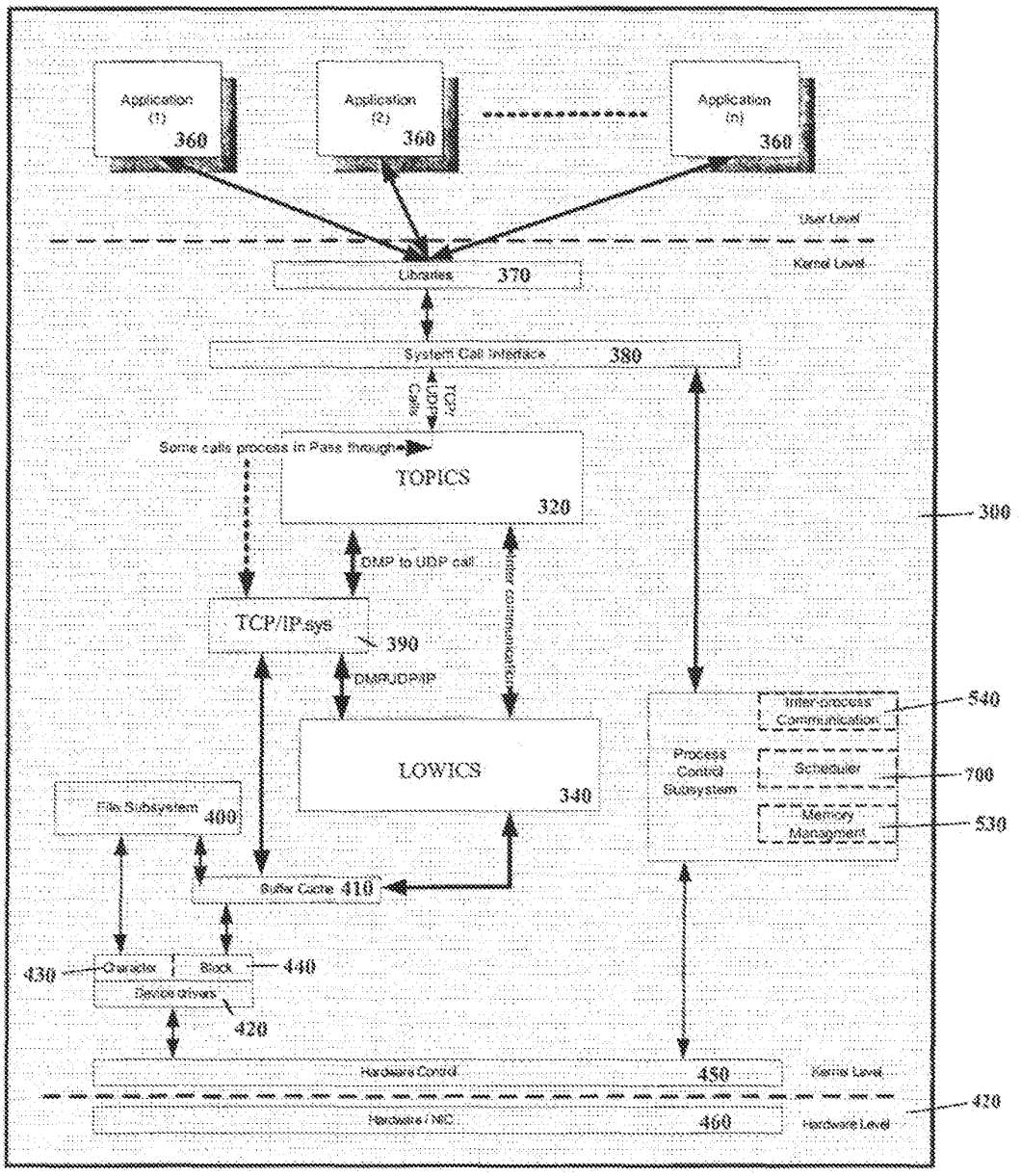

Application (1) 360
Application (2) 360
Application (n) 360
User Level
Kernel Level
Libraries 370
System Call Interface 380
Some calls process in Pass through
TOPICS 320
300
DMP to UDP call
Inter communication
TCP/IP.sys 390
DMP/UDP/IP
LOWICS 340
Inter-process Communication
540
Process Control Subsystem
Scheduler
700
Memory Management
530
File Subsystem 400
Buffer Cache 410
430
Character
Block
440
Device drivers
420
Hardware Control 450
Kernel Level
Hardware / NIC 460
Hardware Level
420

FIGURE 3

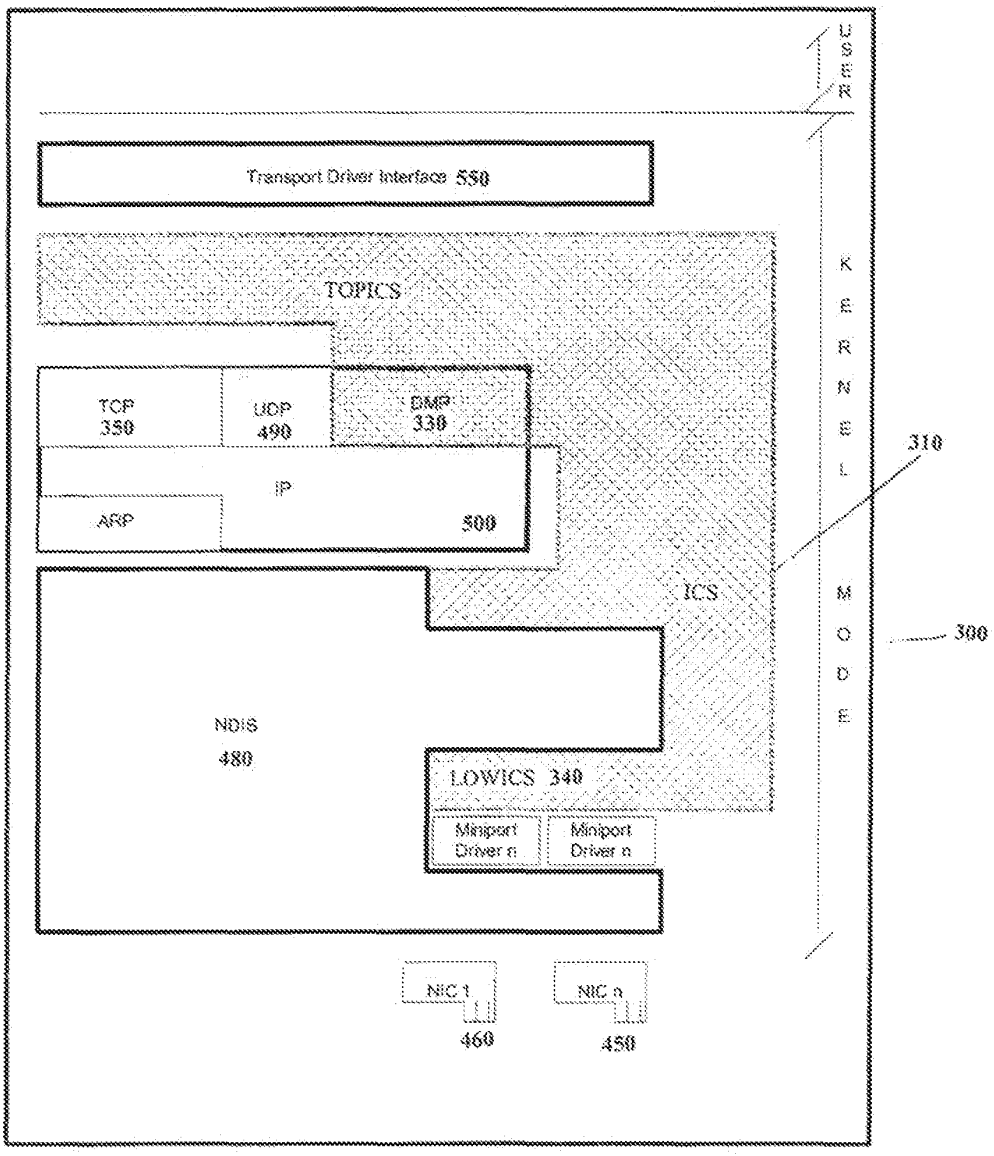

USER
Transport Driver Interface 550
TOPICS
TCP 350
UDP 490
DMP 330
IP
ARP
500
ICS
310
300
MODE
NDIS 480
LOWICS 340
Miniport Driver n
Miniport Driver n
NIC 1
NIC n
460
450

FIGURE 4

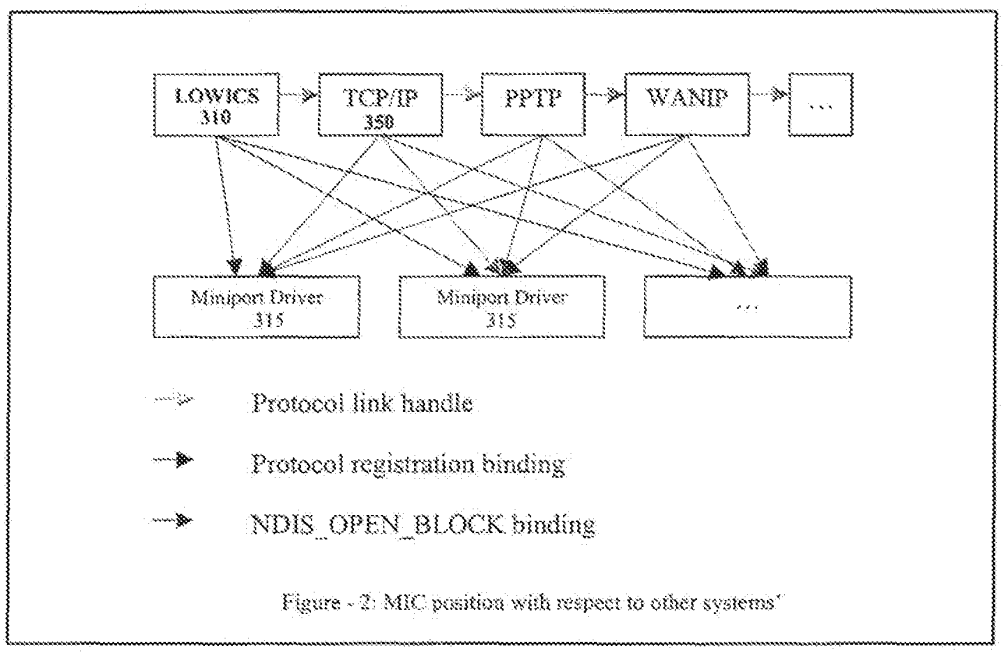


Figure - 2: MIC position with respect to other systems'

FIGURE 5

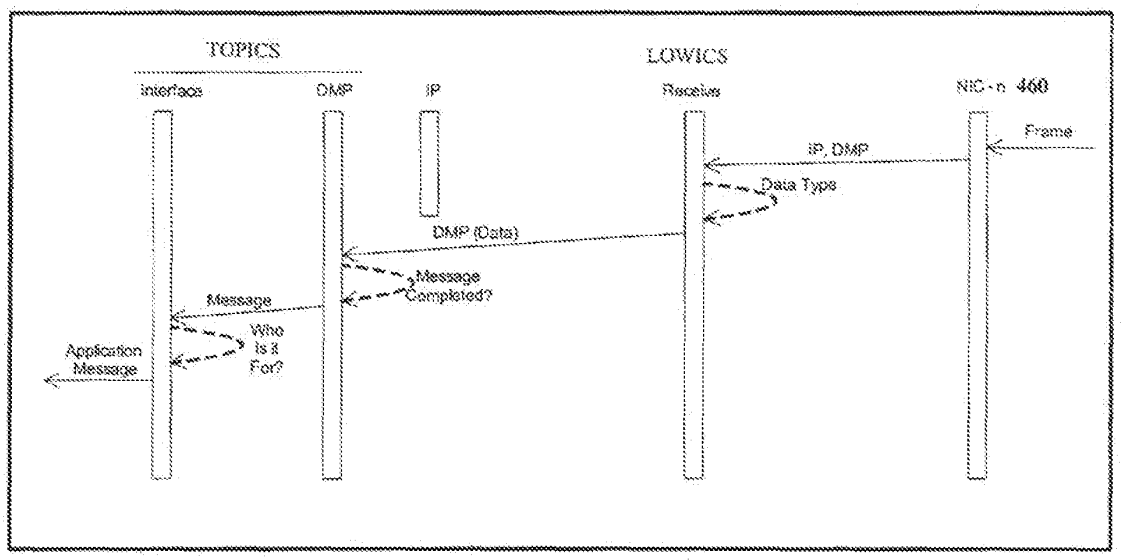

TOPICS
LOWICS
Interface
DMP
IP
Receive
NIC - n 460
Frame
IP, DMP
Data Type
DMP (Data)
Message Completed?
Message
Who Is it For?
Application Message

FIGURE 6

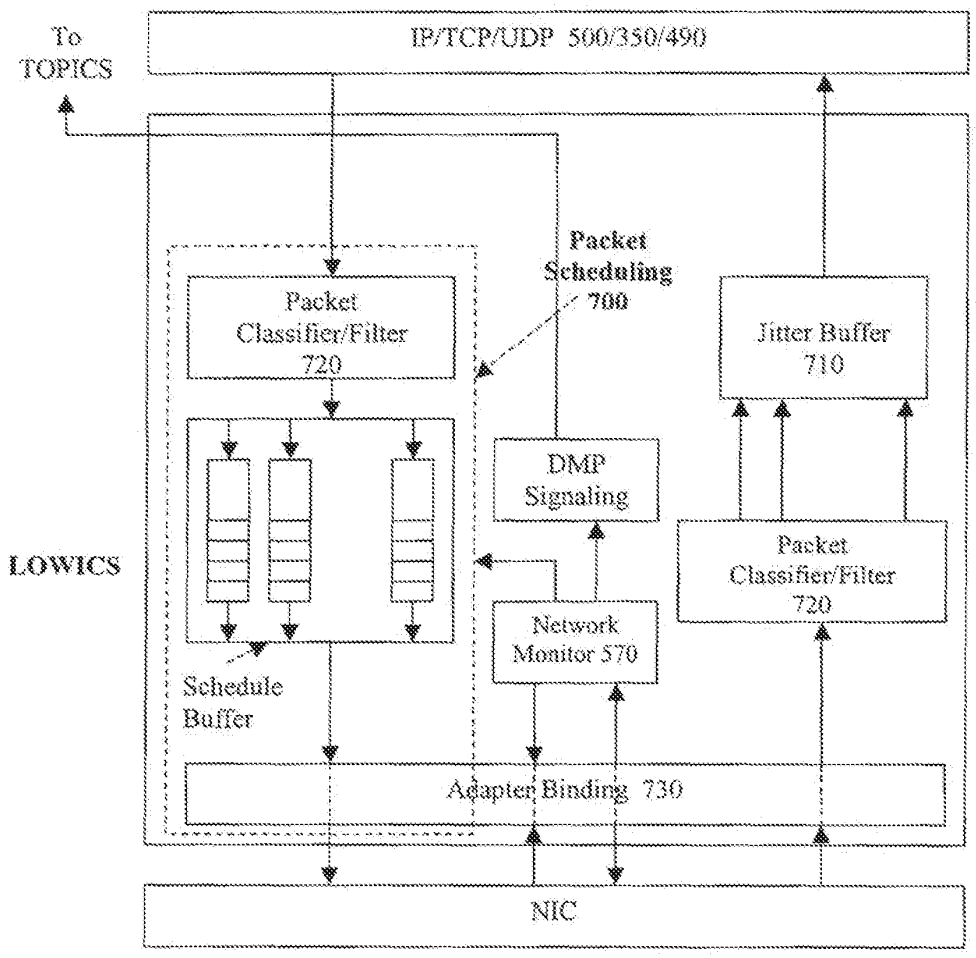

To
TOPICS
IP/TCP/UDP 500/350/490
Packet
Scheduling
700
Packet
Classifier/Filter
720
Jitter Buffer
710
DMP
Signaling
LOWICS
Packet
Classifier/Filter
720
Network
Monitor 570
Schedule
Buffer
Adapter Binding 730
NIC

FIGURE 7

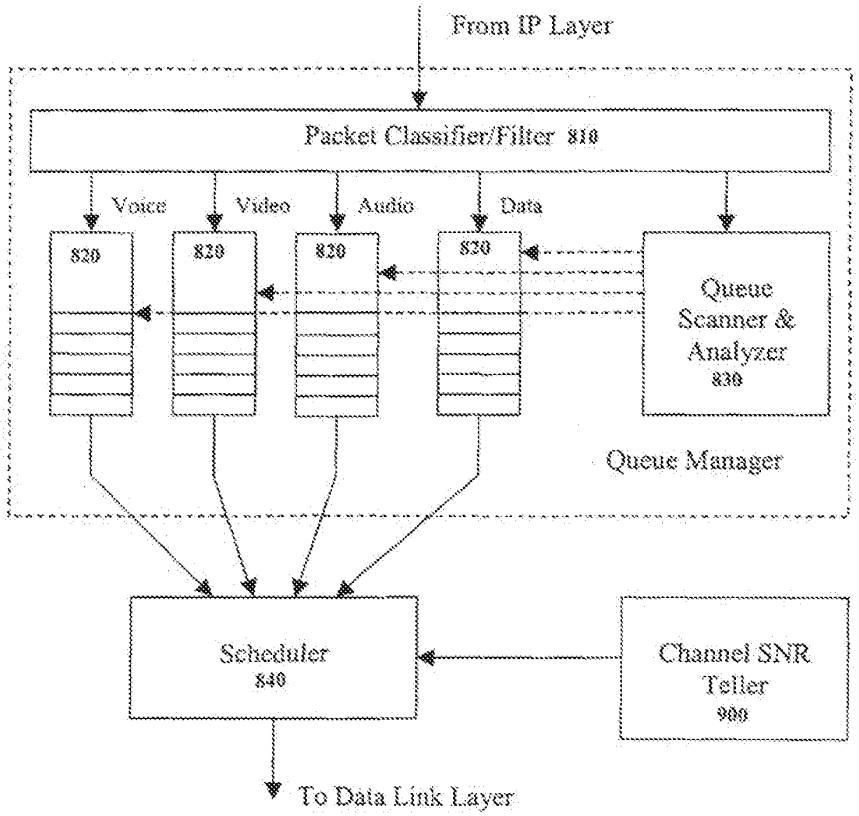

From IP Layer
Packet Classifier/Filter 810
Voice
Video
Audio
Data
820
820
820
820
Queue Scanner & Analyzer 830
Queue Manager
Scheduler 840
Channel SNR Teller 900
To Data Link Layer

FIGURE 8

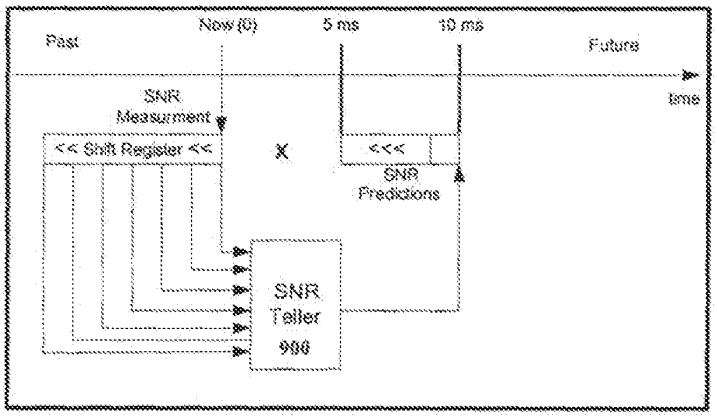

Now (0)
5 ms
10 ms
Past
Future
time
SNR
Measurment
<< Shift Register <<
X
<<<
SNR
Predictions
SNR
Teller
900

FIGURE 9

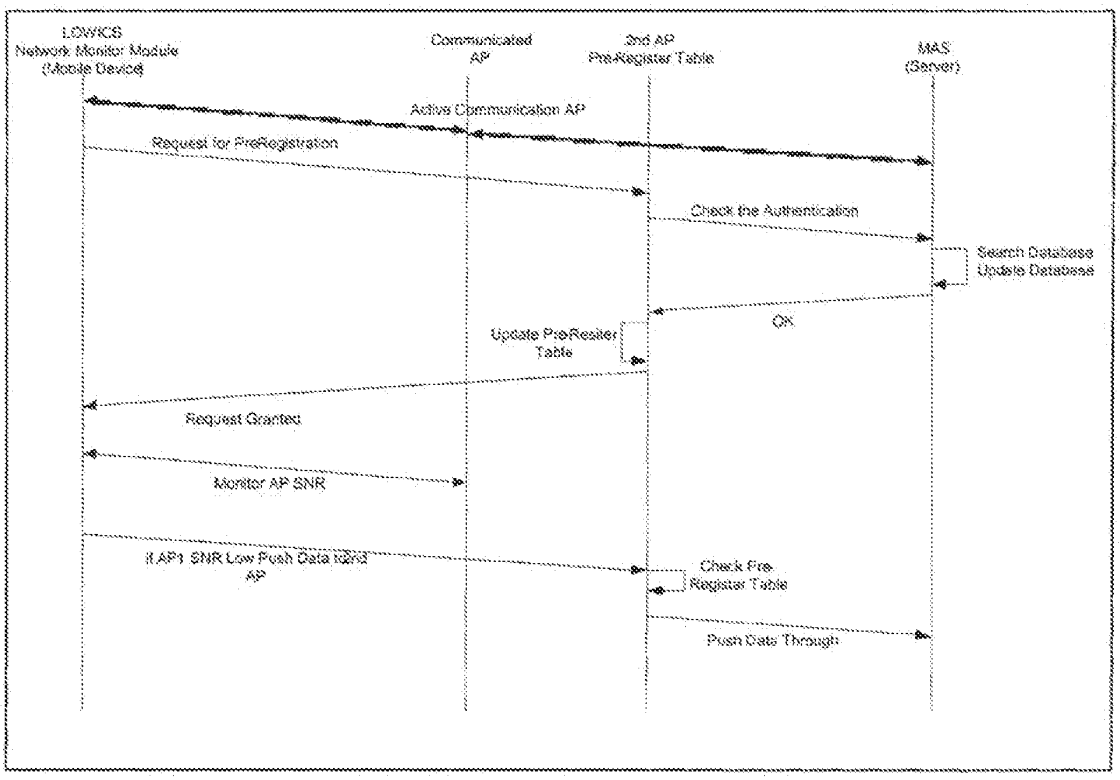
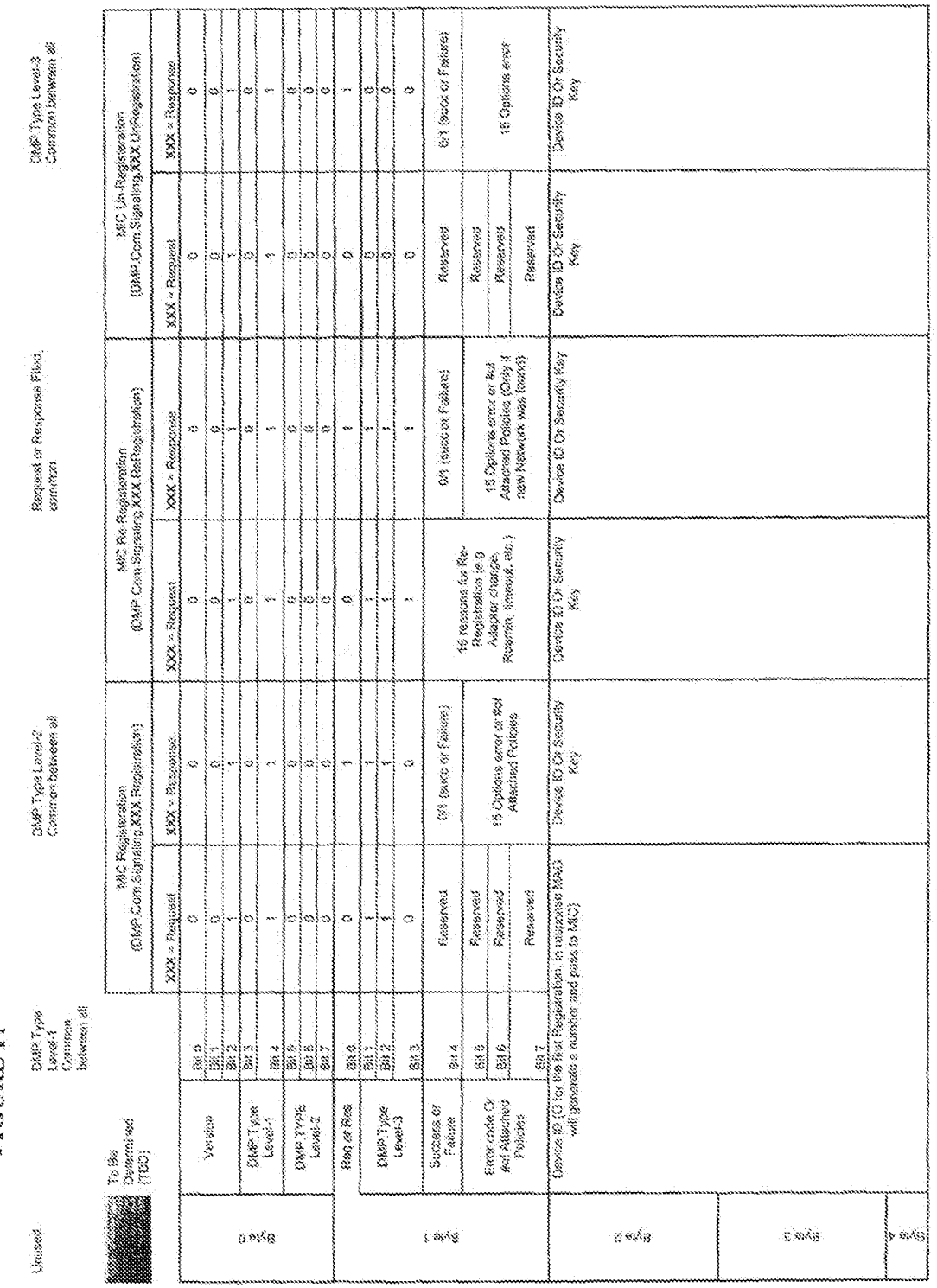

LDWICS
Network Monitor Module
(Mobile Device)
Communicated
AP
2nd AP
Pre-Register Table
MAS
(Server)
Active Communication AP
Request for PreRegistration
Check the Authentication
Search Database
Update Database
OK
Update PreResiter
Table
Request Granted
Monitor AP SNR
If AP1 SNR Low Push Data to2nd
AP
Check Pre
Register Table
Push Data Through

FIGURE 10

FIGURE 11


Unused
To Be Determined (TBD)
DMP Type Level-1 Common between all
DMP Type Level-2 Common between all
Request or Response Field, common
DMP Type Level-3 Common between all
MIC Registration (DMP Com Signaling,XXX Registration)
MIC Re-Registration (DMP Com Signaling,XXX ReRegistration)
MIC Un-Registration (DMP Com Signaling,XXX UnRegistration)
XXX = Request
XXX = Response
Byte 0
Byte 1
Byte 2
Byte 3
Byte 4
Version
DMP Type Level-1
DMP TYPE Level-2
Req or Res
DMP Type Level-3
Success or Failure
Error code Or ref Attached Policies
Reserved
61 (succ or Failure)
15 Options error on Ref Attached Policies
16 reasons for Re-Registration (e.g Adapter change, Roamin, timeout, etc.)
15 Options error on Ref Attached Policies (Only if new Network was found)
16 Options error
Device ID (0 for the first Registration, in response MAS will generate a number and pass to MD)
Device ID Or Security Key

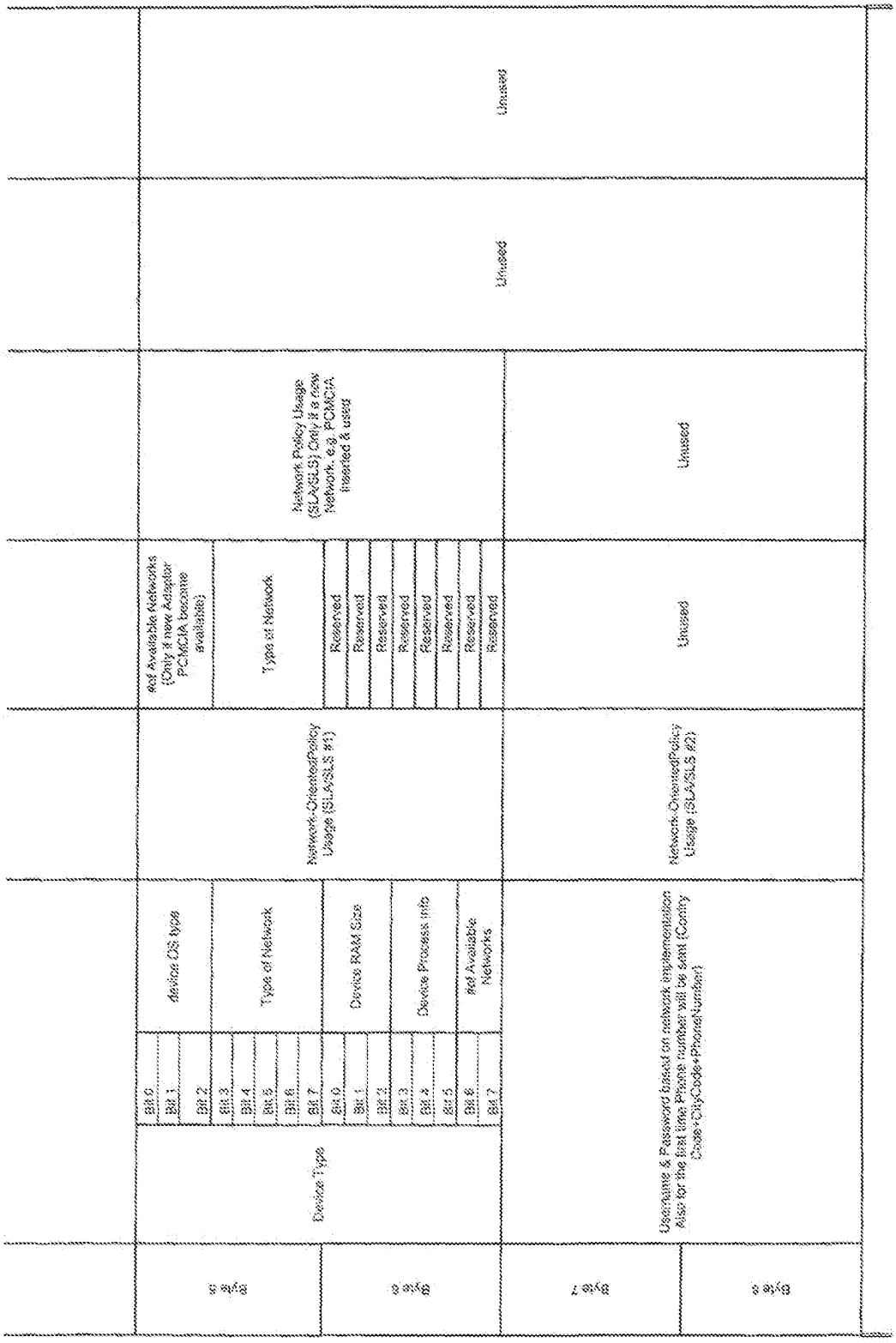
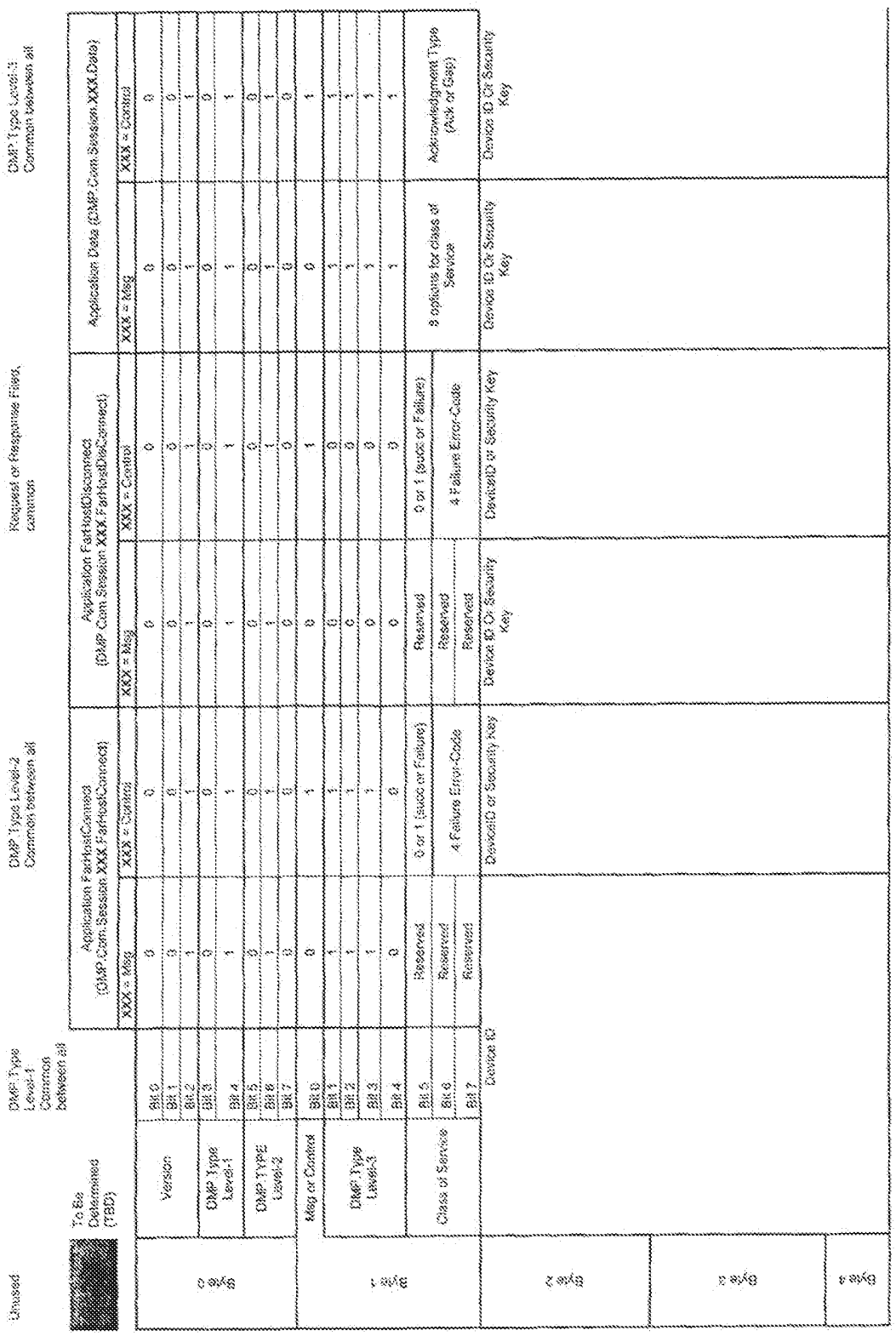
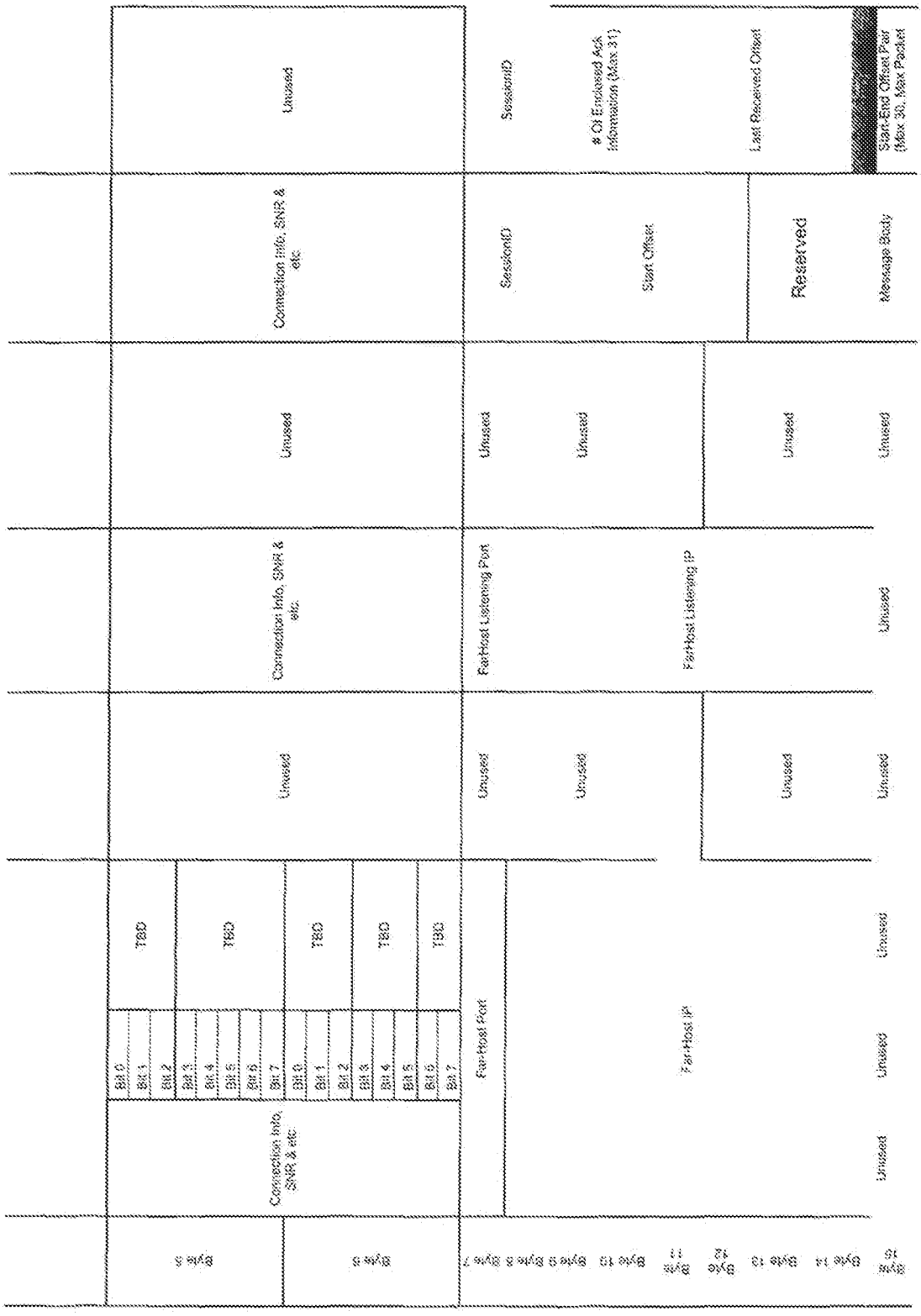
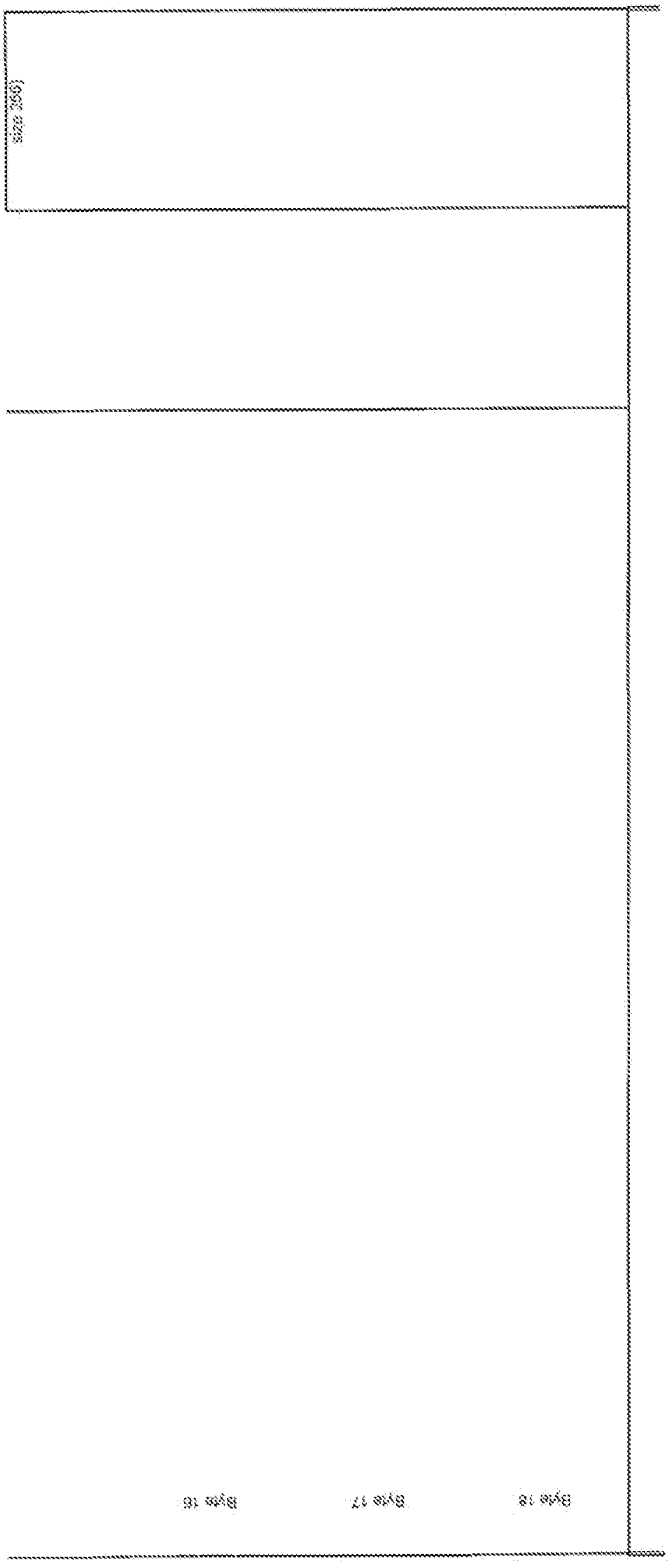

Byte 5
Byte 6
Byte 7
Byte 8
Device Type
Bit 0
Bit 1
Bit 2
Bit 3
Bit 4
Bit 5
Bit 6
Bit 7
device OS type
Type of Network
Device RAM Size
Device Process info
#of Available Networks
Network-OrientedPolicy Usage (SLA/SLS #1)
Network-OrientedPolicy Usage (SLA/SLS #2)
Username & Password based on network implementation
Also for the first time Phone number will be sent (Country Code+CityCode+PhoneNumber)
Unused
#of Available Networks (Only if new Adaptor PCMCIA become available)
Type of Network
Reserved
Reserved
Reserved
Reserved
Reserved
Reserved
Reserved
Reserved
Network Policy Usage (SLA/SLS) Only if a new Network, e.g. PCMCIA inserted & used
Unused
Unused
Unused

FIGURE 12


Unused
To Be Determined (TBD)
DMP Type Level-1 Common between all
DMP Type Level-2 Common between all
Request or Response Flags, common
DMP Type Level-3 Common between all
Byte 0
Byte 1
Byte 2
Byte 3
Byte 4
Version
DMP Type Level-1
DMP TYPE Level-2
Msg or Control
DMP Type Level-3
Class of Service
Device ID
Application FarHostConnect (DMP Com Session XXX.FarHostConnect)
XXX = Msg
XXX = Control
Application FarHostDisConnect (DMP Com Session XXX.FarHostDisConnect)
XXX = Msg
XXX = Control
Application Data (DMP Com Session XXX.Data)
XXX = Msg
XXX = Control
Reserved
0 or 1 (succ or Failure)
4 Failure Error-Code
DeviceID or Security Key
8 options for class of Service
Acknowledgment Type (Ack or Esc)


Byte 0
Byte 1
Byte 2
Byte 3
Byte 4
Byte 5
Byte 6
Byte 7
Byte 8
Byte 9
Byte 10
Byte 11
Byte 12
Byte 13
Byte 14
Byte 15
Connection Info, SNR & etc
TBD
Bit 0
Bit 1
Bit 2
Bit 3
Bit 4
Bit 5
Bit 6
Bit 7
Far-Host Port
Far-Host IP
Unused
SessionID
Of Enclosed AoA Information (Max 31)
Last Received Offset
Start-End Offset Pair (Max 30, Max Packet
Start Offset
Reserved
Message Body
Far-Host Listening Port


Size 256)
Byte 16
Byte 17
Byte 18

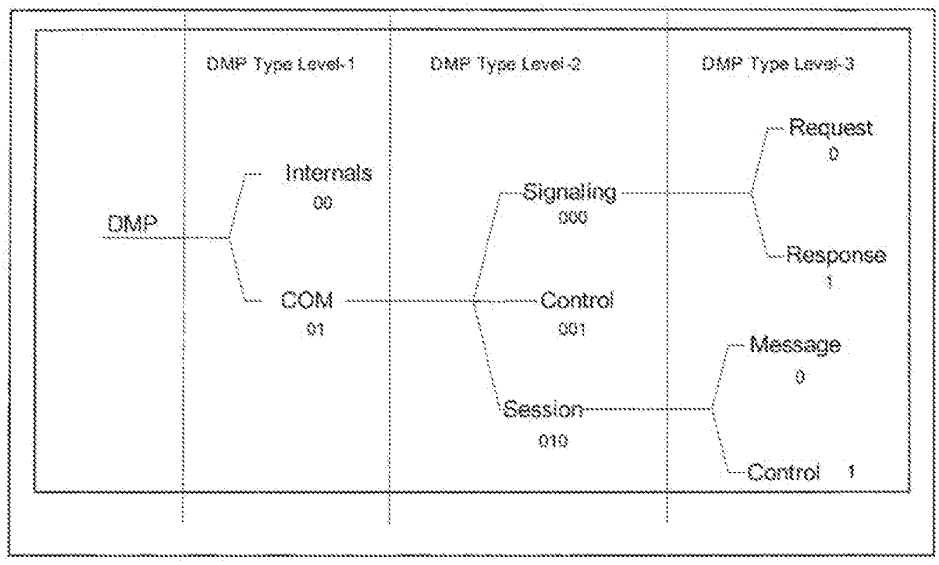

DMP Type Level-1
DMP Type Level-2
DMP Type Level-3
DMP
Internals
00
COM
01
Signaling
000
Control
001
Session
010
Request
0
Response
1
Message
0
Control
1

FIGURE 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2006/000901

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 29/02*** (2006.01) , ***H04L 29/04*** (2006.01) , ***H04Q 7/20*** (2006.01)
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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database, IEEE, USPTO: mobile, wireless, cell, cellular, policy, network, send, download, service

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	WO 2006/044714 A1 Balasubramanian *et al.*, 27 April 2006 (27-04-2006), whole document	1-6
X	WO 97/19525 A1 Dupont, Pierre, 29 May 1997 (29-05-1997), abstract, figures 1-2, page 5 line 25 to page 6 line 19	1-6
A	US 6,714,987 B1 Amin et al., 30 March 2004 (30-03-2004), whole document	1-6

[ ] 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
25 October 2006 (25-10-2006)	27 October 2006 (27-10-2006)
Name and mailing address of the ISA/CA 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	Authorized officer Stuart Ginn 819- 934-5147

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CA2006/000901

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO2006044714	27-04-2006	US2006084432 A1	20-04-2006
WO9719525	29-05-1997	AT268961T T	15-06-2004
		CN1097893C C	01-01-2003
		CN1132355C C	24-12-2003
		CN1147736 A	16-04-1997
		DE69624495D D1	28-11-2002
		DE69624495T T2	06-03-2003
		DE69632680D D1	15-07-2004
		DE69632680T T2	21-10-2004
		EP0804834 A1	05-11-1997
		EP0847652 A2	17-06-1998
		ES2220936T T3	16-12-2004
		US5729542 A	17-03-1998
		US5742592 A	21-04-1998
		WO9711566 A2	27-03-1997
US6714987	30-03-2004	AU7733987B B2	10-06-2004
		AU6968800 A	10-05-2001
		EP1098490 A2	09-05-2001

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

(11) EP 1 772 988 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
11.04.2007 Bulletin 2007/15

(21) Application number: 05820675.6

(22) Date of filing: 20.12.2005

(51) Int Cl.:
H04L 9/36 (2006.01) *H04Q 7/20* (2006.01)

(86) International application number:
PCT/CN2005/002254

(87) International publication number:
WO 2006/069522 (06.07.2006 Gazette 2006/27)

(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: 28.12.2004 CN 200410103467

(71) Applicant: Huawei Technologies Co., Ltd.
Longgang District,
Shenzhen
Guangdong 518129 (CN)

(72) Inventors:
- ZHENG, Zhibin,
Huawei Administration Building
Guangdong 518129 (CN)
- LIU, Tingyong,
Huawei Administration Building
Guangdong 518129 (CN)
- TU, Weihua,
Huawei Administration Building
Guangdong 518129 (CN)
- HOU, Zhipeng,
Huawei Administration Building
Guangdong 518129 (CN)

(74) Representative: Thun, Clemens
Mitscherlich & Partner
Sonnenstrasse 33
80331 München (DE)

(54) A METHOD, SYSTEM AND APPARATUS FOR REALIZING THE DATA SERVICE SAFETY OF THE MOBILE COMMUNICATION SYSTEM

(57) A method for implementing data service security in a mobile communication system includes: obtaining security condition of a user terminal based on security-relevant configuration information reported by the user terminal; determining a security policy for the user terminal based on the security-relevant configuration information of the user terminal and security policy information stored, and sending the security policy determined to a packet service support node and/or the user terminal; implementing, by the packet service support node and/or the user terminal, a control process based on the security policy. The method, system and apparatus provided by the embodiments of the present invention introduce a security mechanism cooperated by the mobile communication network and a user terminal to effectively prevent the mobile communication network against viruses.

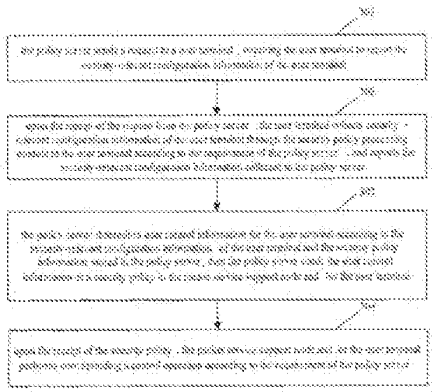


Fig. 3

EP 1 772 988 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the invention

[0001] The present invention relates to communication security technologies, and particularly, to a method, a system and an apparatus for implementing data service security in a mobile communication system.

Background of the invention

[0002] Along with applications of data services in mobile communication systems, and particularly with the development of mobile terminals towards intelligence, the mobile terminals are equipped with not only conventional voice communication functions, but also Personal Digital Assistant (PDA) functions, and may provide intelligent operation systems and application software. Moreover, as Personal Computer Memory Card International Association (PCMCIA) is widely applied, more and more users obtain Internet services via mobile networks by inserting the PCMCIA cards into the mobile terminals. Being equipped with WINDOWS operation systems and various kinds of application software, the mobile terminals act more and more like personal computers. Therefore, viruses in fixed networks are also found in the mobile networks.

[0003] In the mobile network, there are two conventional ways to prevent viruses:

1) Install anti-virus software on a terminal side, the terminal scans data to be transmitted and removes possible viruses using the anti-virus software;

2) Install an anti-virus gateway on the mobile network, the anti-virus gateway implements online scan to the data traffic passing the anti-virus gateway and removes the viruses; this method requires high performance for the anti-virus gateway, e.g., in order to scan viruses in short messages, a short message gateway needs virus scan and remove functions.

[0004] It can be seen from the fore-going descriptions that, in conventional ways, anti-virus software is generally installed where the data traffic passes to scan and remove the viruses. However, all types of anti-virus software may only scan and remove known viruses and are not capable of preventing unknown viruses from spreading, thus unknown viruses are still disturbing network traffics.

[0005] Moreover, the impact of the viruses and worms may be brought out by many factors including the version of the operation system, the version of the anti-virus software and the capability of the anti-virus software. For example, greater damages may result from the absence of a certain operation system patch, e.g., the virus worm.Blaster damages a system through a bug in the Windows operation system. In fact, before a virus breaks out, providers of the operation system usually announce a corresponding patch; however, the virus may still spread to a large scope because the patch is not installed in many personal computers in time. In addition, for a terminal in which the anti-virus software has already been installed, the update of the anti-virus software is also very important.

Summary of the invention

[0006] One embodiment of the present invention provides a method for implementing data service security in a mobile communication system, so as to effectively handle and control viruses in the mobile communication system.

[0007] Another embodiment of the present invention provides a system for implementing data service security in a mobile communication system. The system introduces a security mechanism cooperated by the mobile communication network and a user terminal to improve the defense of the mobile communication network against viruses.

[0008] Yet another embodiment of the present invention provides an apparatus for implementing data service security in a mobile communication system, so as to determine, store and distribute security policies.

[0009] According to an embodiment of the present invention, the method for implementing data service security in a mobile communication system includes:

obtaining security-relevant configuration information of a user terminal;

determining a security policy for the user terminal based on the security-relevant configuration information of the user terminal and security policy information stored, and sending the security policy determined to a packet service support node and/or the user terminal;

upon the receipt of the security policy, implementing, by the packet service support node and/or the user terminal, a control process based on the security policy.

[0010] Another embodiment of the present invention provides a system for implementing data service security in a mobile communication system, including:

a packet service support node;

a user terminal, communicates with the packet service support node through the mobile communication network; the system further includes:

a policy service entity, connected to the packet service support node, and configured to obtain security-relevant configuration information of

the user terminal, determine a security policy for the user terminal and distribute the security policy to the packet service support node and/or the user terminal.

[0011] Another embodiment of the present invention provides an apparatus for implementing data service security in a mobile communication system, including:

a security information obtaining module, configured to communicate with a user terminal, obtain security-relevant configuration information of the user terminal and send the security-relevant configuration information obtained to a security policy determination module;

the security policy determination module, configured to determine a security policy based on the security-relevant configuration information of the user terminal and security policy information stored in a security policy storage module and send the security policy determined to a security policy distribution module;

the security policy storage module, configured to store the security policy information;

the security policy distribution module, configured to send the security policy received to a designated network entity.

[0012] The method, system and apparatus for implementing data service security provided by the embodiments of the present invention in a mobile communication system add a policy service entity into the existing mobile communication system. The policy service entity is configured to store security policy information, determine a security policy based on the security-relevant configuration information of the user terminal, and notify the packet service support node on the network side and/or the user terminal to implement the security process. The embodiments of the present invention have the following advantages:

1) the security policy of the user terminal is associated with that on the network side, and a joint security mechanism is provided for the network and the user terminal. Through the protection on both the user terminal and the network side, not only known viruses, but also unknown viruses may be detected and removed, thus full dimensional security is achieved;

2) since security threats always come from the user terminal, the method provided by an embodiment of the present invention determines a security policy based on the security-relevant configuration information reported by the user terminal, therefore implements control on the user terminal. The method provided by an embodiment of the present invention may implement security control on the headstream, and effectively prevent the security threats from spreading. And, with the cooperation of the network side, the virus may be effectively handled and restricted;

3) with regard to cell phone viruses that tend to be more and more serious in the future, effective security measures may be taken based on the system architecture provided by the embodiments of the present invention to control viruses in the mobile communication network, and further prevent the spreading of cell phone viruses;

4) the embodiments of the present invention may obtain the security condition of the user terminal and determine a security policy according to the security condition of the user terminal, and instructs the packet service support node and/or the user terminal to implement a control process according to the security policy, therefore the embodiments of the present invention may prevent the network from virus infection, especially worm infection;

5) if the packet service support node is a GGSN, the embodiments of the present invention support security control over data packets on both uplink and downlink, thus it is possible to effectively prevent attacks from the mobile network to a public network, and vice versa. Moreover, the implementation of the security policy may be very flexible, i.e., it may be implemented in the GGSN, or implemented in the SSGN or the RNC which is notified to implement the control process by the GGSN;

6) the embodiments of the present invention only need a minor modification or a simple additional protocol to the function modules in the packet service support node, the user terminal and the security gateway to achieve effective security interworking and implement data packets security process. The implementation of the embodiments of the present invention is simple and convenient without increasing hardware cost.

Brief Description of the Drawings

[0013]

Fig. 1 is a schematic structure of a system according to an embodiment of the present invention.

Fig. 2 is a schematic structure of another system according to an embodiment of the present invention.

Fig. 2 is a flow chart of a method for implementing

data service security according to an embodiment of the present invention.

Fig. 4 is a schematic diagram illustrating a structure of the apparatus according to an embodiment of the present invention.

Embodiments of the invention

[0014] The embodiments of the present invention add a policy service entity into the mobile communication network. The policy service entity determines a security policy based on the security-relevant configuration information of a user terminal and notifies a packet service support node on the network side and/or the user terminal to implement a security process according to the determined security policy.

[0015] The policy service entity may be a policy server, a function module embedded in a network entity, or a card. The user terminal may be a mobile intelligent terminal or a portable terminal with card slot. The packet service support node on the network side may be a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN) or a Packet Data Support Node (PDSN).

[0016] As shown in Fig. 1, the system for implementing data service security in the mobile communication system in accordance with an embodiment of the present invention includes a policy service entity, an SGSN and multiple user terminals. The policy service entity is connected to the SGSN directly or through a network, and configured to determine security policies. The policy service entity may interact with the user terminals through the SGSN, obtain the security-relevant configuration information of the user terminals, determine appropriate security policies for different user terminals based on the security-relevant configuration information of the user terminals and the security policy information stored in the policy service entity, and distribute the determined security policies to the user terminals or the SGSN. The policy service entity may store the security policy information issued by a core network device, or directly stores the configured security policy information.

[0017] The policy service entity may be an independent policy server, or a function module in a network entity such as SGSN, or a card equipped with the policy management function and inserted into an SGSN. The user terminal may be the mobile intelligent terminal or the portable terminal with card slot, or any other mobile terminals capable of interacting with the policy service entity to exchange security information.

[0018] To interwork with the policy service entity, the user terminal is equipped with a security policy processing module. The security policy processing module is configured to receive instructions from the policy service entity and perform corresponding operations, e.g., when the policy service entity sends a request to the user terminal requiring security-relevant configuration information of the user terminal, the security policy processing module collects, upon the receipt of the request, security-relevant configuration information of the user terminal and reports the security-relevant configuration information to the policy service entity. In this way, the policy service entity may obtain, through the security policy processing module, the security- relevant configuration information of the user terminal, including the version information of the operation system of the user terminal, the information of the anti-virus software of the user terminal and the installation condition of the patch.

[0019] The security policy processing module may also initiatively reports the security-relevant configuration information of the user terminal to the policy service entity at a fixed time, or regularly, or upon any change in the security-relevant configuration information of the user terminal. The security policy processing module may be independent software, thus the user terminal communicating with the policy service entity only needs to install the software. The security policy processing module may also store anti-virus software.

[0020] The policy service entity, connected to the SGSN, stores the security-relevant configuration information of the user terminals. After a security protocol negotiation between the policy service entity and the security policy processing module of the user terminal, i.e., after a mutual-trust relationship on security is established between the policy service entity and the security policy processing module of the user terminal, the policy service entity may send a request to the user terminal requiring to collect security-relevant configuration information of the user terminal. The user terminal reports the security-relevant configuration information, e.g., the information of the anti-virus software, installation information of the patch, etc., to the policy service entity.

[0021] In order to enable the SGSN to control the user terminal according to the requirement of the policy service entity, a security policy processing module interworking with the policy service entity and a protocol used for negotiation with the policy service entity are added into the SGSN. In this way, the SGSN may control the user terminal according to the security policy from the policy service entity, and on the other hand, may provide security policy requirement for the policy service entity. The protocol used for the negotiation between the SGSN and the policy service entity includes the mutually agreed interaction method and message format.

[0022] As shown in Fig. 2, a system for implementing data service security in the mobile communication system in accordance with an embodiment of the present invention includes a policy service entity, a GGSN and multiple user terminals as well as an SGSN, an RNC and a Node B. The policy service entity is connected to the GGSN directly or through the network, configured to determine security policies for the user terminals. The policy service entity may interact with the user terminals through the GGSN, and further through the SGSN, the RNC and the Node B, obtain the security-relevant configuration in-

formation of the user terminals, determine appropriate security policies for different user terminals based on the security-relevant configuration information of the user terminals and the security policy information stored in the policy service entity, and distribute the determined security policies to the user terminals or the GGSN. The policy service entity may store the security policy information issued by a core network device, or directly stores the configured security policy information.

[0023] The policy service entity may be an independent policy server, or a function module in a network entity such as a GGSN, or a card equipped with the policy management function and inserted into the GGSN. The user terminal may be the mobile intelligent terminal or the portable terminal with card slot, or any other mobile terminals capable of interacting with the policy service entity to exchange security information.

[0024] To interwork with the policy service entity, the user terminal is equipped with a security policy processing module. The security policy processing module is configured to receive instructions from the policy service entity and perform corresponding operations, e.g., when the policy service entity sends a request to the user terminal requiring security-relevant configuration information of the user terminal, the security policy processing module collects, upon the receipt of the request, security-relevant configuration information of the user terminal and reports the security-relevant configuration information to the policy service entity. In this way, the policy service entity may obtain, through the security policy processing module, the security- relevant configuration information of the user terminal, including the version information of the operation system of the user terminal, the information of the anti-virus software of the user terminal and the installation condition of the patch.

[0025] The security policy processing module may also initiatively reports the security-relevant configuration information of the user terminal to the policy service entity at a fixed time, or regularly, or upon any change in the security-relevant configuration information of the user terminal. The security policy processing module may be independent software. The user terminal communicating with the policy service entity only needs to install the software; the security policy processing module may also store anti-virus software.

[0026] The policy service entity interacts with the user terminal through the GGSN, SGSN, RNC and Node B, in which the SGSN, RNC and the Node B transmit the interaction information transparently.

[0027] The policy service entity, which is connected to the GGSN, stores the security-relevant configuration information of the user terminals. After a security protocol negotiation between the policy service entity and the security policy processing module of the user terminal, i.e., after a mutual-trust relationship on security is established between the policy service entity and the security policy processing module of the user terminal, the policy service entity may send a request to the user terminal requiring to collect security-relevant configuration information. The user terminal reports security-relevant configuration information, e.g., the information of the anti-virus software, installation information of the patch, etc., to the policy service entity.

[0028] In order to enable the GGSN to control the user terminal according to the requirement of the policy service entity, a security policy processing module interworking with the policy service entity and a protocol used for negotiation with the policy service entity are added into the SGSN. In this way, the GGSN may control the user terminal according to the security policy from the policy service entity, and on the other hand, may provide security policy requirement for the policy service entity. The protocol used for the negotiation between the GGSN and the policy service entity includes the mutually agreed interaction method and message format.

[0029] The GGSN is able to resolve the uplink and downlink IP packets in layer 7 and has a redirection function, therefore, the system provided by an embodiment of the present invention may further include one or more security gateways that are configured to implement different security functions or detect different kinds of viruses. The GGSN may redirect the IP packets to the security gateway for further security detection, e.g., redirects the IP packets to an anti-virus gateway. The anti-virus gateway scans the IP packets and removes viruses in the IP packets, and returns the IP packets to the GGSN, and then sends the IP packets to the public network such as the Internet through the GGSN.

[0030] Similarly, the GGSN may also redirect the IP packets from the public network to the security gateway. The security gateway processes the IP packets, e.g., an anti-virus gateway scans the IP packets, removes the viruses in the IP packets, and returns the IP packets to the GGSN. Then the GGSN transmits the IP packets through the SGSN, the RNC and the Node B to the user terminal such as a mobile terminal. To which security gateway the GGSN send the IP packets is decided according to the security policy determined by the policy service entity. For example, provided there are three security gateways in a network, each of them is in charge of IP packets from different IP addresses respectively, the policy service entity may determine that the IP packets with addresses from 10.10.10.0 to 10.10.10.256 shall be redirected to the first security gateway for security detection.

[0031] In the system shown in Fig. 2, after receiving the security policy, instead of executing the security policy, the GGSN may send relevant security policy control information, e.g., deactivate information, to the SGSN or the RNC, the SGSN or the RNC implements corresponding operation. In addition, the policy service entity may also be connected to the SGSN directly to perform unidirectional control, since the SGSN cannot resolve the IP packets, the SGSN may only implement simple security policies, e.g., block the user terminal of a certain IP address.

[0032] Based on the systems shown in Fig.1 and Fig. 2, the method provided by an embodiment of the present invention is shown in Fig. 3, in which the policy service entity is a policy server, the SGSN and the GGSN are generally referred to packet service support node. The method includes the steps of:

Step 301: the policy server sends a request to a user terminal, requiring the user terminal to report the security-relevant configuration information of the user terminal. The user terminal may be a mobile intelligent terminal or a portable terminal with card slot.

In this step, the request may be initiated by the policy server at any time, and be transmitted to the user terminal through the SGSN transparently. The request includes an indicator indicating the required information, e.g., indicating the user terminal to report the installation information of the patch. The format of the request may be determined through negotiation between the policy server and the user terminal. For example, different fields in the request may represent different types of information required by the policy server.

Step 302: upon the receipt of the request from the policy server, the user terminal collects security-relevant configuration information of the user terminal through the security policy processing module in the user terminal according to the requirement of the policy server, and reports the security-relevant configuration information collected to the policy server.

Step 303: after receiving the security-relevant configuration information of the user terminal, the policy server determines user control information for the user terminal according to the security-relevant configuration information of the user terminal and the security policy information stored in the policy server, then the policy server sends the user control information as a security policy to the packet service support node and/or the user terminal.

The security policy information stored in the policy server includes: information of the patch that should be installed on the user terminal, information of the anti-virus software that should be installed on the user terminal, etc. The packet service support node may be a GGSN, or an SGSN, or a PDSN.

Step 304: upon the receipt of the security policy, the packet service support node and/or the user terminal performs a corresponding control operation according to the requirement of the policy server. For example, if the security policy is to scan for a certain virus in the data from a certain user terminal, the GGSN may send, upon the receipt of the data to or from the IP address of the user terminal, the data to a designated security gateway for virus scan; or the GGSN transmits the data of the user terminal through a designated security gateway.

[0033] In the system shown in Fig. 1, the policy server sends the security policy to the SGSN, and the SGSN performs corresponding control operation according to the security policy received. In the system shown in Fig. 2, the policy server sends the security policy to the GGSN, the GGSN performs corresponding control operation according to the security policy received or notifies the SGSN to perform corresponding operation, e.g., to block the IP packets from the user terminal with certain IP address.

[0034] The GGSN may also redirect designated uplink and downlink IP packets to a security gateway for corresponding security process, e.g., virus scan. After the security process, the security gateway returns the IP packets to the GGSN for subsequent transmission and process.

[0035] The packet service support node may send a policy request to the policy server, and the policy server executes steps 301 to 304 upon the receipt of the policy request. The user terminal may also initiatively report the security-relevant configuration information of the user terminal to the policy server, and the policy server executes steps 303 and 304 upon the receipt of the security-relevant configuration information. The user terminal may report the security-relevant configuration information regularly, or at a fixed time, or upon any change in the security-relevant configuration information of the user terminal.

[0036] The policy service entity may, in the form of a card, be integrated into the packet service support node, such as the GGSN or the SGSN, to provide corresponding security service.

[0037] In the embodiments of the present invention, through the determination of the security policy by the policy service entity, the security condition of the user terminal may be detected on the network side, and the security threat information or potential threat will be reported to the policy service entity. The policy service entity determines a corresponding security policy for the user terminal through a verification and selection process, and the spread of the threat may be further controlled by the packet service support node.

[0038] Another embodiment of the present invention is described herein, demonstrating an example of patch installation management. Many damages caused by worms, such as worm.Blaster and worm.Sasser are also the result of not installing corresponding patches on the user terminal in time. The method provided by the present invention may prevent the virus from attacking the network.

[0039] In this embodiment, the packet service support node is an SGSN; the policy service entity is a policy server which stores the information of all patches that should be installed and relative information of each patch,

e.g., the importance of each patch. The security-relevant configuration information of the user terminal is the installation information of the patch. In this embodiment, the method includes the steps of:

1) the policy server sends a request to the user terminal M, requiring the user terminal M to return the security-relevant configuration information of the operation system patch of the user terminal M;

2) upon the receipt of the request, the user terminal M obtains the information of the patch that has been installed in the operation system of the user terminal M through the security policy processing module of the user terminal M, and sends the security-relevant configuration information of the operation system patch to the policy server;

3) upon the receipt of the security-relevant configuration information of the operation system patch of the user terminal M, the policy server verifies the operation system patch installation condition of the user terminal M based on the security-relevant configuration information of the operation system patch from the user terminal M and the information stored in the policy server of all patches that should be installed, and finds out that an important patch has not been installed on the user terminal M, e.g., at least four patches, A, B, C and D, should be installed on each user terminal to ensure the basic security of the user terminals, while the user terminal M has only installed A, C and D without installing B;

4) the policy server sends a notification to the user terminal M, informing the user terminal M that a patch has not been installed, e.g., informing the user terminal M that patch B has not been installed; the policy server determines a security policy based on current information obtained, e.g., determines to restrict the bandwidth of the user terminal M and sends a bandwidth restriction message to the SGSN to restrict the bandwidth of the user terminal M;

5) upon the receipt of the bandwidth restriction message, the SGSN applies the bandwidth restriction to the user terminal M, or even blocks the network connection of the user terminal M.

[0040] And the user terminal M may determine whether to install the patch B according to the notification described in step 4).

[0041] In the fore-going example of the patch installation management, if the packet service support node is a GGSN, when the data packets from the user terminal M are transmitted to the GGSN, the GGSN may redirect the data packets received to the security gateway, such as an anti-virus gateway, for corresponding security examination to remove virus, and then the anti-virus gateway returns the data packets to the GGSN.

[0042] The policy service entity may be an independent implementing data service security apparatus in the mobile communication system. As shown in Fig. 4, the apparatus includes a security information obtaining module, a security policy determination module, a security policy storage module and a security policy distribution module.

[0043] The security information obtaining module communicates with the user terminal, obtains the security-relevant configuration information of the user terminal through interaction with the user terminal and sends the security-relevant configuration information obtained to the security policy determination module;

the security policy determination module is configured to determine a security policy based on the obtained security-relevant configuration information of the user terminal and the security policy information stored in the security policy storage module, and send the security policy determined to the security policy distribution module for distribution;

the security policy storage module is configured to store security policy information of the user terminals; and

the security policy distribution module is configured to send the security policy received to designated network entities, such as a user terminal, SGSN or GGSN.

[0044] The security information obtaining module may also be connected directly to the security policy storage module and store the security-relevant configuration information obtained as security policy information. The security policy storage module may also be connected to an external device such as a core network device and directly obtain and store the security policy information configured by the external device; and the security policy storage module may obtain security policy information configured by a configuration command through a man-machine interface.

[0045] The present invention may be applicable to 2G GPRS system, Enhanced Data rates for GSM Evolution (EDGE) system and 3G Wideband Code Division Multiple Access (WCDMA) system, Time Division-Synchronization Code Division Multiple Access (TD-SCDMA) system and Code Division Multiple Access (CDMA) 2000 system. The fore-going is only the preferred embodiments of the present invention and is not for use in limiting the protection scope thereof.

Claims

1. A method for implementing data service security in a mobile communication system, comprising:

obtaining security-relevant configuration information of a user terminal;

determining a security policy for the user terminal based on the security-relevant configuration information of the user terminal and security poli-

icy information stored, and sending the security policy determined to a packet service support node and/or the user terminal;
upon the receipt of the security policy, implementing, by the packet service support node and/or the user terminal, a control process based on the security policy.

2. The method of claim 1, wherein the process of obtaining security-relevant configuration information of a user terminal comprises:

reporting initiatively, by the user terminal, the security-relevant configuration information currently collected of the user terminal.

3. The method of claim 2, wherein the user terminal reports the security-relevant configuration information of the user terminal to the policy service entity at a fixed time, or regularly, or upon any change in the security-relevant configuration information of the user terminal.

4. The method of claim 1, wherein the process of obtaining security-relevant configuration information of a user terminal comprises:

sending a request to the user terminal, requiring the user terminal to report the security-relevant configuration information;
upon the receipt of the request, collecting, by the user terminal, the security-relevant configuration information of the user terminal based on the request, and reporting the security-relevant configuration information collected.

5. The method of claim 4, further comprising:

before sending a request to the user terminal requiring the user terminal to report the security-relevant configuration information, sending, by the packet service support node, a policy request; and
upon the receipt of the policy request, sending the request to the user terminal, requiring the user terminal to report the security-relevant configuration information to the user terminal.

6. The method of any one of claims 1 to 5, wherein the security-relevant configuration information of the user terminal comprises at least one of: version information of the operation system of the user terminal, information of anti-virus software of the user terminal and installation condition of a patch.

7. The method of any one of claims 1 to 5, wherein the policy service entity is any one of: an independent policy server, a function module in a network device, and a card equipped with a policy management function.

8. The method of any one of claims 1 to 5, wherein the packet service support node is any one of: a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN), and a Packet Data Support Node (PDSN).

9. The method of any one of claims 1 to 5, wherein the user terminal is any one of: a mobile intelligent terminal and a portable terminal with cardslot.

10. The method of claim 1, wherein the packet service support node is a GGSN, the process of the packet service support node and/or the user terminal implementing a control process based on the security policy further comprising:

upon the receipt of the security policy, notifying, by the GGSN, a SGSN or a Radio Network Controller (RNC) to implement the control process based on the security policy.

11. The method of claim 1, wherein the packet service support node is a GGSN, the method further comprising:

redirecting, by the GGSN, received data packets to a security gateway for security processing; and
returning, by the security gateway, the data packets to the GGSN after the security processing.

12. The method of claim 11, wherein the security gateway is an anti-virus gateway, and the security processing comprises: scanning the received data packets for virus and removing the virus.

13. A system for implementing data service security in a mobile communication system, comprising:

a packet service support node;
a user terminal, communicating with the packet service support node through the mobile communication network;
a policy service entity, connected to the packet service support node, and configured to obtain security-relevant configuration information of the user terminal, determine a security policy for the user terminal and distribute the security policy to the packet service support node and/or the user terminal;
the user terminal and the packet service support node are respectively equipped with a security policy processing module communicating with the policy service entity, the security policy

processing module is configured to receive an instruction from the policy service entity, implement corresponding process and/or sending of security-relevant configuration information to the policy service entity based on the instruction.

14. The system of claim 13, further comprising:

a security gateway, configured to implement a security process on data packets which are redirected to the security gateway by the packet service support node.

15. The system of claim 14, wherein the security gateway is an anti-virus gateway.

16. The system of claims 13, 14 or 15, wherein the packet service support node is any one of: a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN), and a Packet Data Support Node (PDSN).

17. The system of claim 13, 14 or 15, wherein the policy service entity is any one of: an independent policy server, a function module in a network device, and a card equipped with a policy management function.

18. The system of any one of claims 13 to 16, wherein the packet service support node is any one of: a Serving GPRS Support Node (SGSN), a Gateway GPRS Support Node (GGSN), and a Packet Data Support Node (PDSN).

19. The system of claim 13, 14 or 15, wherein the user terminal is any one of: a mobile intelligent terminal and a portable terminal with card slot.

20. An apparatus for implementing data service security in a mobile communication system, comprising:

a security information obtaining module, configured to communicate with a user terminal, obtain security-relevant configuration information of the user terminal and send the security-relevant configuration information obtained to a security policy determination module;
the security policy determination module, configured to determine a security policy according to the security-relevant configuration information and security policy information stored in a security policy storage module, and send the security policy determined to a security policy distribution module;
the security policy storage module, configured to store the security policy information;
the security policy distribution module, configured to send the security policy received to a designated network entity.

21. The apparatus of claim 20, wherein the security information obtaining module is further connected to the security policy storage module.

22. The apparatus of claim 20, wherein the security policy storage module is further configured to receive and store security policy information configured by an external device and/or a configuration command.

23. The apparatus of claim 20, 21 or 22, wherein the designated network entity comprises at least one of: a user terminal, a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN).

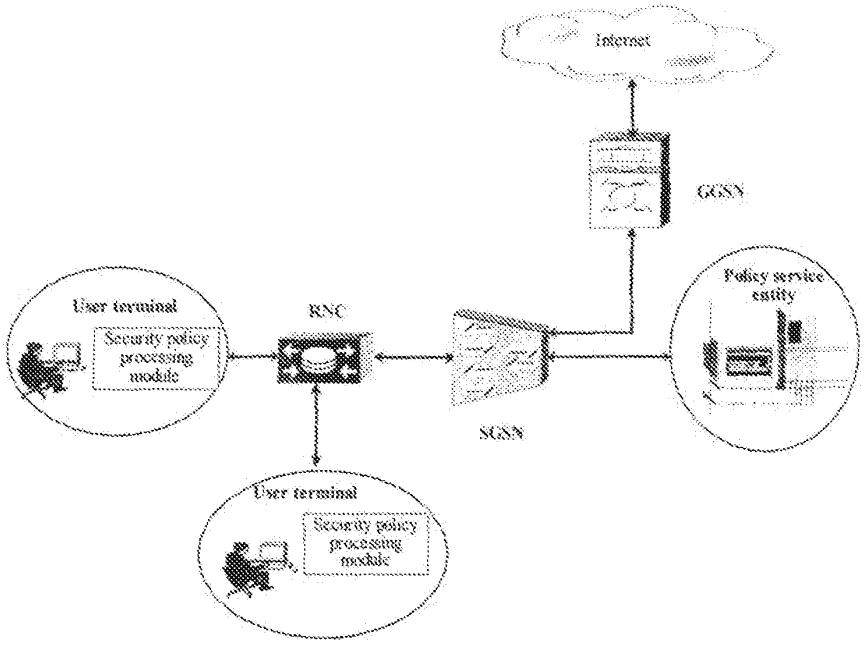

Internet
GGSN
Policy service entity
User terminal
Security policy processing module
RNC
SGSN
User terminal
Security policy processing module

Fig. 1

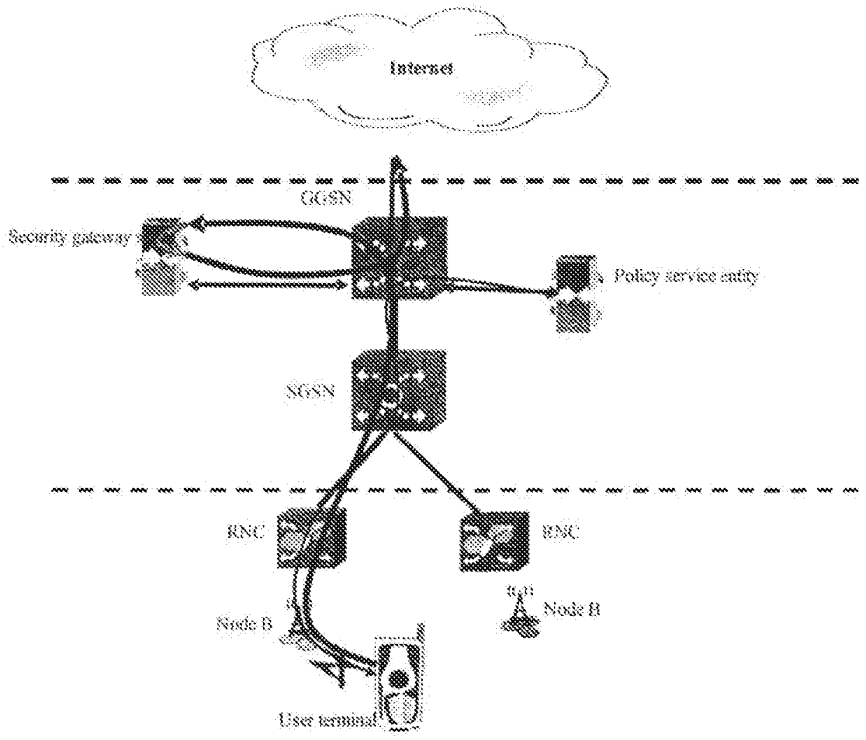

Internet
GGSN
Security gateway
Policy service entity
SGSN
RNC
RNC
Node B
Node B
User terminal

Fig. 2

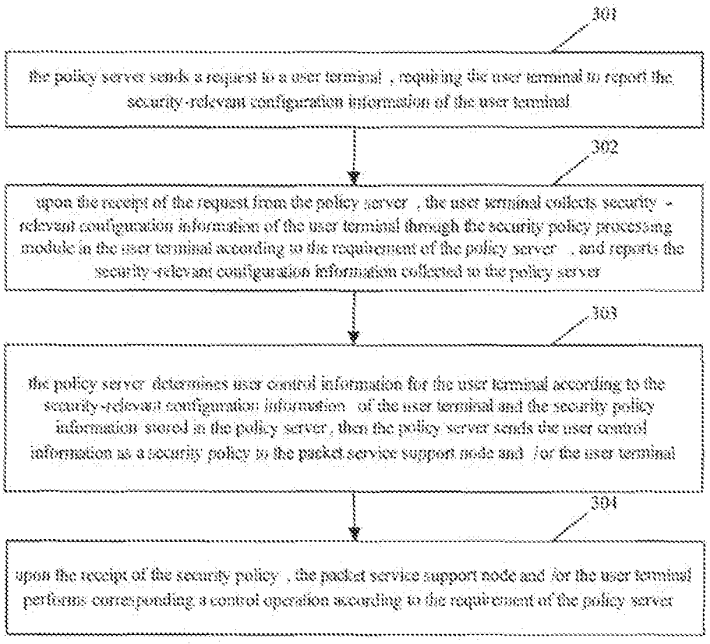

301
the policy server sends a request to a user terminal , requiring the user terminal to report the security-relevant configuration information of the user terminal
302
upon the receipt of the request from the policy server , the user terminal collects security - relevant configuration information of the user terminal through the security policy processing module in the user terminal according to the requirement of the policy server , and reports the security-relevant configuration information collected to the policy server
303
the policy server determines user control information for the user terminal according to the security-relevant configuration information of the user terminal and the security policy information stored in the policy server , then the policy server sends the user control information as a security policy to the packet service support node and /or the user terminal
304
upon the receipt of the security policy , the packet service support node and /or the user terminal performs corresponding control operation according to the requirement of the policy server

Fig. 3

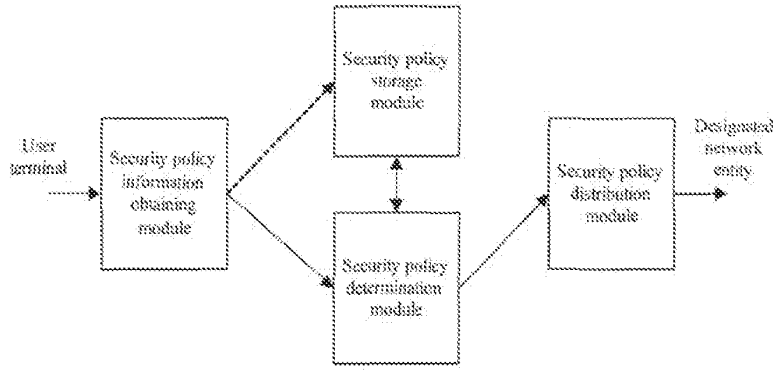

User terminal
Security policy information obtaining module
Security policy storage module
Security policy determination module
Security policy distribution module
Designated network entity

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/002254

A. CLASSIFICATION OF SUBJECT MATTER

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)

H04L, H04Q

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: safety, security, virus, bug, mobile, cellular, radio, wireless

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP, A2, 1443379 (CURITEL CORP) 4 Aug. 2004 (04.08.2004), the whole document.	1-23
A	EP, A2, 1329790 (NTT DOCOMO INC) 23 Jul. 2003 (23.07.2003), the whole document.	1-23
A	WO, A2, 2004057834 (SENFORCE TECHNOLOGIES INC) 8 Jul. 2004 (08.07.2004), the whole document.	1-23

☐ 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
15 Mar. 2006 (15.03.2006)	30 MAR 2006 (30.03.2006)
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) 62084529

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2005/002254

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
EP1443379A2	04.08.2004	KR2004059328 A	05.07.2004
		US2004127195 A1	01.07.2004
		CN1512798 A	14.07.2004
EP1329790A2	23.07.2003	CN1433243 A	30.07.2003
		US2003154409 A1	14.08.2003
		JP2003216448 A	31.07.2003
WO2004057834A2	08.07.2004	AU2003299729 A1	14.07.2004
		US2004123153 A	24.06.2004
		US2004123130 A	24.06.2004
		US2005055578 A	10.03.2005

Form PCT/ISA/210 (patent family annex) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/002254

CLASSIFICATION OF SUBJECT MATTER

H04L 9/36（2006.01）i
H04Q 7/20 （2006.01）n

Form PCT/ISA /210 (extra sheet) (April 2005)

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

(11) EP 1 978 772 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.10.2008 Bulletin 2008/41

(51) Int Cl.:
H04Q 7/38 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(21) Application number: **07251454.0**

(22) Date of filing: **02.04.2007**

(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
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **British Telecommunications Public Limited Company**
London
EC1A 7AJ (GB)

(72) Inventor: **The designation of the inventor has not yet been filed**

(74) Representative: **Sayer, Robert David et al**
BT Group Legal
Intellectual Property Department
PP C5A
BT Centre
81 Newgate Street
London EC1A 7AJ (GB)

(54) Authentication policy

(57) A method of managing an authentication policy in a mobile telecommunications device, wherein the mobile telecommunications device comprises a plurality of security module applications, said method comprising the steps of: providing a profile associated with each of the plurality of security module applications, wherein each profile identifies at least one network with which the associated security module application can be used to enable communications; generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications; and determining, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

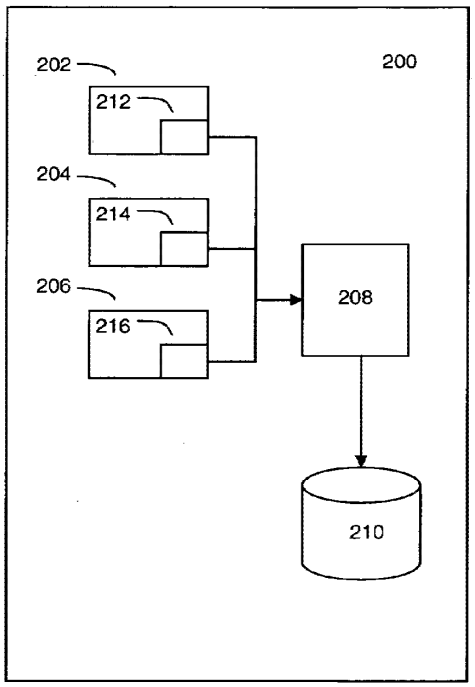


Figure 2

EP 1 978 772 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to a method of managing security modules in mobile devices, in particular a method of managing network authentication profiles in multiple security modules for connecting to multiple networks.

Background to the Invention

[0002] Provision of communications services in mobile cellular networks, such as GSM and UMTS, are based upon a key sharing principle, where a secure smart card, a SIM (subscriber identity module), is used in a mobile device to store subscriber details, applications as well as an authentication key. Specifically, the subscriber details are stored in a SIM application resident on the SIM card and include an international mobile subscriber identity (IMSI), an authentication key Ki, as well as various operator secrets and other applications for handling authentication and encryption of communications data.

[0003] The SIM application is thus the core element that enables network identification i.e. it enables network operators to identify and subsequently authenticate a subscriber. In addition to the subscriber details and authentication keys used for identification and authentication, also programmed into the SIM application are the network operator's Mobile Country Code (MCC) and Mobile Network Code (MNC). These provide a reference to the network operator with which the SIM card can be used. Usually, the SIM application has a list of "preferred networks" with which it can connect, listing the MNC associated with each of the "preferred networks". Also commonly found is a list of "barred networks" with lists all the MNCs with which a SIM application should never be used with.

[0004] When the mobile device is switched on, the device scans the MNC list stored on the SIM application and at the same time scans all the GSM frequency bands the device can receive. Any networks operating in the area of the mobile device will be broadcasting their MNC over a broadcast channel. The mobile device determines all the available networks broadcasting in the area and attempts to connect to the MNC highest up on the preferred networks list. This is usually the MNC corresponding to home network of the SIM application i.e. the network belonging to the network operator that issued the SIM card.

[0005] The other MNCs on the preferred network list usually relate to other network operators for use when the subscriber "roams" in a different country for example.

[0006] Whilst a user can usually swap SIM cards in and out of a device to give access to multiple networks, there are no provisions to manage multiple simultaneously active SIM cards in a single device. In particular, existing solutions are based on the fact that there is only one active SIM in a device at any given time. Furthermore, the SIM functionality provided by a SIM card is actually provided for by the SIM application. In practice, there can also be multiple SIM applications resident on a single card, each capable of providing network access to different networks and supporting distinct applications. These multiple SIM applications, either on a single SIM card or across multiple SIM cards, need to be managed efficiently in order for services to be delivered to the user effectively, in particular in relation to access to different networks.

Summary of the Invention

[0007] It is the aim of embodiments of the present invention to address one or more of the above-stated problems.

[0008] According to a first aspect of the present invention, there is provided a method of managing an authentication policy in a mobile telecommunications device, wherein the mobile telecommunications device comprises a plurality of security module applications, said method comprising the steps of:

i) providing a profile associated with each of the plurality of security module applications, wherein each profile identifies at least one network with which the associated security module application can be used to enable communications;

ii) generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications;

iii) determining, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

[0009] The security module applications may be subscriber identity module, or SIM applications, and the SIM applications may be located on a SIM card.

[0010] The profiles in the security module applications can identify a list of preferred networks with which the security module application is able to operate. These identified networks are listed by a network type element and a network identifier element. For example, the network type may be GSM, and the network identifier may be the mobile network code (MNC) of the particular GSM network.

[0011] Preferably, the network broadcasts a network identifier and the mobile telecommunications device uses the network identifier to identify the network.

[0012] The profiles may be stored with the associated security module application, and preferably on a SIM card.

[0013] Preferably, the step of generating comprises combining each of the profiles and adding to each network identified in each profile the application identifier corresponding to security module application associated with the profile.

[0014] According to a second aspect of the present invention, there is provided a mobile telecommunications device comprising a plurality of security module applications, wherein each security module application is providing with a profile and each profile identifies at least one network with which the associated security module application can be used to enable communications, said mobile telecommunications device further comprising:

> a processor for generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications; and wherein said mobile device is adapted to determine, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

[0015] As the mobile device has several network connection means allowing connection to several networks at the same time (e.g. GSM, WiFi, Bluetooth), the ability to effectively and conveniently manage such connectivity is very important.

[0016] By having a device that can accept several SIM cards, or more particularly to manage several simultaneously active SIM applications in the device at the same time, authentication and connectivity to different networks at the same time is possible.

[0017] Furthermore, SIM cards and SIM applications from different operators that are potentially competing on the marketplace can co-exist within a single device for the benefit of the user.

[0018] The device can also implement a 'best connected' policy for optimising connectivity so that it is always connected in a manner that is beneficial for the user. Such a policy can be fully automated and does not require any intervention for the user, thus improving usability and delivering true seamless roaming experience.

[0019] Embodiments of the present invention also allow for SIM cards and SIM applications implemented in the device in different formats (e.g. on a standard SIM card, in software only, within some other trusted hardware module, on memory card), thus increasing flexibility of operator's provisioning methods.

Brief Description of the Drawings

[0020] For a better understanding of the present invention reference will now be made by way of example only to the accompanying drawings, in which:

> Figure 1 is a simplified diagram of a SIM card showing two separate SIM applications in an embodiment of the present invention;
> Figure 2 is a diagram showing a mobile device and a plurality of SIM applications and their associated profile files in an embodiment of the present invention;
> Figure 3 is a table showing the format of an authentication policy in an embodiment of the present invention;
> Figure 4 is a network diagram showing an arrangement in which an embodiment of the present invention can be utilised with three different networks.

Description of the Preferred Embodiments

[0021] The present invention is described herein with reference to particular examples. The invention is not, however, limited to such examples.

[0022] Figure 1 shows a SIM card 100 holding two SIM applications, SIM_app_1 102 and SIM_app_2 104. Each SIM application holds separate subscriber details such as an IMSI, authentication key Ki, and other unique parameters. Each SIM application is also provided with an authentication profile file. SIM_app_1 102 includes authentication profile file 106 and SIM_app_2 includes authentication profile 108.

[0023] Each of the authentication profile files list details of the network type and network ID that the corresponding SIM application can be used in. The network type details the type of network the SIM can be used in such as a GSM network, a WiFi network or a Bluetooth network. The network type can be specified by name or preferably by the broadcast frequency or frequency band of the network. The network ID uniquely identifies the specific network within the network type or frequency band. For example, the network ID may be specified by the mobile network code (MNC) if the network type is a GSM network, or the network ID may be a service set identifier (SSID) if the network type is a WiFi network.

[0024] Figure 2 shows a mobile device 200, such as a smart phone, having multiple network access means. The mobile device 200 can access the various communications networks such as GSM mobile networks, WiFi network and also has Bluetooth access. Mobile device 200 also includes two SIM cards. The SIM cards are not shown in the Figure, but the SIM applications that are resident on the SIM cards are shown. In this example, the first SIM card (not shown) holds two SIM applications, which are shown as SIM_A_1 202 and SIM_A_2 204. The first SIM card may be issued by network operator A, and the associated SIM applications are enabled for use with networks controlled by network operator A.

[0025] The other SIM card (not shown) has only one SIM application, SIM_B_1 206. The other SIM card may be issued by network operator B, and the SIm application

therein for use with networks run by network operator B.

[0026] Each SIM application also has a corresponding authentication profile file. SIM_A_1 202 has authentication profile file File_A_1 212, SIM_A_2 204 has authentication profile file File_A_2 214 and SIM_B_1 206 has authentication profile file File_B_1 216. The authentication profile file includes a list of networks that the SIM application can be used with, where the network is specified by a network type field and a network ID field as described in relation to Figure 1 above.

[0027] In this example, File_A_1 212 has entries for one network identified by "GSM 900, MNC 200", where GSM 900 is the network type and MNC 200 is the network ID, and similarly another network identified by "WiFi, SSID 1111". File_A_2 214 has entries for the network "WiFi, SSID 1111". File_B_1 216 has entries for "GSM 1800, MNC 300".

[0028] The mobile device 200 also includes a processor 208 for handling the SIM applications and processing the authentication profile files. When the mobile device 200 is first switched on, the processor detects the presence of the different SIM applications and starts reading the authentication profile files. The processor 208 then takes the details of the networks listed in the authentication profile file and generates an authentication policy table 300 as shown in Figure 3.

[0029] The authentication policy table 300 has a network_type field 302, a network_ID field 304 and a SIM_app field 306. Four entries 308, 310, 312 and 314 are shown in the policy table 300 based on the entries from the authentication profile files collected from the SIM applications by the processor 208. Each entry includes the network type and network_ID as taken from the individual authentication profile files 212, 214 and 216. Also included in each entry is a reference to the SIM application to which the entry corresponds under the SIM_app field 306.

[0030] The authentication policy table 300 is stored locally on the mobile device in data store 210, such as RAM or flash memory, and is used by the mobile device 200 to automatically determine which SIM application to use for a network connection.

[0031] Figure 4 shows a network arrangement 400 including a mobile device 200 loaded with the SIM applications and authentication policy table 300 described above. Figure 4 shows 3 different networks: a GSM network 402, another GSM network 404 and a WiFi network 406. After the mobile device 200 has been activated and generated the authentication policy table 300 as described above, the mobile device starts scanning for the available networks. The mobile device 200 detects GSM network 402, GSM network 404 and WiFi network 406. The mobile device then scans each of these networks further to determine the network type and/or the network ID. In many cases the network type is automatically determined depending on which receiver the mobile device 200 has used to scan for networks e.g. network 402 is detected using a GSM receiver in the mobile device 200 and thus is automatically determined as a GSM network.

[0032] The network ID associated with each network may be broadcasted over a general broadcast channel that can be received by the mobile device 200 or any similar device equipped with a suitable receiver. In this example, the GSM network 402 is identified as having a network ID (in this case a mobile network code MNC) of 200. Similarly, the GSM network 404 is identified as having a network ID of 300. The mobile device 200 also scans the WiFi channels of WiFi network 406 and determines that the network ID, the SSID of the router, is 1111.

[0033] The processor 208 in the mobile device 200 then uses the authentication profile table 300 to determine which SIM application it should use to connect to which network. The processor 208 determines that GSM network 402 with a network ID of 200 can only be connected to using SIM application SIM_A_1 (see 308 of Figure 3) which is associated with the same network type and identifier. The processor 208 also determines that GSM network 404 with a network ID of 200 can only be connected to using SIM application SIM_B_1 (see 310 of Figure 3) which is associated with the same network type and identifier. However, for WiFi network 406 which has a network ID of 1111, either SIM application SIM_A_1 or SIM_A_2 can be used to connect. In such cases, the processor 208 can employ a suitable resolution method, for example giving priority to one of the applications which the user has previously defined as being the preferred application.

[0034] In practice, it may also only be possible to connect to one network of any one type at a time, due to limitations on receivers unless the mobile device 200 includes more than one receiver. So in this example, the mobile device 200 can only connect to one of the GSM networks 402 or 404 at any given time. The determination of which one to connect to can be resolved again by providing a priority to the SIM applications and network IDs. Assuming that each network ID for each SIM application is given a priority, then in the event of any conflict in network type where the device can only connect to one network of a given network type, or if there is a conflict between SIM applications for a given network, then the priority is used to determine which network or SIM application to use in each respective situation. The priorities can be represented in the authentication policy table by the order in which the entries are listed.

[0035] After the mobile device 200 has used the authentication policy table 300 to determine that SIM application SIM_A_1 should be used to connect to the GSM network 402, the mobile device can use the subscriber details, such as the IMSI, stored on SIM_A_1 to register and authenticate with the network 402. The process of authentication will include verification of the SIM application where the network 402 issues a challenge to the authentication key Ki stored at the SIM application. The response generated by the SIM application is checked against a response generated by the network based on a copy of the authentication key Ki stored in the network.

[0036] The authentication profile file associated with each SIM application can be preloaded with the preferred network details when the SIM card is loaded with the SIM applications during manufacture. Furthermore, the authentication profile file can be modified by the network operator over the network to add or delete network details.

[0037] More complex policies that include e.g. a history of connections, presence of other networks, availability of billing information or current time can be deployed as well. Specifically, policies that are used to determine the selection of the network can be remotely updated, independently from the update of authentication profile files.

[0038] In general, it is noted herein that while the above describes examples of the invention, there are several variations and modifications which may be made to the described examples without departing from the scope of the present invention as defined in the appended claims. One skilled in the art will recognise modifications to the described examples.

Claims

1. A method of managing an authentication policy in a mobile telecommunications device, wherein the mobile telecommunications device comprises a plurality of security module applications, said method comprising the steps of:

   i) providing a profile associated with each of the plurality of security module applications, wherein each profile identifies at least one network with which the associated security module application can be used to enable communications;
   ii) generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications;
   iii) determining, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

2. A method according to claim 1, wherein each network identified in the profiles comprises a network type element and a network identifier element.

3. A method according to claim 1 or claim 2, wherein each security module application is a subscriber identity module application.

4. A method as claimed in any preceding claim, wherein the mobile telecommunications device uses a network identifier broadcast by the network to identify the network.

5. A method as claimed in any preceding claim, wherein each profile is stored with the associated security module application.

6. A method as claimed in any preceding claim, wherein the step of generating comprises combining each of the profiles and adding to each network identified in each profile the application identifier corresponding to security module application associated with the profile.

7. A method as claimed in any preceding claim wherein the security module application is located on a tamper proof security module.

8. A method as claimed in claim 7, wherein the tamper-proof security module is a subscriber identity module.

9. A mobile telecommunications device comprising a plurality of security module applications, wherein each security module application is providing with a profile and each profile identifies at least one network with which the associated security module application can be used to enable communications, said mobile telecommunications device further comprising:

   a processor for generating an authentication table based on the plurality of profiles provided, wherein said authentication table specifies each of the networks identified in the profiles provided and associates with each of the networks identified an application identifier, wherein each application identifier corresponds to one of the security module applications; and wherein said mobile device is adapted to determine, based on the authentication table, one of the plurality of security module applications to use to enable communications with a network identified by the mobile telecommunications device.

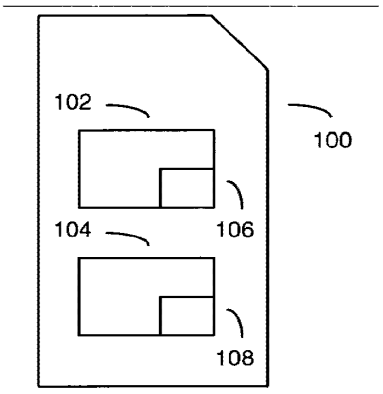


Figure 1

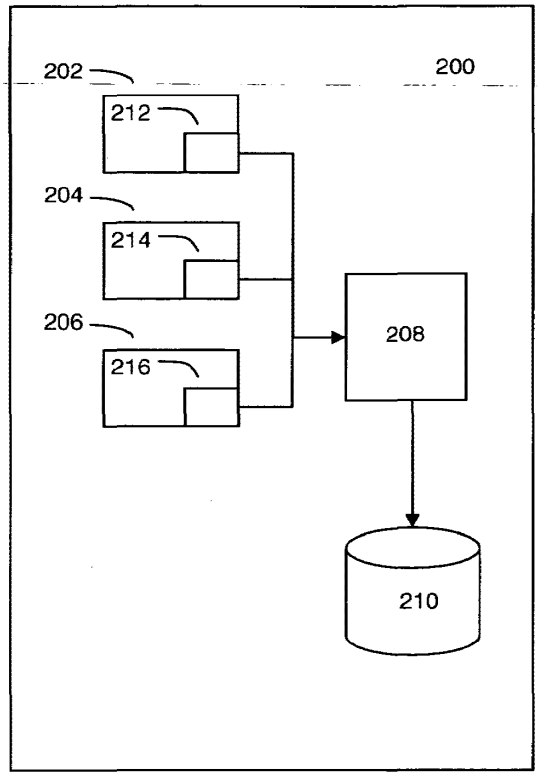


Figure 2

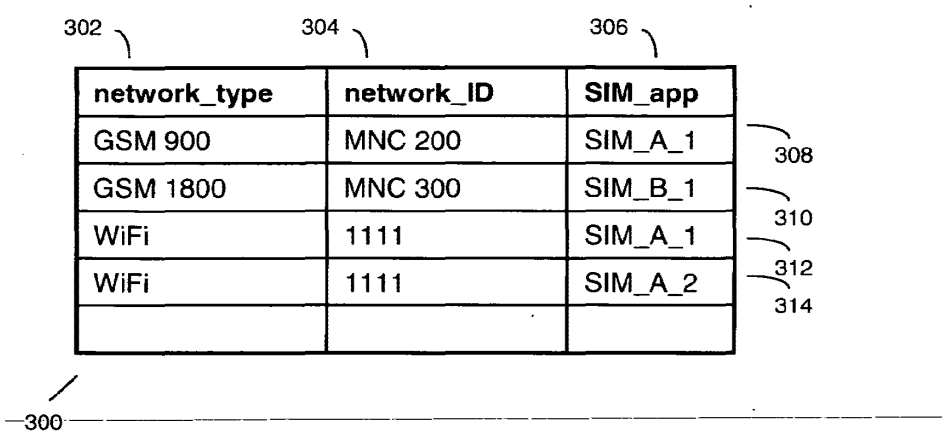


Figure 3

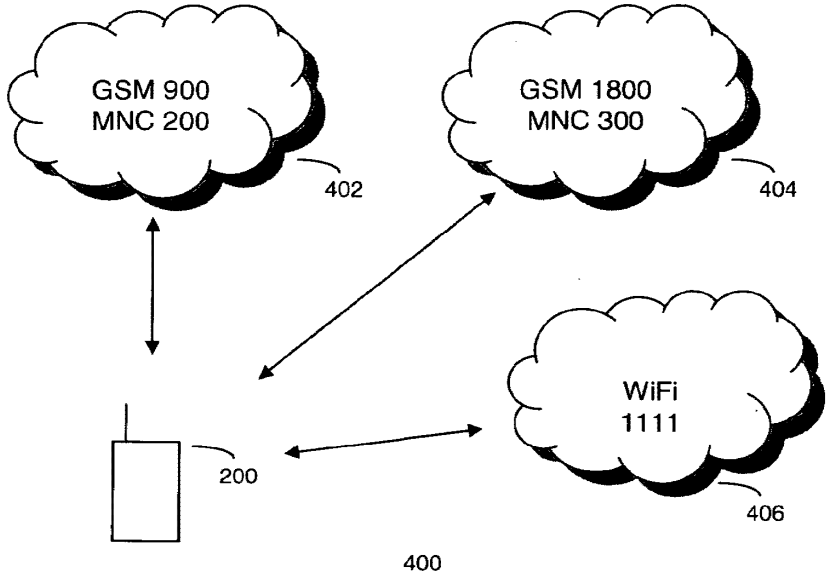


Figure 4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 25 1454

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	EP 1 513 358 A (RES IN MOTION LTD [CA]) 9 March 2005 (2005-03-09) * abstract * * paragraph [0003] * * paragraph [0008] - paragraph [0009] * * paragraph [0016] - paragraph [0018] * * paragraph [0044] - paragraph [0045] * * paragraph [0047] * * paragraph [0051] - paragraph [0054] * * claims 1-3,8-10 * * figures 4,5,7 * -----	1-9	INV. H04Q7/38 H04L29/06
X	US 2004/022216 A1 (SHI GUANGMING CARL [US]) 5 February 2004 (2004-02-05) * abstract * * paragraph [0007] - paragraph [0008] * * paragraph [0010] - paragraph [0014] * * paragraph [0024] - paragraph [0026] * * paragraph [0028] - paragraph [0031] * * paragraph [0035] * * paragraph [0040] - paragraph [0041] * * paragraph [0047] - paragraph [0049] * * paragraph [0085] - paragraph [0106] * * figures 1,2,5 * -----	1-9	TECHNICAL FIELDS SEARCHED (IPC) H04L H04Q
X	WO 03/100647 A (RUSSELL JESSE E [US]) 4 December 2003 (2003-12-04) * abstract * * page 1 - page 6 * * page 9 - page 13 * * page 15 - page 19 * * claims 1,16,25 * * figures 1,2B,2C,2D,2E * ----- -/--	1-9	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	29 November 2007	Kopp, Klaus

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 07 25 1454

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	GB 2 395 867 A (ORANGE PERSONAL COMM SERV LTD [GB]; ORANGE SA [FR]) 2 June 2004 (2004-06-02) * abstract * * figure 3 * * page 1, line 13 - line 19 * * page 2, line 8 - line 15 * * page 8, line 14 - page 11, line 3 *	1-9	
X	WO 2006/138338 A (QUALCOMM INC [US]; KHANDELWAL DEEPAK [US]; JAIKUMAR SELVARAJ [US]; UCH) 28 December 2006 (2006-12-28) * paragraph [0013] * * paragraph [0017] - paragraph [0018] * * paragraph [0028] - paragraph [0029] * * paragraph [0047] - paragraph [0048] * * paragraph [0053] - paragraph [0056] * * figures 2,5,6A,6B *	1-9	
A	DE 101 38 835 A1 (T MOBILE DEUTSCHLAND GMBH [DE]) 27 February 2003 (2003-02-27) * the whole document *	1-9	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	29 November 2007	Kopp, Klaus

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 07 25 1454

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.

29-11-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1513358 A	09-03-2005	AT 356515 T	15-03-2007
		CA 2478008 A1	03-03-2005
		DE 60312326 T2	08-11-2007
		HK 1075996 A1	14-09-2007
		US 2005113088 A1	26-05-2005
US 2004022216 A1	05-02-2004	AU 2003254291 A1	23-02-2004
		CN 1682563 A	12-10-2005
		MX PA05001360 A	27-05-2005
		WO 2004014100 A1	12-02-2004
WO 03100647 A	04-12-2003	AU 2003241592 A1	12-12-2003
		EP 1540499 A1	15-06-2005
GB 2395867 A	02-06-2004	AU 2003302358 A1	18-06-2004
		CN 1717946 A	04-01-2006
		EP 1568243 A1	31-08-2005
		WO 2004049744 A1	10-06-2004
		US 2006217153 A1	28-09-2006
WO 2006138338 A	28-12-2006	US 2006286977 A1	21-12-2006
DE 10138835 A1	27-02-2003	NONE	

EPO FORM P0459

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

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2007 (10.05.2007)

PCT

(10) International Publication Number
WO 2007/053848 A1

(51) International Patent Classification:
H04L 12/22 (2006.01)

(21) International Application Number:
PCT/US2006/060446

(22) International Filing Date:
1 November 2006 (01.11.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/732,253	1 November 2005 (01.11.2005)	US
60/732,254	1 November 2005 (01.11.2005)	US
60/732,380	1 November 2005 (01.11.2005)	US
11/381,291	2 May 2006 (02.05.2006)	US

(71) Applicant *(for all designated States except US)*: **MOBILE ARMOR, LLC** [US/US]; 400 South Woods Mill Road, Suite 110, Chesterfield, MO 63017 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GERMANO, Vernon, P.** [US/US]; 154 Whisper Creek Drive, Wentzville, MO 63385 (US). **AYERS, Jeff**; 15616 Fern Creek Drive, Chesterfield, MO 63107 (US).

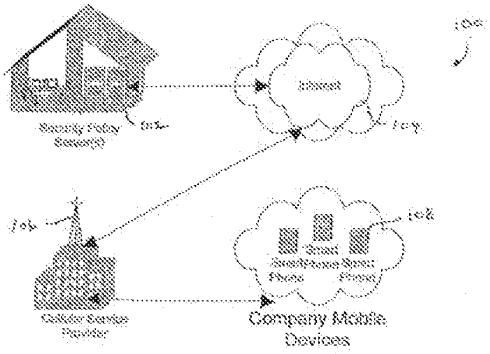
(74) Agents: **TAYLOR, Morgan, M.** et al.; LEWIS, RICE & FINGERSH, L.C., 500 North Broadway, Suite 2000, BOX IP DEPARTMENT, St. Louis, MO 63102 (US).

(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, 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,

[Continued on next page]

(54) Title: CENTRALIZED DYNAMIC SECURITY CONTROL FOR A MOBILE DEVICE NETWORK



(57) Abstract: An security system for an enterprise network and data automates the revision, deployment, enforcement, auditing and control of security policies on mobile devices connected to said enterprise network, through automated communication between a security policy server and the mobile device. Control of the security system is centralized through administrative control of security policies stored on the security policy server. Automation of deployment of security policies to mobile devices occurs through transparent background communication and transfer of updated policies either triggered by a change in a security policy within the central repository of security policies or upon the expiration of a certain time period during which no policies were downloaded to the mobile device. When the mobile device is not in compliance with a security policy, a software security agent operating thereon limits access to said enterprise network and enterprise data. To aid in preventing the overwhelming of the enterprise network and the security policy server as a result of to many synchronization communications coming from too many mobile devices, a randomized timer is set by the software security agent upon receipt by the mobile device of a synchronization command from the security policy server.

WO 2007/053848 A1

BO, 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*

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.

TITLE

Centralized Dynamic Security Control for a Mobile Device Network

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Provisional Patent Applications No. 60/732,380, 60/732,253, and 60/732,254, each of which were filed November 1, 2005, and is a continuation-in-part of and claims priority to US Utility Application No. 11/381,291, filed May 2, 2006. Each of the prior referenced documents is incorporated herein in its entirety by this reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The invention relates to an electronic security system for the protection of enterprise network usage and enterprise data stored on the enterprise network; and more particularly to a system in which a security policy relevant to a mobile device can be centrally managed from a policy server and automatically transmitted to the mobile device.

2. Description of Related Art

[0003] The technology world is a constantly changing environment, with computers gaining power while at the same time continually becoming smaller. Of course these are not the only aspects that change as the digital wizards constantly create new ways to "simplify" our lives with completely new devices to connect us to an increasingly wired and wireless world. Today, laptops, PDAs, and Smart Phones are standard equipment for the mobile corporate environment.

[0004] The basic premise of a mobile computing device ("mobile device") is to either enhance one's working capabilities, or to add convenience with the ultimate goal of increasing productivity. Applications are written for mobile devices allowing them to provide basic, and in many cases complete, functionality when compared to using a desktop computer in the office. Mobile devices are able to store, or at least access, an organization's information. This access requires the implementation of "mobile data security", i.e., security for data accessible through mobile devices.

[0005] Today's mobile devices are powerful computing platforms, capable of storing tremendous amounts of valuable assets, including financial spreadsheets, presentations, employee/customer/patient information, intellectual property, etc.,

which can create serious security risks to the enterprise to which such information belongs or has been entrusted.

[0006] Every year more mobile devices are issued to employees and the percentage of hardware thefts increases respectively. However, the value of the information stolen from those lost devices far exceeds that of the hardware.

[0007] Organizational computer security has traditionally revolved around the concept of a secured perimeter. The idea is to build an impenetrable fence or wall around the organization's internal network and all its data. Traditional security efforts therefore have been focused on enforcing this network boundary security with products such as firewalls, virtual private networks, and anti-virus software. While these safeguards are critical to any computer system, mobile or stationary, this is not the full scope of security necessary for protection.

[0008] The difficulty with security for mobile and wireless devices is that they do not generally reside within the enterprise's primary security installations. Historically, an enterprise has relied in significant part upon the physical isolation of its computing network and its data, and its ability to limit physical access to such an isolated network and data. In particular for mobile devices, however, data is carried outside of the physical boundaries of the enterprise property on mobile devices carried anywhere persons travel, and enterprise network access is gained through network connections that travel through electronic nodes controlled other than by the enterprise. For these reasons, security of data stored on a mobile device and security of data communicated between a mobile device and an enterprise is challenging.

SUMMARY OF THE INVENTION

[0009] The following is a summary of the invention in order to provide a basic understanding of some aspects of the invention. This summary is not intended to identify key or critical elements of the invention or to delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented later.

[0010] A network security system as herein described includes a system and methods for delivering security policies in real time to mobile devices from a security policy server using over-the-air techniques.

[0011] In an embodiment, the security system is for use in aiding in the exclusion of unauthorized access to an enterprise network or enterprise data. In such an embodiment, the system comprises a mobile device on which operates a software security agent that monitors compliance of the mobile device with at least one security policy; a security policy server on which is stored the at least one security policy applicable to the mobile device and through use of which the at least one security policy can be modified; an enterprise network or enterprise data accessible by the mobile device only through communication with the security policy server; and a network connected to but external to the enterprise network, through which the mobile device can transmit data to and receive data from the security policy server. In an embodiment, the at least one security policy comprises data correlated to a hardware or software configuration or both a hardware and software configuration of the mobile device. In an embodiment, the network connected to but external to the enterprise network includes a communication pathway that includes a wireless communication connection.

[0012] In an alternate embodiment the security is provided by a method for automated centralized control of security features of an enterprise communication network or of enterprise data. In an embodiment, the method comprises the steps of providing a security system such as that described above; providing the mobile device with an initial configuration compliant with an initial security policy; connecting the mobile device to the security policy server without mobile device user participation; downloading a revised security policy from the security policy server to the mobile device. In an embodiment, the step of connecting is triggered by a lapse of a pre-set amount of time after a prior execution of the step of downloading. In an embodiment, the step of connecting is triggered by a change in the security policy stored on the security policy server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 illustrates a schematic of a network system as an embodiment of the security system.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0014] The network security system and methods described herein are generally designed to protect enterprise data, and those persons accessing it with authorization, from the unwarranted and malicious access, including access by unauthorized users, such as when a mobile device is lost or stolen, and damaging software like worms and viruses. The security system provides for self-service and automated administration, including policy enforcement and reporting.

[0015] The security system includes a variety of features. It provides delivery to end-user devices of security policy updates automatically without user intervention, including over the air for wireless devices, and does so for a variety of hardware configurations and a variety of operating system. It provides centralized security policy management across heterogeneous devices from a single self-service console. It allows delegation of administration for end users. It provides complete installation and management of security policies and applications on end-user devices, including over the air for wireless devices. It monitors security policy compliance for local and remotely deployed systems and provides remediation of the non-compliant devices automatically, enabling an organization's conformity with regulatory requirements. The security system can be enhanced with full-device encryption, i.e., encryption for all data stored on a device, for each device authorized to access the enterprise information via the controlled network.

[0016] As used herein, the term mobile devices means any device that a reasonable person uses for mobile data communications and for which the functionality thereof can be altered through software programming. Such mobile devices may also be referred to as Smart Phones or Personal Digital Assistant ("PDAs"), and further include portable and laptop computers, but regardless of the

name, the mobile device software will allow the mobile device access to the Internet or will allow email communication.

[0017] As used herein, the term over-the-air ("OTA") means a communication pathway between a two devices connected by a network, e.g., a server and a mobile device, wherein a portion of the pathway is wireless communication, i.e., data transmitted from one antennae to another antennae through the air via electromagnetic waves, such as the over-the-air communication that occurs from a cellular phone to a cell tower.

[0018] As used herein in broad scope, the term security policy refers to a dataset that correlates to a hardware or software configuration on a networked device. Generally, a mobile device will be configured to conform with a policy, and such configuration will be maintained or otherwise enforced by a software security agent operating on the mobile device so configured. Thus, a portion of the security system herein disclosed operates to ensure that a certain security policy has a common definition as between the security policy server, where policy definition is controlled and maintained by a system administrator, and on the mobile device. For example, for a policy that requires firewall port blocking with regard to a specific port, a software security agent operating on the mobile device will operate to prohibit communication through such port, thereby enforcing the requirement of the policy. The security policies are centrally controlled.

[0019] The security system is effective across various mobile device platforms (i.e., the various hardware and software configurations of mobile devices, and particularly the various operating systems operating various mobile devices) because the centralized policies are segmented into groups of policies, each group of policies being applicable to one or more mobile device platforms. In an embodiment, only

security policies applicable to a mobile device, as based upon the mobile device platform, are synchronized as between the security policy server and the mobile device. In an embodiment, security policies that the security policy server attempts to communicate to a mobile device, but which are inapplicable to the particular mobile device due to the mobile device's platform, are rejected by the mobile device or are accepted and ignored or deleted by the mobile device, which communicates that inapplicability of the policy back to the security policy server.

[0020] Figure 1 illustrates an exemplary OTA hardware architecture that an organization may employ in order to deliver security policies to mobile devices. In general, the security system herein disclosed is operable within such architecture to provide platform-independent security for controlling access to data stored on the at least one server computer 102, or on computers connected thereto, such as on a private enterprise network. Security policies intended to be utilized by a mobile device 108 are stored on a security policy server 102, and synchronized with a mobile device 108. The mobile device 108 is allowed to access enterprise data not stored on the mobile device only if the mobile device 108 operates in compliance with the security policies provided by and stored on the security policy server 102. Such compliance is automatically verified through communications between the mobile device 108 and the security policy server 102 whenever the mobile device 108 attempts to connect to the enterprise network or access enterprise data either stored on the at least one security policy server 102 or on a computer networked thereto, and is verified at regular time intervals while the mobile device 108 is connected to the security policy server 102 or otherwise connected to the enterprise network.

[0021] Such verification is accomplished through a security policy synchronization process, as is described herein. Descriptions of the communications between a networked server and a mobile device such as can be utilized for the purpose of such synchronization are provided in U.S. Patent Publication No. 2006/0224742, published October 5, 2006, which is incorporated herein in its entirety by this reference. A compliant status for the mobile device preferably includes an approved hardware and software structure and configuration, and approved functionality, status, and activity.

[0022] In an embodiment, at least one security policy server 102 which is part of an enterprise network is provided with access to the Internet 104, whether such connection is wired or wireless. The security policy server 102 communicates with authorized cell phones 108 (mobile devices) by sending and receiving OTA data to and from such cell phones through the Internet 104 and a cellular service cell tower 106. The illustrated system including the policy server 102, the Internet 104, cell tower 106, and cell phones 108 is generally referred to as a networked environment 100, wherein exchange of data and sharing of network resources is allowed between and among computing devices and their users when each is properly authenticated. Communication, i.e., the sharing of data, occurs over the networked environment through exchange of data packets, which are discrete groups of electronic signals encoded according to standard protocols so as to be recognizable by various components, i.e., computing devices, of the network environment 100. Such communication over a networked environment via protocol compliant data packets is described in U.S. Patent Publications No. 2006/0179140 and 2006/0179141, each published on August 10, 2006, and U.S. Patent Publication No. 2006/0236370, published on October 19, 2006, each of which is incorporated by reference herein.

[0023] In an embodiment of the security system, OTA communication allows an exchange of security data between a mobile device 108 and a security policy server 102. In an embodiment, the exchange of OTA data is initiated either when a security policy is changed on the security policy server 102 or when a threshold amount of time has expired without a download of a security policy to the mobile device 108 from the security policy server 102, triggering a software security agent operating on a mobile device 108 to initiate download of one or more security polices from the security policy server 102.

[0024] In an embodiment, when a security policy is changed, such as by an authorized administrator, the security policy server 102 formats a predetermined message and sends the message to all affected mobile devices 108. The software security agent operating on a mobile device 108 receiving such message receives the message and responds accordingly by taking the action directed by the message. In an embodiment, the action taken will be for the software security agent to initiate communication to the security policy server 102, such communication directing the transfer of the changed security policy from the security policy server 102 to the mobile device 108.

[0025] In an embodiment, as monitored by the software security agent operating on a mobile device 108, after a pre-set amount of time has past since the last download of a security policy to that mobile device 108, the software security agent sends a message to the security policy server 102 directing transfer of one or more security policies. In an embodiment, the message from the mobile device 108 directs transfer of only those security policies that have changed since the last time that mobile device 108 downloaded security policies. In an embodiment, the message from the mobile device 108 directs the transfer of all security policies

relevant to that mobile device 108, including those security policies that have changed as well as those security policies that have not changed since the last download of a security policy by this mobile device 108. This time-triggered download of security policies may be particularly important in situations when a mobile device 108, for whatever reason, such as due to hardware or software failure, did not receive the last message sent by the security policy server 102 upon a change in a security policy relevant to that mobile device 108.

[0026] In a preferred embodiment, data transmitted between the software security agent operating on the mobile device 108 and the security policy server 102 is encrypted. Such encryption is likely to prevent unwanted access to the message structure of the messages. Unauthorized access to such message structure could allow a loss of integrity to enterprise data, for instance, if a security policy was altered by a person or machine gaining unauthorized access to such message structure and thereby allowing uncontrolled and unauthorized access to the mobile device 108 and the data stored thereon.

[0027] In an embodiment, security policy compliance requires the mobile device 108 comprise at least one of an authorized device serial number, device ESN, device manufacturer, device model name, device operating system (OS) or OS version, device ROM version, device peripherals list, device total memory, device free memory, application list and versions, applications currently running, registry setting snapshot (for relevant devices), date and time of most recent reset or policy update or OTA or USB synchronization, policy number, network interface list and configuration, network connections, geographical location, user name or user ID or user group of current user, or combinations thereof.

[0028] In an embodiments, a security policy includes but is not limited to a policy that ensures that a mobile devices has communicated to the security policy server in a given period of time. In an alternate embodiment, a security policy may contain values dictating the objects that must be available on a mobile device, such as one or more software programs, data files, or other objects that may be stored in the mobile device's file systems, data storage areas, or other volatile or non-volatile storage media associated with the remote device.

[0029] Security policy enforcement is via a management agent software application that exists on the mobile device, a software security agent. The purpose of the management agent is to maintain the device's integrity by ensuring that security policy is up to date and is enforced through methods such as authentication, encryption, and port control.

[0030] In an embodiment, the security system includes a process termed Security Policy Based Network Access and Network Compliance Control (SNANC), which ensures that a mobile device is restricted from access to all but specific network resources when a device is out of compliance with published security policy.

[0031] SNANC consists of a centralized management server, a synchronization infrastructure to implement sharing of security policy and a remote device enforcement agent. In an embodiment, SNANC works as follows:

[0032] A security policy server is configured with a set of security policies that are synchronized onto a mobile device, as described above.

[0033] The set of security policies includes a limited access security policy that requires the mobile device to use a specific network route for network

communication when the mobile device is non-compliant with a certain one or more of the other security policies applicable to the mobile device.

[0034] When a violation of the certain one or more security policies is detected by the enforcement agent software running in the background on the mobile device, network communications to and from the mobile device will be limited by the enforcement agent to the network route specified by the limited access security policy. In this regard, all external communications packets are checked to identify the sending or receiving port ID and address, and only those communications incorporating the specified identifications for recipient or sender will be allowed to pass through to the mobile device from the networked environment or to pass out to the networked environment from the mobile device.

[0035] The mobile device enforcement agent will continue to limit access to network resources to those identified within the limited access security policy, until such a time as either: (a) the security policies change, the changed policies are synchronized with the mobile device, and the enforcement agent is able to verify that the mobile device is in compliance with the security policy set applicable to that mobile device; or (b) the mobile device comes into compliance via user action or via the implementation of self-corrective measures, such as automated restoration of deleted files or other configuration changes. When the mobile device is again determined to be in compliance with the security policy set, the limitation of specific network routing is removed and the device is allowed to connect to other network resources.

[0036] In an embodiment, the specified network communication routing in the limited access security policy allows communication between the mobile device and the security policy server for various purposes including security policy

synchronization, software installation, data manipulation, password recovery, and log message handling.

[0037] In an embodiment, the security system operates to block access to data stored on an enterprise network by blocking access by the mobile device 108 to the enterprise network altogether, or by restricting such enterprise network access to a remediation server. In an embodiment, software running on such a remediation server can direct communication to the mobile device 108, which includes instructions that, when followed by the software security agent operating on the mobile device 108, corrects the non-compliant configuration of the mobile device 108. In an embodiment, if the mobile device cannot be made compliant through interaction with the remediation server, enterprise network access by the mobile device is blocked until a network administrator can reconfigure the mobile device 108 so as to be compliant with the applicable security policy set.

[0038] Through such a process, of communication between the mobile device 108 and the security policy server 102, with consequent communication between the mobile device 108 and a remediation server, if necessary, the security system provides automated enforcement of the security policies relevant to each mobile device 108 in communication with the enterprise network. Preferably, these functions of the security system can operate transparently to the user of the mobile device 108. By operating in the background of the user-directed operations of the mobile device 108, the user of the mobile device 108 only becomes directly aware of the operation of the security system when certain problems arise, such as denial of access to the enterprise data through the enterprise network.

[0039] A further aspect of the security system herein disclosed relates to the scheduling of the synchronization processes for the multiple mobile devices having

authorization to access the enterprise network and its data, and particularly those mobile devices for which security policy control is exercised by the security policy server. Because the number of mobile devices controlled by the security policy server may be so great that simultaneous synchronization of security policies for each mobile device would have a significant negative impact on network function, and may even disable the network. Therefore, the security system herein disclosed includes, in an embodiment, a Bi-Directional Collision Protection and Synchronization Scheduling (BCPSS) module, which addresses the problem of overwhelmed centralized systems, such as the security policy server, by limiting the number of simultaneous pull synchronization transactions requested by mobile devices and processed by the security policy server at one time.

[0040] In an embodiment of the BCPSS module, a remote device's software security agent queues the processing of a command from the security policy server for a random period of time within a pre-determined range. The time based range may be determined by security system administrators, and, for instance, be incorporated into a security policy synchronized between the mobile device and the security policy server, or may be built into the security system by the system architect. The randomizing of the queue wait time, i.e., the time that the command remains in a queue on the mobile device prior to being processed by the mobile device results in various times between the issuance of the command by the security policy server and the response to the command (as through communication from the mobile device to the security policy server) by the various mobile devices controlled by the security policy server.

[0041] In an embodiment, this queue wait time variation among mobile devices ensures that not all or even most of the mobile devices controlled by the security

policy server will simultaneously respond to the command with communications to the security policy server, and thereby avoids a overwhelming the security policy server with incoming communications. Generally, the larger the range of time allowed to the mobile device's software security agent for setting the randomized queue wait time, the greater the chance that fewer mobile devices will initiate sessions simultaneously for synchronization with the security policy server. Thus, the BCPSS module can be used to reduce enterprise network bandwidth requirements, enterprise network latency, and security policy server simultaneous connections.

[0042] In an embodiment, another benefit of the BCPSS module is provided to the mobile device on which it is implemented, in that frequent incoming synchronization commands do not result in the mobile device initiating synchronize action multiple times, but only after a period of delay that ensures that command messaging from the security policy server has completed.

[0043] As an example, a method for implementing a BCPSS-based synchronization process is as follows:

[0044] Remote devices are configured to run a software security agent that listens for incoming synchronization commands from the security policy server. These incoming commands may take several forms including but not limited to Short Message Service (SMS) based messages, e-mail, and other methods that may contain command payloads. SMS using encrypted XML message payloads is one basic example of an implementation for sending commands to the software security agent running on the mobile device. Other implementations may use socket based listeners or other standard methods for signaling the mobile device.

[0045] A security policy server pushes properly formatted command messages to an address list of all configured remote devices. These messages may be triggered by time based events or may occur whenever a change to a specific data element occurs in the security policy server. As discussed above, wherein a policy is applicable to various mobile device platforms, commands to revise that policy may be formatted differently to accommodate the various platforms.

[0046] Mobile devices operating the software security agent receive the security policy server commands, unwrap the command message payload via decryption, cyclic redundancy check (CRC), or through the implementation of other techniques for ensuring the command is properly formatted and meets all of the system security requirements.

[0047] The mobile device software security agent determines whether to reset a randomization timer and queue the command to be processed at the end of the time set on the timer, or, in the case of commands that should not be queued, the software security agent clears the queue timer and the command is immediately processed.

[0048] Should an incoming command message be received by the mobile device before the queue timer has expired for a prior command message, the queue timer is cleared and is reset to a randomized time value. This reset feature ensures that incoming synchronization commands will only be processed in a configurable time range and that successive commands sent to the mobile device from the security policy server will not result in the mobile device repeatedly or continually synchronizing with the security policy server.

[0049] In addition to the above disclosure, current versions of the following guide documents produced for Mobile Armor, LLC to support commercial embodiments of a security system as herein described, are incorporated by

reference: PolicyServer v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide; PolicyServer v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide Appendices; MobileSentinel v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide; DataArmor v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide; FileArmor v2.2.5 for MSPs – Sprint Edition, Administrator/User Guide; VirusDefense v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide; RemoteNetwork v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide; MobileFirewall v3.0 for Managed Services Providers – Sprint Edition, Administrator Guide.

[0050] While the invention has been disclosed in conjunction with a description of certain embodiments, including those that are currently believed to be the preferred embodiments, the detailed description is intended to be illustrative and should not be understood to limit the scope of the present disclosure. As would be understood by one of ordinary skill in the art, embodiments other than those described in detail herein are encompassed by the present invention. Modifications and variations of the described embodiments may be made without departing from the spirit and scope of the invention.

CLAIMS:

1. A security system for use in aiding in the exclusion of unauthorized access to an enterprise network or to enterprise data, said system comprising:

a mobile device on which operates a software security agent that monitors compliance of said mobile device with at least one security policy and limits access of said mobile device to a networked environment when said mobile device is not in compliance with said security policy;

a security policy server on which is stored said at least one security policy applicable to said mobile device;

server management agent software through which said at least one security policy on said security policy server can be modified by an administrator, and which automatically sends a command message over said networked environment to said mobile device upon a change to said security policy; and

wherein upon processing said command message by said software security agent operating on said mobile device said security policy on said mobile device is revised.

2. The security system of claim 1 wherein said at least one security policy comprises data correlated to a hardware or software configuration or both a hardware and software configuration of said mobile device.

3. The security system of claim 1 wherein said mobile device connects to said networked environment through a wireless communication connection.

4. A method for automated centralized control of security features of an enterprise communication network, said method comprising the steps of:

providing a security system comprising:

a mobile device on which operates a software security agent that monitors compliance of said mobile device with at least one security policy;

a security policy server on which is stored said at least one security policy applicable to said mobile device and through use of which said at least one security policy can be modified;

a networked environment through which said mobile device can transmit data to and receive data from said security policy server;

providing said mobile device with an initial configuration compliant with said at least one security policy;

initiating a communication session between said mobile device and said security policy server without mobile device user participation;

downloading a revised security policy from said security policy server to said mobile device.

5. The method of claim 4 wherein said initiating is commenced by said software security agent and triggered by a lapse of a pre-set amount of time after a previously executing said downloading.

6. The method of claim 4 wherein said initiating is commenced by said security policy server sending a command message to said mobile device and is triggered by a change in said security policy stored on said security policy server.

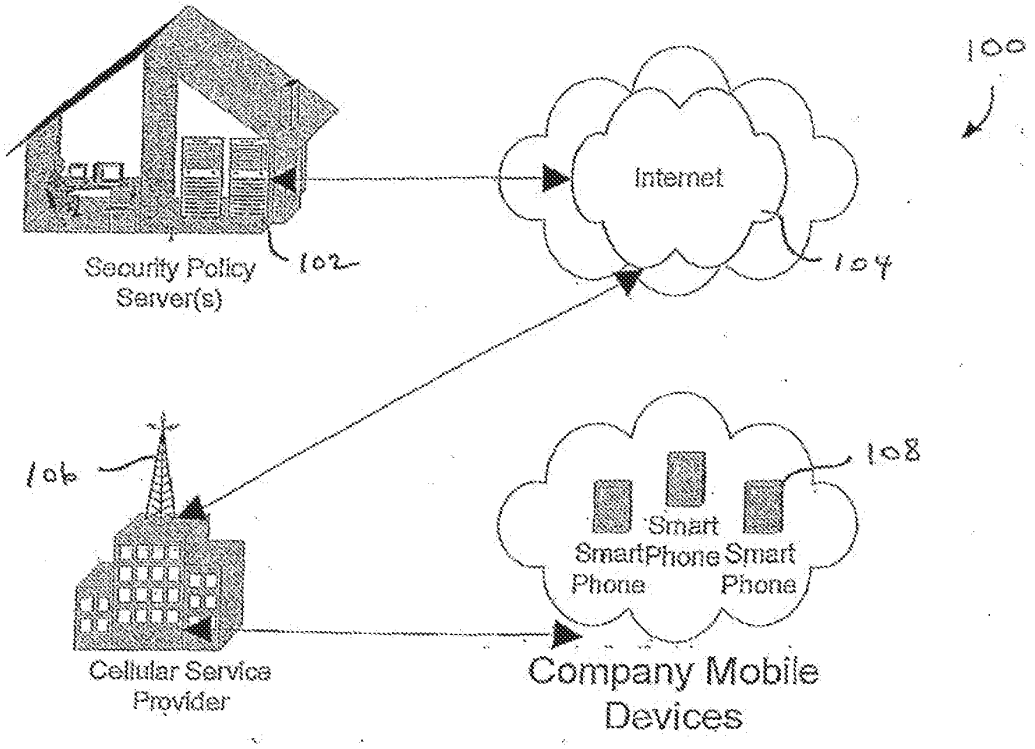

100
Internet
104
Security Policy Server(s)
102
106
108
Smart SmartPhone Smart Phone Phone
Cellular Service Provider
Company Mobile Devices

Figure 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2006/060446

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/22(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)

IPC8: G06F 11/30, 15/16, H04L 9/00, H04Q 7/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, eKIPASS(KIPO internal)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004-0123153 A1 (MICHAEL WRIGHT et al.) 24 June 2004 See abstract, figures 1, 2A, 2B, 3C, 8; paragraphs 11-14, 46-52, 64, 144-151; claims 1, 6, 8 - 11, 14-21.	1-6
X	WO 2004-028070 A1 (CREDANT TECHNOLOGIES, INC.) 1 April 2004 See abstract; page 3 line 1 - page 4 line 3; claims 1, 3-9.	1-6
A	US 6775536 B1 (ROBERT L. GEIGER et al.) 10 August 2004 See abstract; claims 1-8.	1-6
A	US 2004-0111519 A1 (GUANGRUI FU et al.) 10 June 2004 See abstract; paragraphs 7-12; claims 1-7.	1-6

☐ 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 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
17 APRIL 2007 (17.04.2007)	**17 APRIL 2007 (17.04.2007)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	YANG, CHAN HO Telephone No. 82-42-481-5689

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2006/060446

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US20040123153 A1	24.06.2004	AU2003296729A1	14.07.2004
		US2005055578A1	10.03.2005
		US2006004400AA	04.05.2006
		US2006120526AA	08.06.2006
		WO2004057834A3	14.10.2004
WO2004028070 A1	01.04.2004	AU2003276868AA	08.04.2004
		EP1547303A1	29.06.2005
		JP18500657	05.01.2006
		US2006147043A1	06.07.2006
		US2006190984A1	24.08.2006
		US2006239363A1	19.10.2006
		US2006242665AA	26.10.2006
US6775536 B1	10.08.2004	None	
US20040111519 A1	10.06.2004	JP2004165922A2	02.07.2004

Form PCT/ISA/210 (patent family annex) (April 2007)

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
13 July 2006 (13.07.2006)

(10) International Publication Number
WO 2006/073837 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2005/046422

(22) International Filing Date:
21 December 2005 (21.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/028,814 4 January 2005 (04.01.2005) US

(71) Applicant *(for all designated States except US)*: **SYMBOL TECHNOLOGIES, INC.** [US/US]; One Symbol Plaza, Holtsville, NY 11742-1300 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **D'AGOSTINO, Anthony** [US/US]; 57 Ridge Road, Smithtown, NY 11787 (US).

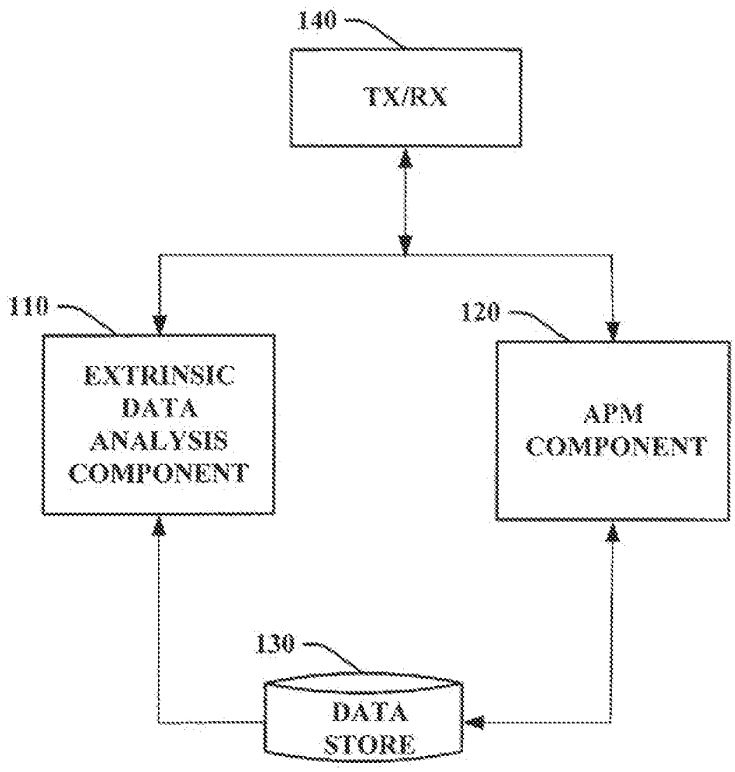
(74) Agents: **AMIN, Himanshu** et al.; Amin & Turocy, LLP, 1900 E. 9th Street, 24th Floor, National City Center, Cleveland, OH 44114 (US).

(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: METHOD AND APPARATUS OF ADAPTIVE NETWORK POLICY MANAGEMENT FOR WIRELESS MOBILE COMPUTERS



(57) Abstract: System(s) and method(s) are provided that utilize external resources and protect the integrity of data within a mobile communication device and data communicated with the mobile communication device. The device includes an extrinsic data analysis component that receives information about both an external environment and an internal state. The device also includes an adaptive policy manager (APM) component. The APM component is adapted to analyze and prioritize policies based upon received input from external resources, stimuli, threats and/or parameters. The method of protecting data integrity is performed automatically and autonomously with minimal user intervention and awareness. The APM component includes a profile component, a policy modification component, a rules component, an authentication component, and an access control component.

WO 2006/073837 A2

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.

Title: METHOD AND APPARATUS OF ADAPTIVE NETWORK POLICY MANAGEMENT FOR WIRELESS MOBILE COMPUTERS

FIELD OF INVENTION

[0001] The invention generally relates to computer systems, and in particular to a method and apparatus to utilize external resources and protect data integrity of a mobile computing device.

BACKGROUND OF THE INVENTION

[0002] The usage of mobile communications systems utilizing mobile devices has become widespread and there is an ongoing and increasing need for the establishment of systems, methods and apparatus to maintain data integrity against unauthorized access while, concurrently, increasing user productivity.

[0003] Most networks utilize a requirement of successful compliance with security procedures in order to obtain a data connection to the network. These security procedures protect against unauthorized access to the network and are generally stored in local memory storage areas of the network. In such a system, the remote terminal provides its identity to the server by supplying various information, including user credential(s) information. The server then processes the user credentials and either permits or denies access to the network based upon the supplied information.

[0004] Typically, the user credentials must be entered and re-entered upon every authentication occurrence. The continuous re-entry of information places a burden on the user to continuously input the data numerous times as well as increasing user frustration. Additionally, users are generally not aware of a loss of data integrity nor are they usually able to make necessary changes to a predefined policy of the device. Additionally, if a network is inaccessible or "down" when the remote terminal is within its physical domain, access to local memory is prevented. Thus, the user is denied access to needed resources because there is no way to circumvent the network.

Therefore, there is a need to provide a remote device that can adapt dynamically, automatically and autonomously, to various network environments to ensure premium use of the device with a minimum amount of user awareness and user required

intervention. This provides the user with a more flexible device that can avail itself to certain resources while, at the same time, properly safeguarding its data payload. It also decreases the necessary support from the device provider and, more importantly, increases user productivity.

SUMMARY OF INVENTION

[0005] The following presents a simplified summary of the invention in order to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is intended to neither identify key or critical elements of the invention nor delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented later.

[0006] According to an aspect of the invention, a portable communication device is provided. The device includes an extrinsic data analysis component that receives and analyzes information relating to an internal state and an external environment of the device and an adaptive policy manager (APM) component that employs the analyzed extrinsic information to dynamically enforce policies that affect data security of the device.

[0007] The APM component can include various internal components such as, for example, a profile component that receives a user input, an authentication component that validates a user based upon the user input, a policies component that retains a set of policies, a policy modification component that selectively overrides the retained set of policies and an access control component that selectively provides access to external resources and data.

[0008] According to another aspect of the invention, the APM component selectively enforces policies that affect data security of the device. For example, the APM component can selectively enforce the policies based upon a defined set of criteria specifying normal behavior in a network environment. The APM component provides prioritization of the policies based upon an assessment of resources available to the device and threats external to the portable communication device. The APM component can automatically and autonomously select and implement a set of actions based upon the policy prioritization. These policies can also be selected and enforced by the APM component based upon an inferred user state.

[0009] According to another aspect of the invention, the APM component is configurable to operate in various user model modes or states, which can be a high-threat model mode, a low-threat model mode or any state there between. In the low-threat model mode, the APM component uses separate criteria, such as user credentials, to determine the availability of local memory resources. In a high-threat model mode, the device can be denied assess to all or some external devices.

[0010] According to another aspect of the invention, a communication architecture is provided that includes a network and an adaptive policy manager (APM) component. The network includes a plurality of stimuli, such as, for example, external resources and external threats. The APM component provides prioritization of policies based upon an assessment of the plurality of stimuli. The policies are a set of rules indicating expected behavior in a particular environment. The prioritization of policies determines a user model mode, which can be a high-level mode, a low-level mode or any state there between.

[0011] According to yet another aspect of the invention is a method of providing data security in a portable computing environment. The method includes assessing an environment external to the mobile communication device. The method receives information from external resources and prioritizes internal system priorities based upon the assessed external environment. The method further selects an action set based upon the received information and implements the selected action set to provide optimal performance of the mobile communication device.

[0012] According to still another aspect of the invention, the method further includes generating parameters that identify criteria, such as user credentials, for at least one stimuli and storing the parameters in a memory location. The parameters are selectively enforced based upon the identified criteria. The method is adapted to dynamically assess any resources and threats external to the portable computing environment. Selecting an action set based upon the received use model information can be performed autonomously.

[0013] According to still another aspect of the invention, the method further includes assessing a threat mode based upon received information and determining if user criteria are acceptable to continue operating in that network based on the assessed threat mode. If the user criteria are acceptable, the method can also determine available local memory resources and establish a network connection to

those available local memory resources. If the user criteria are not acceptable, the method can deny access to the available local memory resources.

[0014] To the accomplishment of the foregoing and related ends, certain illustrative aspects of the invention are described herein in connection with the following description and annexed drawings. There aspects are indicative, however, of but a few of the various ways in which the principles of the invention can be employed and the subject invention is intended to include all such aspects and their equivalents. Other aspects, advantages and novel features of the invention will become apparent from the following detailed description of the invention when considered in conjunction with the drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0015] Figure 1 illustrates a high-level architecture in accordance with an aspect of the invention.

[0016] Figure 2 illustrates an adaptive policy manager component in accordance with an aspect of the invention.

[0017] Figure 3 illustrates exemplary components of the policy manager component according to an aspect of the invention.

[0018] Figure 4 illustrates additional exemplary components in accordance with an aspect of the invention.

[0019] Figure 5 illustrates another exemplary component utilized according to an aspect of the invention.

[0020] Figure 6 illustrates a methodology of enforcing policies according to an aspect of the invention.

[0021] Figure 7 illustrates a methodology of modifying policies in accordance with an aspect of the invention.

[0022] Figure 8 illustrates a methodology of determining a use model in accordance with an aspect of the invention.

[0023] Figure 9 illustrates a schematic block diagram of a computer operable to execute the invention.

[0024] Figure 10 illustrates a device operate to execute an aspect of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0025] The subject invention is now described with reference to the accompanying drawings, which form a part hereof, wherein like reference numerals are used to refer to like elements throughout. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It may be evident, however, that the invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate describing the invention. It is to be understood that other embodiments may be utilized and changes may be made without departing from the scope of the invention.

[0026] As used in this application, the terms "component", "system" and "module" are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution. For example, a component may be, but is not limited to being, a process running on a processor, programmable hardware such as an ASIC or FPGA, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components may reside within a process and/or thread of execution and a component may be localized on one computer and/or distributed between two or more computers.

[0027] As used herein, the terms to "infer" or "inference" refer generally to the process of reasoning about or inferring states of the system, environment, and/or user from a set of observations as captured via events and/or data. Inference can be employed to identify a specific context or action, or can generate a probability distribution over states, for example. The inference can be probabilistic--that is, the computation of a probability distribution over states of interest based on a consideration of data and events. Inference can also refer to techniques employed for composing higher-level events from a set of events and/or data. Such inference results in the construction of new events or actions from a set of observed events and/or stored event data, whether or not the events are correlated in close temporal proximity, and whether the events and data come from one or several event and data sources.

[0028] Referring initially to Figure 1, illustrated is a high-level architecture of a wireless computing device according to an aspect of the invention. The wireless computing device includes an extrinsic data analysis component 110 that

communicates with an adaptive policy manager component (APM) component 120 and a data store 130.

[0029] The extrinsic data analysis component 110 receives information relating to an external environment, such as through a transceiver/receiver 140. The extrinsic data analysis component 110 analyzes the received information, for example, by retrieving information captured in a data store 130. The information captured in the data store may include data regarding expected behavior in various network environments.

[0030] The extrinsic data analysis component 110 transmits the analyzed information to the APM component 120 where policies that affect data security are dynamically enforced. The APM component 120 analyzes the information from the extrinsic data analysis component 110 with additional information received from, for example, the data store 130. The APM component 120 is adapted selectively to allow the wireless computing device access to various resources and data in the external environment.

[0031] The APM component 120 employs information received from the extrinsic data analysis component 110 and dynamically enforces a policy or a set of policies that affect data security of the wireless computing device and access to resources in the network environment. A policy is a set of rules defining what normal behavior should be in a specific situation.

[0032] For example, the user can specify a set of top level rules that correspond to a desired network environment. The policy or set of polices are generated for use on the portable communication device and identify what actions should and/or should not be taken for a given set of stimuli. The policy, written in software, can be generated for use in a particular mobile communication environment.

[0033] When the APM component 120 obtains information concerning the communicating environment, the information is stored in a memory location. The predefined policy is adapted by performing a query using the expected nominal behavior and comparing it with a defined set of criteria from the received network environment information. The APM component 120 adapts the policy to the current environment automatically and autonomously by selectively enforcing certain policies based upon the defined set of criteria. This provides optimal performance of the wireless computing device while protecting data integrity.

[0034] For example, the policy or set of policies can be written in software to produce an action based on a successful test of the defined set of criteria. The defined set of criteria may incorporate, for example, certain threats to the wireless device, each threat given a priority or threat level, such as "1" to "5", with "5" being the highest priority or threat level, for example. When inputs are received that correspond to a particular threat, the existence of that input is ranked according the priority or threat level. For example, if a particular ranking indicates a high threat level to the portable communication device it is assigned a "5". When the portable device receives an input indicating that a particular threat is operating within the network, it queries the nominal behaviors against the input and determines what level threat is present. The APM component can be configured to take account of each threat separately or a plurality of threats contained in the network that when combined exceed a predetermined threshold or tolerance level. The APM component then takes appropriate action, based upon the predefined policy relating to the threshold or tolerance level of the portable device. The policy may be, for example, to restrict access to/from a particular device or resource that is causing the threat or disconnect the portable device from the computing environment.

[0035] Therefore, the user only needs to specify a set of top-level rules and the APM component 120 is adapted to interpret and execute those rules on a case-by-case basis depending upon the known and sampled network parameters in which the portable communication device is operating. The automatic and autonomous function of the APM component 120 provides a flexible wireless computing device that can avail itself to various resources while concurrently properly safeguarding its data payload. The APM component 120 can be configured to continuously assess the external environment or only periodically access the environment to save system resources.

[0036] The APM component 120 can also receive input directly from the user based upon user actions or requests to access external resources. The APM component can also infer from the user actions that may be desired by the user and access the environment for achieving a proper result and provide the user optimal performance of the portable device.

[0037] Referring now to Figure 2, illustrated is a wireless mobile computer 200 the includes an extrinsic data analysis component 210 and an adaptive policy management (APM) component 220. The extrinsic data analysis component 210 is

adapted to receive information about an external environment and an internal state of the mobile computer 200.

[0038] The external information includes available network resource and network parameters. Examples of the available network resources are printers, PBX's, file servers, etc. Parameters include network signal strength, network performance, average network packet size, and network threat level. The internal state of the mobile computer 200 includes current user state information, resource request information, etc.

[0039] The APM component 220 can be suitably configured to maintain data integrity *via* a profile component 230, an authentication component 240, a policy modification component 250, a rules component 260 and an access control component 270. The APM component can also receive/send information to the extrinsic data analysis component 210 and the data store 280.

[0040] The profile component 220 identifies a user based upon user input data. The profile component 220 also captures user domain information as well as the user's authority in a particular network, such as security clearance levels, etc.

[0041] The authentication component 230 retains information about various users of the device. In some instances, a mobile computer may be used by more than one person. The device retains the user information to verify which user is signed-on at a particular time, and allowing that person access to resources and data that are relevant to that person.

[0042] The rules component 260 contains a rule or set of rules that indicate expected behavior in a particular environment. These rules help ensure data security of both the mobile computer 200 and the data communicated to and from the mobile computer 200. The rules can also relate to external devices or resources available in the external network environment that have approval to communicate with the mobile computer 200.

[0043] The policy modification component 250 is able to capture data regarding an environment external to the computer as well as information regarding the device itself. The policy modification component 250 is configured to receive user input information. For example, a user specifies a set of top-level rules and inputs that information into the computer. These rules will be interpreted and executed by the computer based upon the current operating environment.

[0044] The access control component 270 is capable of detecting user state information. It also maintains an internal register of files or databases accessible and available to the computer. Additionally, the access control component detects objects or resources available to the computer.

[0045] Through use of the individual components, the APM component 220 selectively enforces policies based upon a defined set of criteria. For example, the APM component 220 may be configured with a set of rules that define what normal behavior should be in a particular environment. If a behavior is expected, it is given a ranking of "1" or "0", for example. If a behavior is not expected, but does not pose a significant threat, it is given a ranking, such as "2" or "3". If a behavior is unacceptable or poses a significant threat to the device or data, it is given a ranking of "4" or "5". Thus, when that particular behavior is detected by the APM component, it is recognized in relationship to its ranking and the APM component takes appropriate action based upon the defined policies or rules relating that that particular behavior.

[0046] For example, if the network is a work related network and only workers or those with certain access privileges are allowed to access local memory storage of the work related network, the policy may be enforced by denying the device access to that network if the device does not have the specified credentials. In this way, sensitive work related data would only be accessible when the portable communication device is connected to a work related network and has the proper credentials. These credentials may include various parameters, such as access codes, access privileges and rights, user database rights, user clearance levels, department, etc.

[0047] The APM component 220 can selectively enforce policies depending upon a set of criteria that affects the specific portable communication device. The set of criteria are inputs to the APM component 220 and are evaluated by the APM component 120. The set of criteria can be resources available to the portable communication devices. These available resources include printers, PBX's, and file servers, etc. Another set of criteria may be external stimuli including parameters based on various factors including network signal strength, network performance, average network packet size, and network threat levels, etc.

[0048] The APM component 220 is capable of providing classification or ranking of policies based on a dynamic assessment of the resources, stimuli and threats external to the wireless mobile computer 200. The APM component 220

autonomously selects and implements a set of actions based upon its assessment of the resources and stimuli. This is performed automatically and autonomously by the APM component 220 and does not require user intervention. Thus, allowing the user premium use of the mobile computer without requiring the user to be aware of each resource and/or stimuli and intervening for each specific situation.

[0049] For example, the APM component may enforce a policy by denying the wireless mobile computer access to certain areas of a local memory storage device if the local memory storage device is not recognized or is of unknown data reliability. This would allow sensitive data on the computer to be protected from access by the local memory storage device, maintaining the integrity of both the local memory storage device and the mobile computer. In this situation, the APM component can be configured to operate in a high threat use mode or a low threat use mode. While in low threat use mode, the APM manager can look at other criteria, such as user credentials, to determine the availability of local memory resources that the computer can utilize in place of the local memory storage device. The user credentials relate to various rights or privileges of the user and may be assigned and/or determined by a user's log on information. While in high threat use mode, the APM component can deny the computer access to some or all external devices or resources.

[0050] Figure 3 illustrates exemplary components contained in the APM component according to an aspect of the invention. A profile component 230 includes an identification module 310, a domain module 320 and an authority module 330. The profile component 230 is capable of receiving user input 240, which includes changing a user profile to allow a higher/lower access level. The user input 240 can be either from the user, administrator or computer manufacturer. The identification module 310 contains user identification information, such as user credentials, user access rights, etc. The authority module 330 of the profile component 230 stores additional information about the user, such as authority levels. The profile component 230 works autonomously or may interact with an authentication component 240.

[0051] The authentication component 240 authenticates multiple user access rights based upon user input criteria. A $user_1$ module 350 contains information regarding user1, which includes user credential information, user access rights, etc. $User_2$ module contains all known information about user2. The authentication component 240 contains information for all users of the device and contains as many user profile modules as required, shown as $user_x$ profile module.

[0052] Figure 4 illustrates exemplary components utilized in and by the APM component according to another aspect of the invention. A rules component 260 contains rules modules 410, 420 that define the expected behavior of the device in a network environment. Each rules module stores a different set of rules and the rules component 260 may contain a large number of rules modules 430. The rules component 260 interacts with the policy modification component 250 to implement a policy to automatically and autonomously adapt to the computing environment. Both the rules component 260 and the policy modification component can work autonomously or together to bring out the desired result.

[0053] The policy modification component 250 includes an environment module 450, a state module 450 and a user input 470. The user input 470 includes a set of top-level rules to be used in the network environment that can be provided by a user, administrator or computer manufacturer. The environment module 440 captures information regarding the external environment of the device. This may include available resources or potential threats to the mobile device. Also included in the policy modification component 250 is a state module 450 that detects an internal state of the mobile device.

[0054] Figure 5 illustrates an access control component for use with the invention. The access control component 270 includes a user profile module 510, a file module 530 and an object module 520. The user profile module 510 contains user access rights information. The file module 530 maintains a listing of files that are available for use by the mobile device. It is understood that files include any data accessible by the mobile device and is not limited to documents. The object module 520 maintains a listing of the objects or resources that are available to the device at any given time.

[0055] Certain methodologies that can be implemented in accordance with the invention are illustrated in Figures 6-8. While, for purposes of simplicity of explanation, the methodologies are shown and described as a series of blocks, it is to be understood and appreciated that the invention is not limited by the order of the blocks, as some blocks can, in accordance with the invention, occur in different orders and/or concurrently with other blocks from that shown and described herein. Moreover, not all illustrated blocks may be required to implement the methodologies in accordance with the invention.

[0056] Referring initially to Figure 6, illustrated is a methodology 600 of selectively enforcing policies in a mobile computer in accordance with an aspect of the invention. The method starts when a mobile computer powers up and runs either continuously while the computer is operating or periodically to conserve system resources. At 602 data from the mobile computer and external to the mobile computer is retrieved, such as *via* an extrinsic data analysis component. The retrieved data includes various use states of the mobile computer including user information and computer state information. The external information includes available resources the mobile computer can access such as printers, file servers, PBX's, IR (Infra-Red) ports, serial / USB ports, etc.

[0057] At 604, the retrieved data is analyzed *via* for example, the extrinsic data analysis component. At 606, the analyzed data is compared or tested against a set of policies, for example by an adaptive policy manager (APM) component, and are prioritized. The set of policies are located, for example in a data store, and represent those actions that should or should not be taken for a given set of analyzed data. The method autonomously selects an action or an action set based on the policy prioritization.

[0058] For example, the method is able to detect if a mobile computer is not connected to a specific network but the user is attempting to make the connection. The method is able to detect that the mobile computer is not connected based upon receiving an input and analyzing the input against a set of rules or policies. If it is determined that the mobile computer is to be denied access, the method will inhibit the computer accessing the network, preventing sensitive work related data being available to non-network devices.

[0059] At 608, a determination is made if the tested policies represent the defined nominal criteria. If the tested policies do not meet the nominal criteria, the method continues at 614 and access to external resources or data is denied. If the tested policies substantially match the nominal criteria, the method continues at 610 and access to the external resource or data is allowed.

[0060] The method continues at 612 where the APM component selectively enforces policies based upon the retrieved and analyzed data. The method, through a dynamic assessment of resources, stimuli and threats external to the mobile communication device is able to prioritize the policy or set of policies and take the appropriate action necessary. The method may generate a parameter that identifies

criteria for at least one stimuli and stores the parameter in a memory location. Using this stored parameter the method can selectively enforce the parameter based upon the identified criteria.

[0061] The method implements selected action(s) by either allowing or not allowing access to a particular resource based on the inputted resource data, stimuli and/or threats. The method is also able to determine a use mode based upon the input information and implement an action based upon that use mode. Depending on the use mode, the device may be configured to operate in a high threat use mode or a low threat use mode. In a high threat use mode the device may have restricted access to all or some external resources or devices due to loss of data integrity. In a low threat use model, the method looks at other criteria, such as user credentials, to determine if, instead of a work related network connection, there is other local memory resources available based upon the predefined criteria. The user credentials include user access rights, user clearance level, etc.

[0062] Figure 7 is a methodology of modifying rules to allow a mobile computer to access external resources or data. The method starts at 702 with data input to the mobile computer, which includes external environment information as well as user information. The external environment information includes a listing of all system resources available as well as various parameters. These parameters may include indication of average network packet size, network threat level, network performance, network signal strength, etc. Other inputs are threats that may jeopardize the integrity of the device or data communicated with the device. Another input includes an assessment of whether the mobile device is in a particular operating network and whether or not that device has the proper access for that network. The mobile device is adapted to receive this information or to actively seek the information though user requests or an inferred user state. The input data is then evaluated 704 against a known set of data to verify a proper working environment.

[0063] At 706, the method authenticates the particular user of the mobile computer out of a set of possible users. At 708 rules are retrieved that indicate expected behavior in a particular environment. These rules help ensure data security of both the portable communication device and the data communicated to and from the portable communication device. The rules can also relate to external devices or resources available in the external network environment that have approval to communicate with the portable device.

[0064] At 710, a determination is made to override the rules. If it is determined that the rules should not be overridden, at 712 the user is denied access to the requested resource or data. If it is determined that the rules should be overwritten, at 714 the rules are modified. After the rules are modified, the user is allowed access to the requested resources or data.

[0065] Referring now to Figure 8, illustrated is a methodology that determines use model criteria. The method starts 802 when use model information is received. The method accesses the current external environment of the mobile communication device. This external environment includes all system resources available as well as various parameters. These parameters may include indication of average network packet size, network threat level, network performance, network signal strength, etc.

[0066] At 806 policies are tested according to the use model information. The method receives a defined set of criteria including information from the system resources and/or parameters and analyzes or compares the received information against a system policy based upon the predefined rules or policies internal to the mobile computing device. These rules or policies are predefined and, for example, are stored in a computer readable medium of the mobile computing device to establish nominal behavior standards for a given network environment. The policies or rules are located internal to the mobile communication device to avoid a situation where a work related network may be "down" or unable to communicate. By employing internal policies or rules, the mobile communication device is still able to access local resources and/or local memory even when a work related network is unresponsive.

[0067] At 808, a determination is made whether the mobile computer is at a high use model level or a low use model level. If the input data indicates a threat level, such as a work related network being inaccessible, the threat mode is assessed and selected. This assessment is performed by analyzing various policies or rules and prioritizing those policies or rules based upon the input data. If it is determined that the mobile computer is in a high use model, the method switches to a high use model and access to external resources and data is denied or limited at 814. If the threat mode is low, the method switches to low use model and the method evaluates user information at 810. For example, credentials, user access rights to file servers, etc. may be analyzed to determine if that particular user has the appropriate access level to connect to a work related network. If the criteria are not acceptable, the method may deny the user access to a network connection. The method continues at 812 to

determine the available local memory resources that can be utilized by the mobile communication device in place of a work related network, for example.

[0068] Referring now to Figure 9, there is illustrated a schematic block diagram of a portable hand-held terminal device 900 (similar to the portable scanning device 1000 as illustrated in Figure 10) according to one aspect of the present invention, in which a processor 902 is responsible for controlling the general operation of the device 900. The processor 902 is programmed to control and operate the various components within the device 900 in order to carry out the various functions described herein. The processor 902 can be any of a plurality of suitable processors. The manner in which the processor 902 can be programmed to carry out the functions relating to the present invention will be readily apparent to those having ordinary skill in the art based on the description provided herein.

[0069] A memory 904 connected to the processor 902 serves to store program code executed by the processor 902, and serves as a storage means for storing information such as user credential and receipt transaction information and the like. The memory 904 can be a non-volatile memory suitably adapted to store at least a complete set of the information that is displayed. Thus, the memory 904 can include a RAM or flash memory for high-speed access by the processor 902 and/or a mass storage memory, *e.g.*, a micro drive capable of storing gigabytes of data that comprises text, images, audio, and video content. According to one aspect, the memory 904 has sufficient storage capacity to store multiple sets of information, and the processor 902 could include a program for alternating or cycling between various sets of display information.

[0070] A display 906 is coupled to the processor 902 *via* a display driver system 908. The display 906 can be a color liquid crystal display (LCD), plasma display, or the like. In this example, the display 906 is a ¼ VGA display with sixteen levels of gray scale. The display 906 functions to present data, graphics, or other information content. For example, the display 906 can display a set of customer information, which is displayed to the operator and can be transmitted over a system backbone (not shown). Additionally, the display 906 can display a variety of functions that control the execution of the device 900. The display 906 is capable of displaying both alphanumeric and graphical characters.

[0071] Power is provided to the processor 902 and other components forming the hand-held device 900 by an onboard power system 910 (*e.g.*, a battery pack). In

the event that the power system 910 fails or becomes disconnected from the device 900, a supplemental power source 912 can be employed to provide power to the processor 902 and to charge the onboard power system 910. The processor 902 of the device 900 induces a sleep mode to reduce the current draw upon detection of an anticipated power failure.

[0072] The terminal 900 includes a communication subsystem 914 that includes a data communication port 916, which is employed to interface the processor 902 with a remote computer. The port 916 can include at least one of Universal Serial Bus (USB) and IEEE 1394 serial communications capabilities. Other technologies can also be included, for example, infrared communication utilizing an infrared data port.

[0073] The device 900 can also include a radio frequency (RF) transceiver section 918 in operative communication with the processor 902. The RF section 918 includes an RF receiver 920, which receives RF signals from a remote device *via* an antenna 922 and demodulates the signal to obtain digital information modulated therein. The RF section 918 also includes an RF transmitter 924 for transmitting information to a remote device, for example, in response to manual user input *via* a user input device 926 (*e.g.*, a keypad) or automatically in response to the completion of a transaction or other predetermined and programmed criteria. The transceiver section 918 facilitates communication with a transponder system, for example, either passive or active, that is in use with product or item RF tags. The processor 902 signals (or pulses) the remote transponder system *via* the transceiver 918, and detects the return signal in order to read the contents of the tag memory. In one implementation, the RF section 918 further facilitates telephone communications using the device 900. In furtherance thereof, an audio I/O section 928 is provided as controlled by the processor 902 to process voice input from a microphone (or similar audio input device) and audio output signals (from a speaker or similar audio output device). In another implementation, the device 900 can provide voice recognition capabilities such that when the device 900 is used simply as a voice recorder, the processor 902 can facilitate high-speed conversion of the voice signals into text content for local editing and review, and/or later download to a remote system, such as a computer word processor. Similarly, the converted voice signals can be used to control the device 900 instead of using manual entry *via* the keypad 926.

[0074] Onboard peripheral devices, such as a printer 930, signature pad 932, and a magnetic strip reader 934 can also be provided within the housing of the device 900 or accommodated externally through one or more of the external port interfaces 916.

[0075] The device 900 can also include an image capture system 936 such that the user can record images and/or short movies for storage by the device 900 and presentation by the display 906. Additionally, a dataform reading system 938 is included for scanning dataforms. It is to be appreciated that these imaging systems (936 and 938) can be a single system capable of performing both functions.

[0076] Figure 10 is provided to assist in understanding and to provide context to an embodiment of the present invention. Specifically, Figure 10 illustrates an example of a handheld terminal 1000 in accordance with an aspect of the present invention.

[0077] The handheld terminal 1000 includes a housing 1002 which can be constructed from a high strength plastic, metal, or any other suitable material. The handheld terminal 1000 includes a display 1004. As is conventional, the display 1004 functions to display data or other information relating to ordinary operation of the handheld terminal 1000 and/or mobile companion (not shown). For example, software operating on the handheld terminal 1000 and/or mobile companion can provide for the display of various information requested by the user. Additionally, the display 1004 can display a variety of functions that are executable by the handheld terminal 1000 and/or one or more mobile companions. The display 1004 provides for graphics based alpha-numerical information such as, for example, the price of an item requested by the user. The display 1004 also provides for the display of graphics such as icons representative of particular menu items, for example. The display 1004 can also be a touch screen, which can employ capacitive, resistive touch, infrared, surface acoustic wave, or grounded acoustic wave technology.

[0078] The handheld terminal 1000 further includes user input keys 1006 for allowing a user to input information and/or operational commands. The user input keys 1006 can include a full alphanumeric keypad, function keys, enter keys, etc. The handheld terminal 1000 can also include a magnetic strip reader 1008 or other data capture mechanism (not shown). An electronic signature apparatus can also be employed in connection with the magnetic strip reader or a telecheck system.

[0079] The handheld terminal 1000 can also include a window 1010 in which a bar code reader/bar coding imager is able to read a bar code label, or the like, presented to the handheld terminal 1000. The handheld terminal 1000 can include a light emitting diode (LED) (not shown) that is illuminated to reflect whether the bar code has been properly or improperly read. Alternatively, or additionally, a sound can be emitted from a speaker (not shown) to alert the user that the bar code has been successfully imaged and decoded. The handheld terminal 1000 also includes an antenna (not shown) for wireless communication with a radio frequency (RF) access point; and an infrared (IR) transceiver (not shown) for communication with an IR access point.

[0080] What has been described above comprises examples of the invention. It is, of course, not possible to describe every conceivable combination of components or methodologies for purposes of describing the invention, but one of ordinary skill in the art can recognize that many further combinations and permutations of the invention are possible. Accordingly, the invention is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims. Furthermore, to the extent that the term "comprises" is used in either the detailed description or the claims, such term is intended to be inclusive in a manner similar to the term "comprising" as "comprising" is interpreted when employed as a transitional word in a claim.

CLAIMS

What is claimed is:

1. A portable communication device comprising:

an extrinsic data analysis component that receives and analyzes information relating to internal state and external environment of the device; and

an adaptive policy manager (APM) component that employs the analyzed extrinsic information to dynamically enforce policies that affect data security of the device.

2. The portable communication device of claim 1, the APM component further comprising a profile component that receives a user input.

3. The portable communication device of claim 2, the APM component further comprising an authentication component that validates a user based upon the user input.

4. The portable communication device of claim 1, the APM component further comprising:

a policies component that retains a set of policies; and

a policy modification component that selectively overrides the retained set of policies.

5. The portable communication device of claim 1, the APM component further comprising an access control component that selectively provides access to external resources and data.

6. The portable communication device of claim 1, the APM component selectively enforcing the policies based upon a defined set of criteria.

7. The portable communication device of claim 1, the APM component providing prioritization of the policies based upon an assessment of resources available to the portable communication device.

8. The portable communication device of claim 3, the APM component providing prioritization of the policies based upon threats external to the portable communication device.

9. The portable communication device of claim 1, the APM component autonomously selecting and implementing a set of actions.

10. The portable communication device of claim 1, the APM component enforcing the policies based upon an inferred user state.

11. The portable communication device of claim 1, the APM component is configurable to operate in a use model.

12. The portable communication device of claim 11, the use model is a high-threat model or a low-threat model.

13. The portable communication device of claim 12, the APM component in the low-threat model using separate criteria to determine availability of local memory resources in lieu of a work related network connection.

14. The portable communication device of claim 13, the separate criteria is a user credential.

15. A communication architecture, comprising:

a network that includes a plurality of resources;

a data analysis component that captures data about the plurality of resources; and

an adaptive policy manager (APM) component that provides prioritization of policies based upon an assessment of the plurality of resources.

16. The communication architecture of claim 15, the plurality of resources comprising external resources and external threats.

17. The communication architecture of claim 15, the policies are a set of rules indicating expected behavior in a particular environment.

18. The communication architecture of claim 15, the APM component determining a use model.

19. The communication architecture of claim 18, the use model is either a high-level model or a low-level model.

20. A method of providing data security in a portable computing environment, comprising:

assessing an external environment;

receiving information from resources in the external environment;

prioritizing system policies based upon the received information;

selecting an action based upon the prioritized system policies; and

implementing the selected action.

21. The method of claim 20, prioritizing system priorities based upon the assessed external environment further comprising:

testing a defined set of criteria; and

comparing the defined set of criteria with a system policy.

22. The method of claim 21, prioritizing system priorities based upon the assessed external environment further comprises dynamic assessment of resources and threats external to the portable computing environment.

23. The method of claim 20, selecting an action set based upon the received information is performed autonomously.

24. The method of claim 20, further comprising:

selecting a use mode based upon the received information; and

determining if user criteria are acceptable based on the assessed use mode.

25. The method of claim 24, further comprising:

determining available local memory resources if the user criteria is acceptable; and

establishing a network connection to the available local memory resources.

26. The method of claim 24, further comprising denying access to local memory resources if the user criteria are unacceptable.

27. A computer readable medium of a portable device to provide safe operation of the portable device, comprising:

a component that evaluates an external environment and develops a query;

a component that combines a set of policies with the developed query to prioritize the set of policies; and

a component that implements action sets based on the prioritized set of policies.

28. A portable communication system that protects data integrity, comprising:

means for querying a portable communication system;

means for selecting a set of rules based upon the queried system; and

means for selectively enforcing the set of rules.

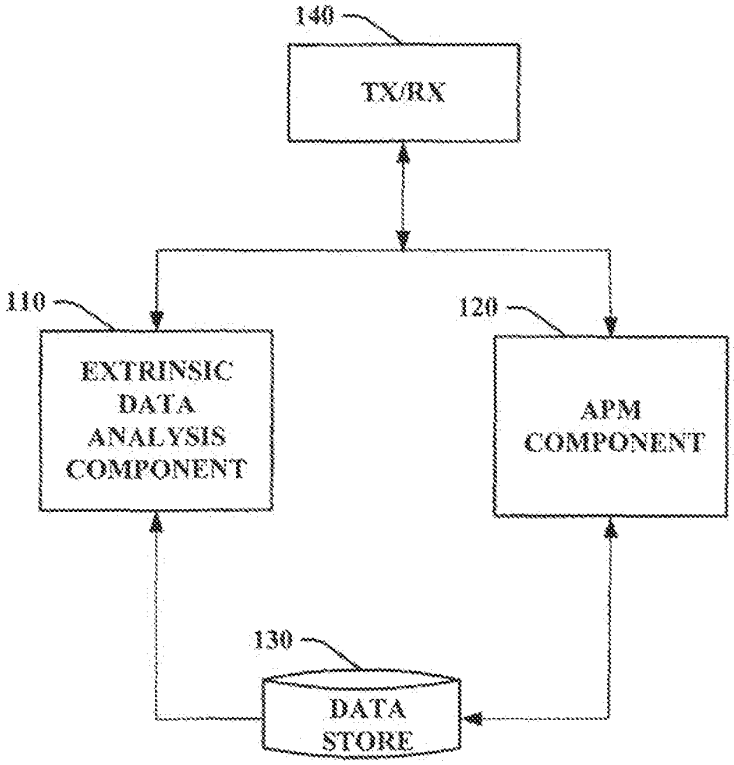

140
TX/RX
110
EXTRINSIC DATA ANALYSIS COMPONENT
120
APM COMPONENT
130
DATA STORE

FIG. 1

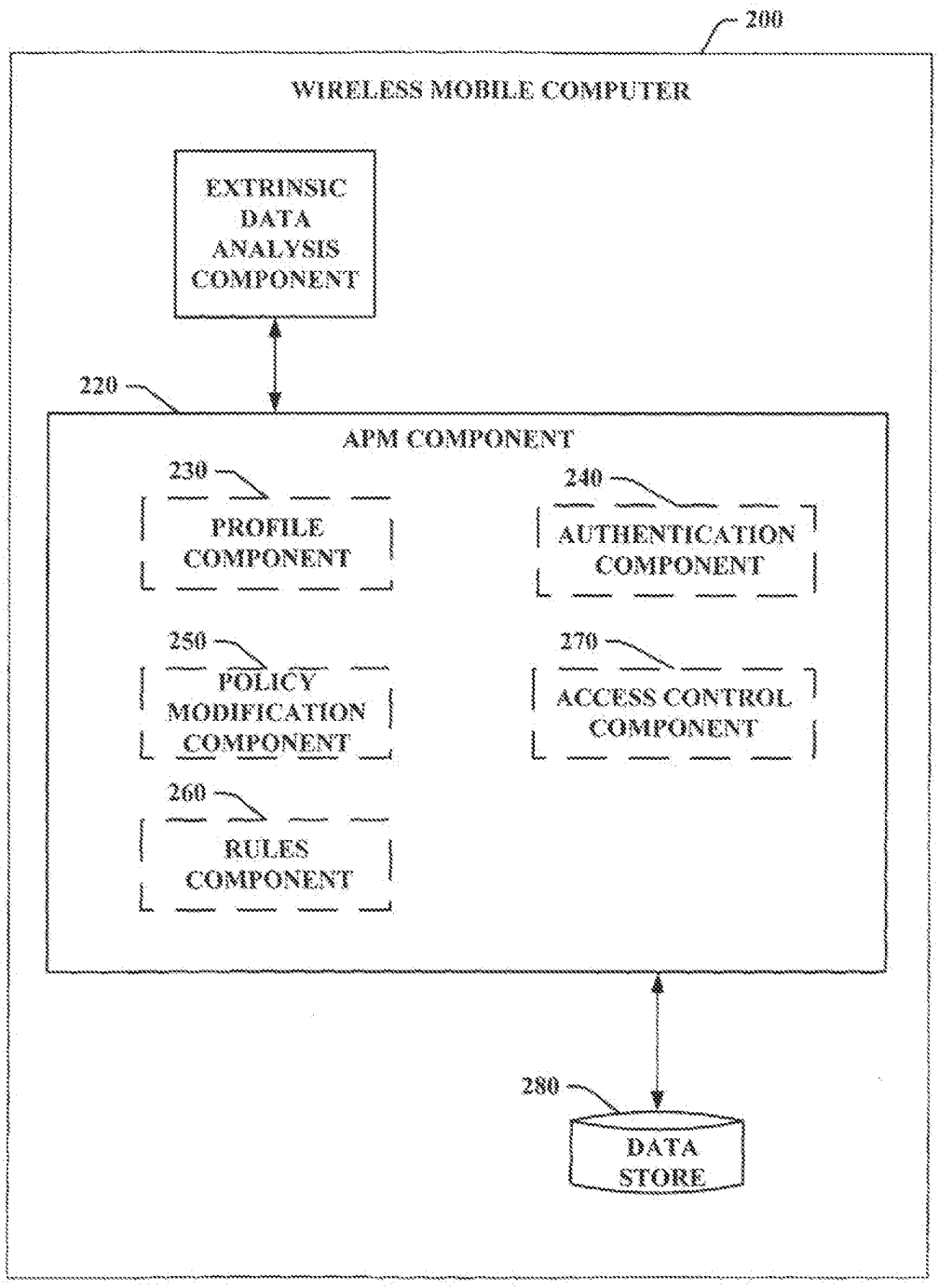

200
WIRELESS MOBILE COMPUTER
EXTRINSIC DATA ANALYSIS COMPONENT
220
APM COMPONENT
230
PROFILE COMPONENT
240
AUTHENTICATION COMPONENT
250
POLICY MODIFICATION COMPONENT
270
ACCESS CONTROL COMPONENT
260
RULES COMPONENT
280
DATA STORE

FIG. 2

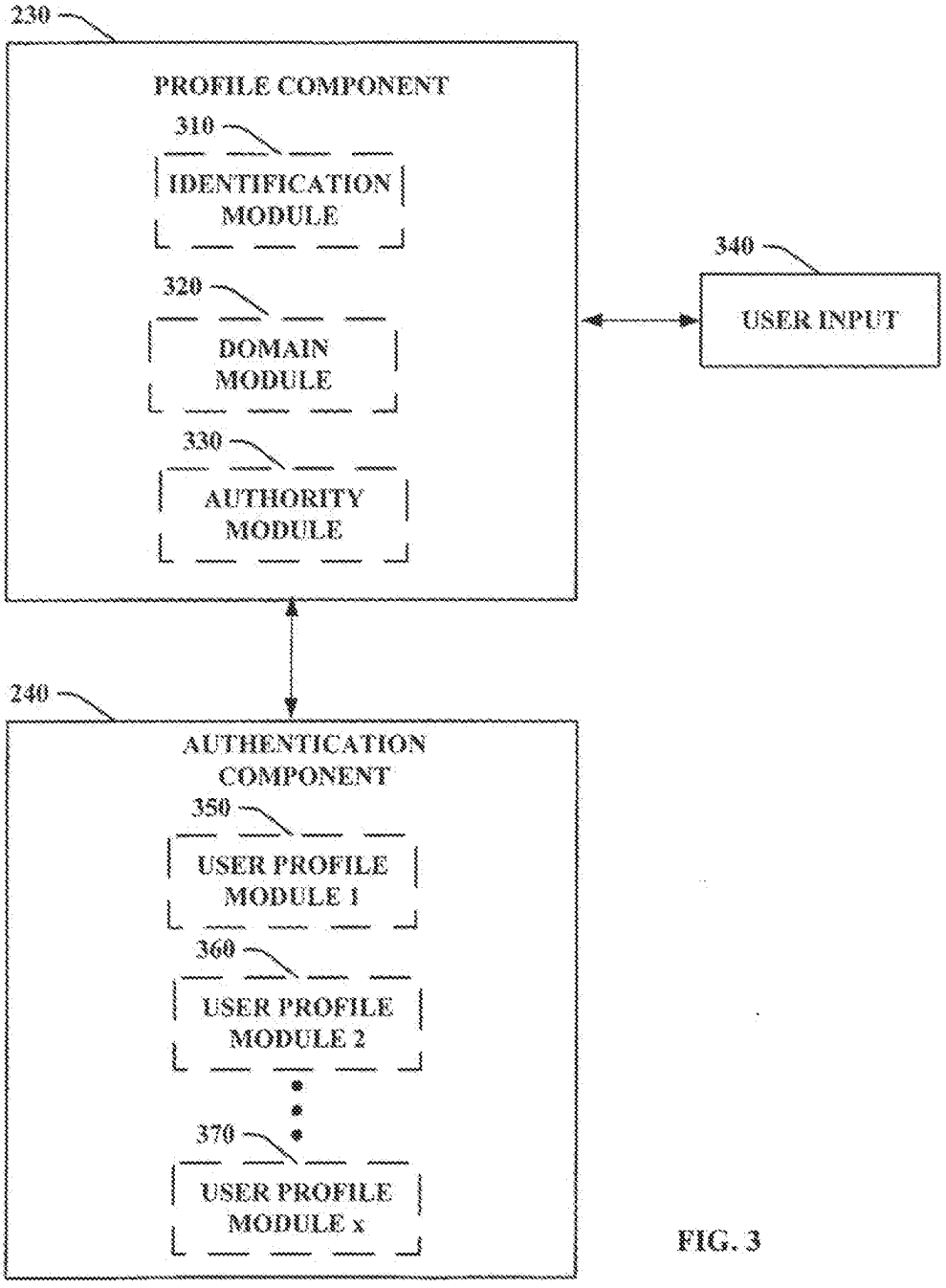

230
PROFILE COMPONENT
310
IDENTIFICATION MODULE
320
DOMAIN MODULE
330
AUTHORITY MODULE
340
USER INPUT
240
AUTHENTICATION COMPONENT
350
USER PROFILE MODULE 1
360
USER PROFILE MODULE 2
370
USER PROFILE MODULE x

FIG. 3

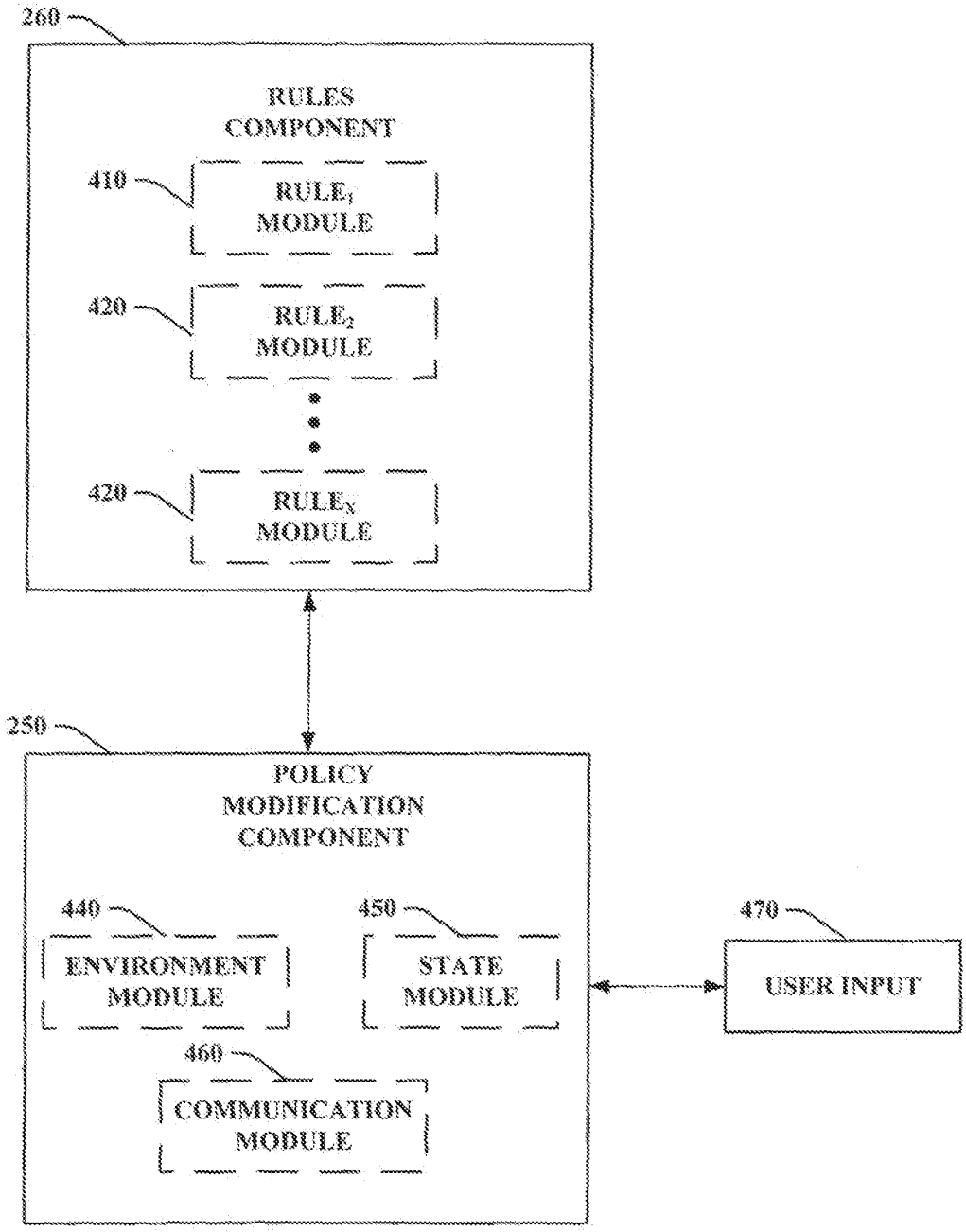

260
RULES COMPONENT
410
RULE1 MODULE
420
RULE2 MODULE
420
RULEN MODULE
250
POLICY MODIFICATION COMPONENT
440
ENVIRONMENT MODULE
450
STATE MODULE
460
COMMUNICATION MODULE
470
USER INPUT

FIG. 4

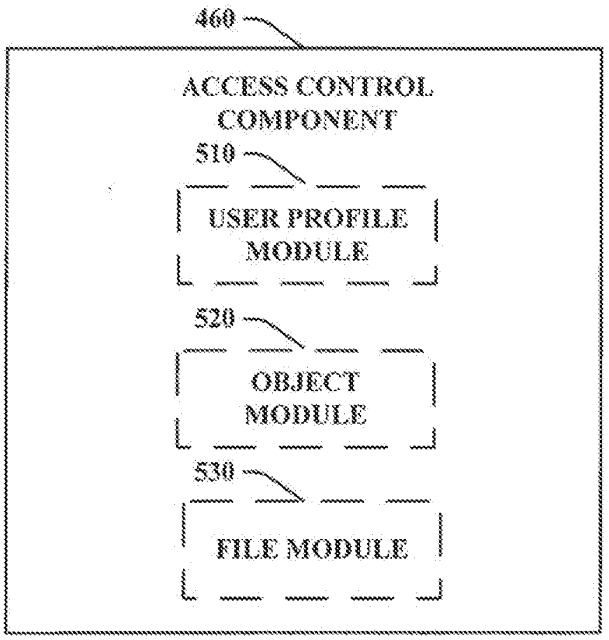

460
ACCESS CONTROL COMPONENT
510
USER PROFILE MODULE
520
OBJECT MODULE
530
FILE MODULE

FIG. 5

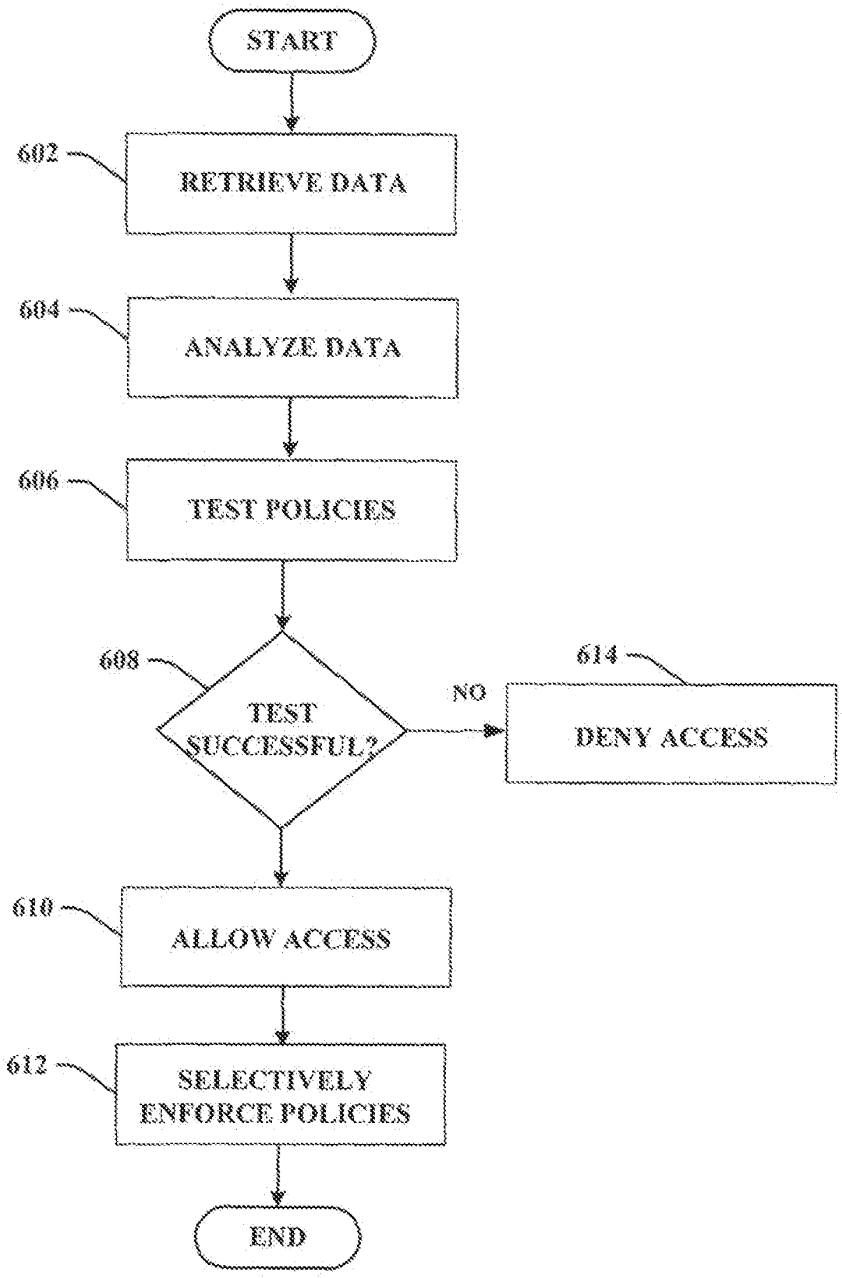

START
602
RETRIEVE DATA
604
ANALYZE DATA
606
TEST POLICIES
608
TEST SUCCESSFUL?
NO
614
DENY ACCESS
610
ALLOW ACCESS
612
SELECTIVELY ENFORCE POLICIES
END

FIG. 6

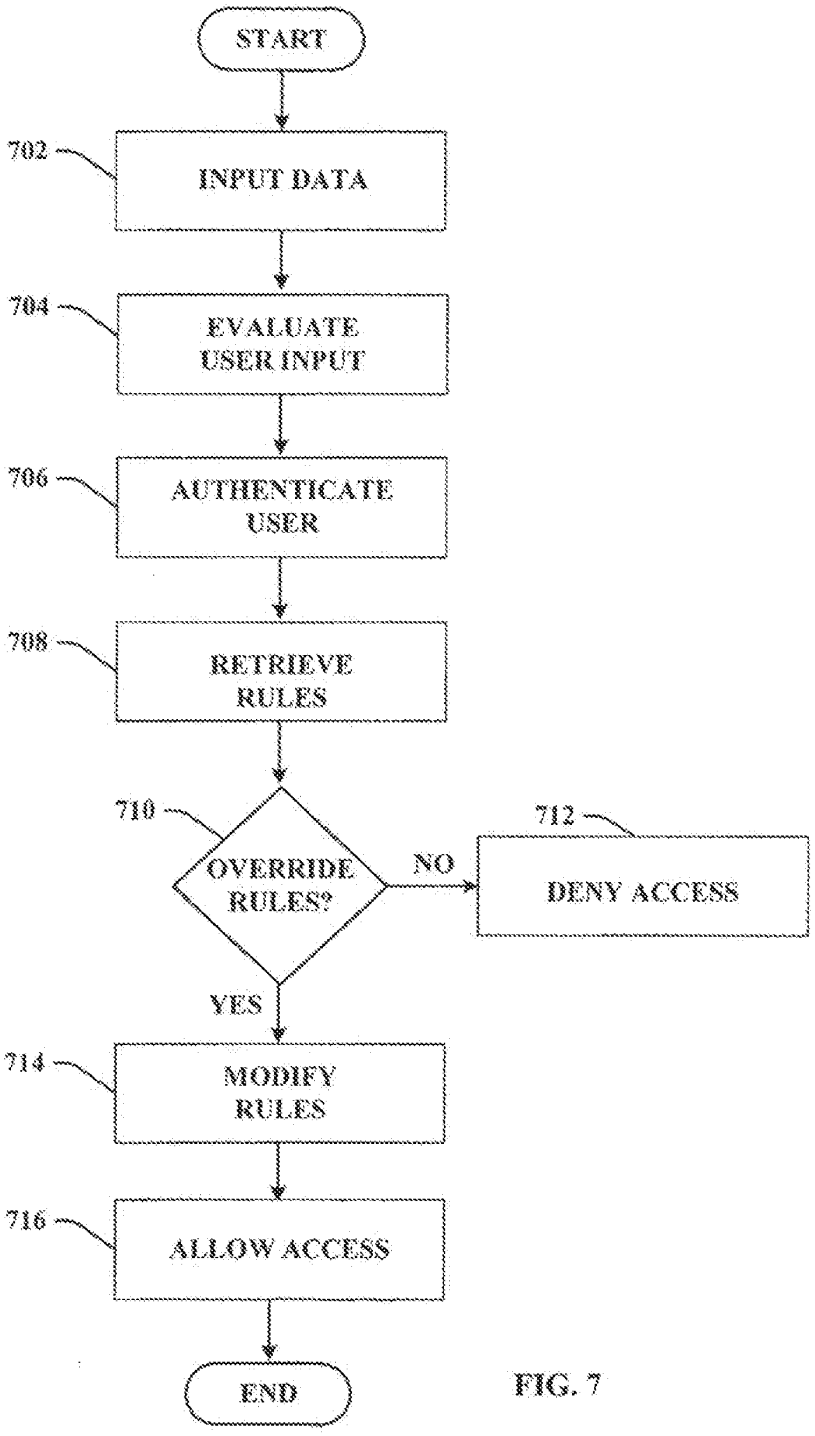

START
702
INPUT DATA
704
EVALUATE USER INPUT
706
AUTHENTICATE USER
708
RETRIEVE RULES
710
OVERRIDE RULES?
NO
712
DENY ACCESS
YES
714
MODIFY RULES
716
ALLOW ACCESS
END

FIG. 7

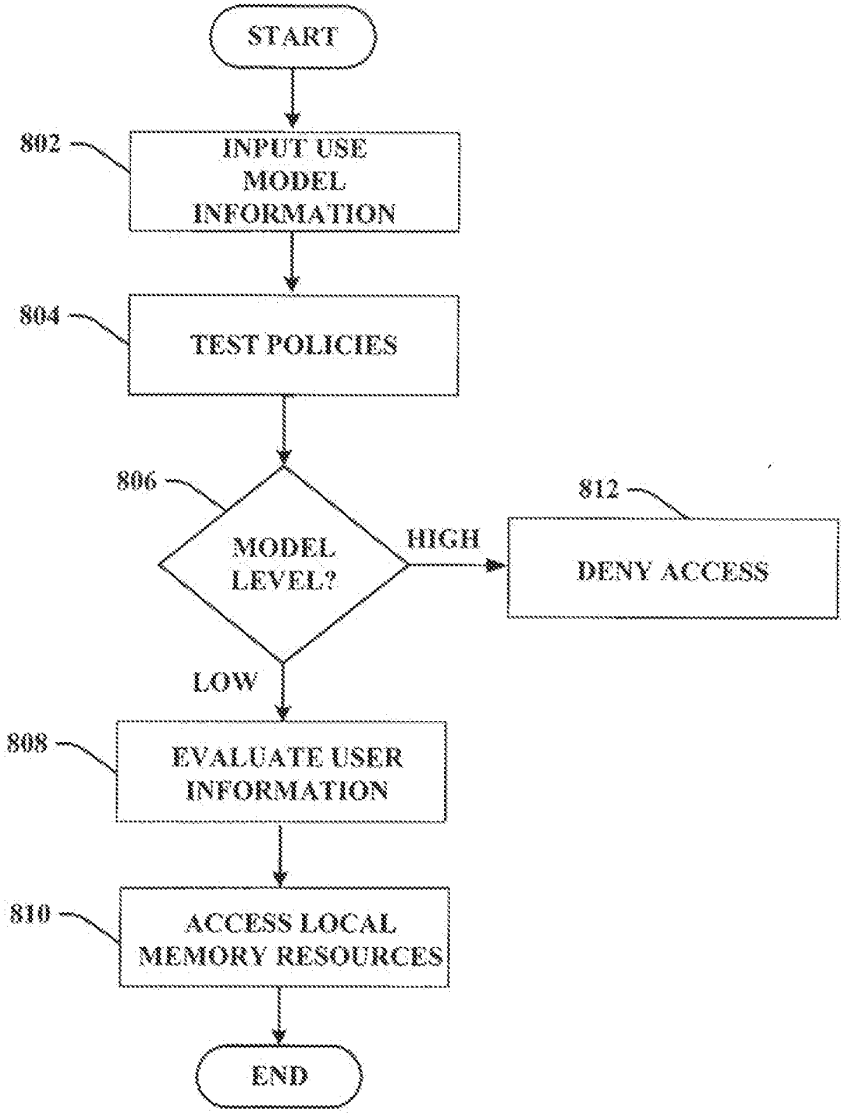

START
802
INPUT USE MODEL INFORMATION
804
TEST POLICIES
806
MODEL LEVEL?
HIGH
812
DENY ACCESS
LOW
808
EVALUATE USER INFORMATION
810
ACCESS LOCAL MEMORY RESOURCES
END

FIG. 8

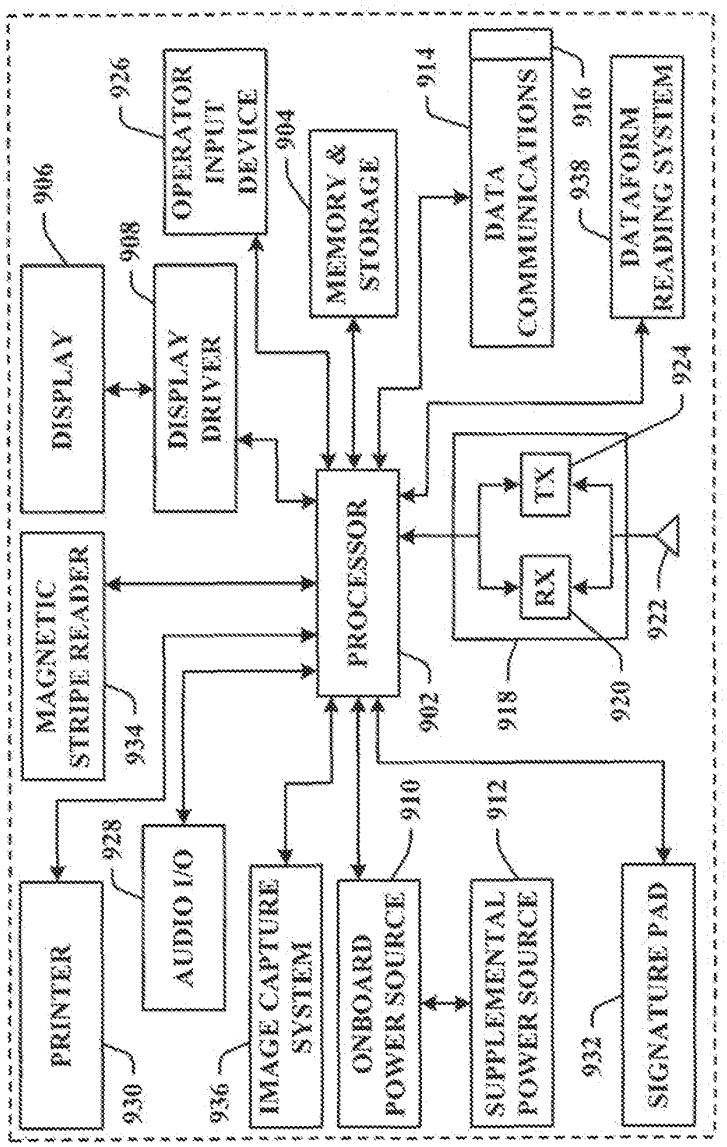

900
PRINTER
930
AUDIO I/O
928
IMAGE CAPTURE SYSTEM
936
ONBOARD POWER SOURCE
910
SUPPLEMENTAL POWER SOURCE
912
SIGNATURE PAD
932
MAGNETIC STRIPE READER
934
DISPLAY
906
DISPLAY DRIVER
908
OPERATOR INPUT DEVICE
926
MEMORY & STORAGE
904
PROCESSOR
902
RX
TX
DATA COMMUNICATIONS
914
DATAFORM READING SYSTEM
916
938
924
922
918
920

FIG. 9

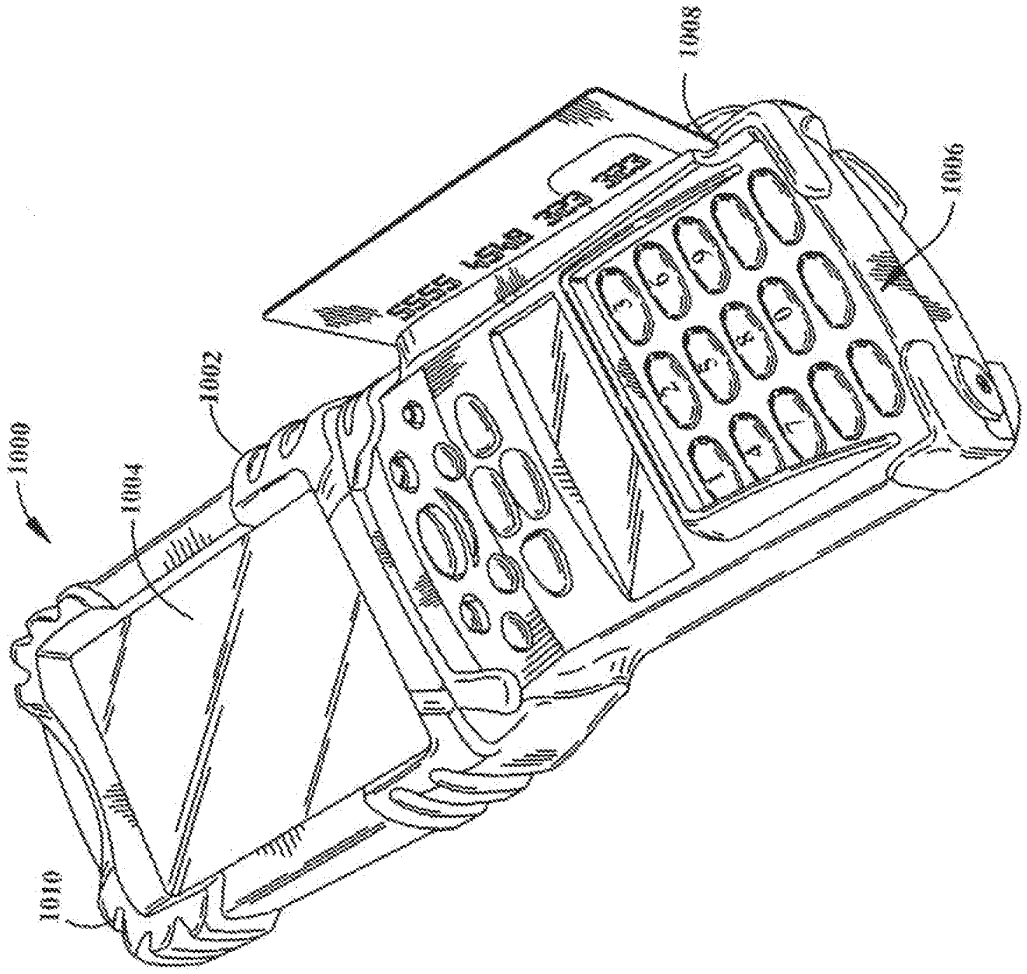


FIG. 10

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/028070 A1

(51) International Patent Classification[7]: H04L 9/00, 9/32

(21) International Application Number:
PCT/US2003/029347

(22) International Filing Date:
19 September 2003 (19.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/252,212	23 September 2002 (23.09.2002)	US
10/252,225	23 September 2002 (23.09.2002)	US
10/252,213	23 September 2002 (23.09.2002)	US
10/252,211	23 September 2002 (23.09.2002)	US

(71) Applicant: CREDANT TECHNOLOGIES, INC. [US/US]; Suite 1010, 15305 Dallas Parkway, Addison, TX 75001 (US).

(72) Inventors: MANN, Dwayne, R.; 401 Del Rio Court, Allen, TX 75013 (US). HEARD, Robert, W.; 3321 Wolfe Court, Plano, TX 75025 (US). BURCHETT, Christopher, D.; 1019 Sir Lancelot Circle, Lewisville, TX 75056 (US). GORDON, Ian, R.; 32 Melgund Avenue, Ottawa, Ontario K1S 2S2 (CA).

(74) Agents: TOLER, LARSON & ABEL, LLP, ET AL., et al.; 5000 Plaza on the Lake, Suite 265, Austin, TX 78746 (US).

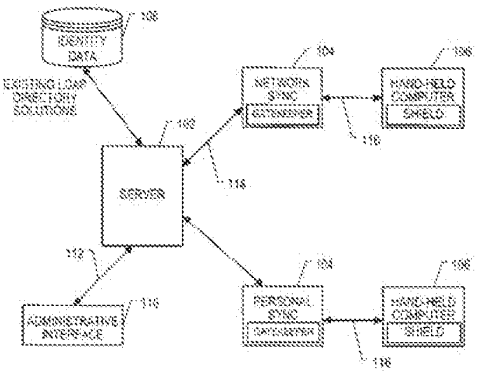
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, 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: SERVER, COMPUTER MEMORY, AND METHOD TO SUPPORT SECURITY POLICY MAINTENANCE AND DISTRIBUTION



(57) Abstract: In a particular embodiment, a server module deployed on a server (102) is disclosed. The server module is connected to a wireless network access node (104). The server modules includes a database (108) containing user information for multiple wireless devices (106). Each element in the database (108) is attributable to at least one authorized wireless device (106) and contains at least one type of data file from the following group: (i) wireless connectivity permissions, (ii) authorized wireless device identification, and (iii) authorized network access node information.In another embodiment, a method of enforcing security policies at a mobile computing device (106) is provided. The method includes receiving a policy at the mobile computing device (106) and enforcing the policy at the mobile computing device (106) by disallowing a user of the mobile computing device (106) from engaging in the use precluded by the use limitation. The policy includes at least one device use limitation.

WO 2004/028070 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.

SERVER, COMPUTER MEMORY, AND METHOD TO SUPPORT SECURITY POLICY MAINTENANCE AND DISTRIBUTION

BACKGROUND

Field of the Invention

The present application relates to systems and methods of distributing and enforcing security policies.

Description of the Related Art

The use of mobile devices, such as personal digital assistants (PDAs), in corporate environments is projected to grow significantly over the next 3-5 years. These smart devices are increasing in diversity and capability as well as number. These devices offer a unique blend of lightweight mobility, convenience and functionality providing an instant-on access to information such as email, calendar, address book and other documents. Many enterprises are developing or have deployed special applications for mobile devices that transform the platform into a mission critical tool and repository for sensitive corporate data.

As a result, mobile devices have become indispensable tools for business communications. The use of these devices is expected to grow rapidly according to industry experts.

The prevalence and power of mobile computing devices and the increasing availability of wireless connectivity represents a paradigm shift in how people will use computers and access data. The current use and diversity of these devices are impacting the integrity of corporate IT infrastructures in many ways. These devices connect to the corporate network in multiple, unsecured and difficult to monitor transient ways. Cradles are used to 'synch' the devices to laptops or desktops using serial or USB lines. Modems and wired or wireless networks are used. Cell phones are converging with PDAs to provide

a new generation of devices that may access corporate data in an expanding network of advanced cellular access points. Finally, since these devices have significant storage, computing power and operate in a connected and disconnected mode, security management and control of these devices remains an important challenge.

Mobile devices provide an "open door" into the enterprise, especially if lost or stolen. A variety of sensitive information may reside on these devices including passwords and access codes for most corporate databases, network files and applications. These pocket-size devices have become the "password sticky note" of the 21st century. In a wireless "always-on" world, these devices can enter and exit numerous unknown and ad hoc networks in a single day. At industry tradeshows, cyber-cafes or industry networking environments, corporate data is especially exposed to unauthorized access.

These devices have become large walking repositories for business confidential information. Mobile professionals frequently synch or copy proprietary corporate information from laptops, such as financial results, launch plans, personnel information, client records or application specific information. The large memory capacity of mobile devices and the plummeting price of after market memory cards make it more likely that users will store additional information on their devices.

The emerging corporate use and capabilities of these devices make unique challenges for an enterprise scale mobile security solution. Because mobile devices often operate in a disconnected mode, on-device policy enforcement is required.

The number of mobile devices entering the enterprise and the complexity of the security requirements is placing an increased demand on the enterprises ability to manage and enforce corporate security on mobile devices. Many information technology (IT) departments do not know how many non-company issued devices are currently being used by employees. They have no tools to restrict these devices from accessing corporate data. Simply put, current IT departments are not equipped to respond to the emerging computing standard of the mobile device.

Accordingly, there is a need for an improved system and method of handing security policies with respect to mobile devices.

SUMMARY

In a particular embodiment, a server module deployed on a server that is connected to a wireless network access node is disclosed. The server module includes a database containing user information for multiple wireless devices. Each element in the database is attributable to at least one authorized wireless device and contains at least one type of data file from the following group: (i) wireless connectivity permissions, (ii) authorized wireless device identification, and (iii) authorized network access node information.

In another embodiment, a computer memory is disclosed. The computer memory includes a plurality of operating keys for use in connection with security features of a mobile computing device and a root key. The root key is to encrypt the plurality of operating keys.

In another embodiment, a method of enforcing security policies at a mobile computing device is provided. The method includes receiving a policy at the mobile computing device and enforcing the policy at the mobile computing device by disallowing a user of the mobile computing device from engaging in the use precluded by the use limitation. The policy includes at least one device use limitation.

In another embodiment, a security method is provided. The security method includes receiving a password from a user of a mobile computing device; deriving a security code from the password by applying a non-linear function; and encrypting the security code using the password as an encryption key.

In another embodiment, a method of selectively providing a mobile computing device with access to a software application on a server is provided. The method includes receiving a request to access the software application from the mobile computing device and determining whether to grant access to the software application by checking whether the mobile computing device has an installed security program.

In a further embodiment, a method of updating policies and key materials is provided. The method includes providing a shared encryption key that is shared by a server and a client module; encrypting data on the client using the shared encryption key; authenticating a user of a mobile computing device by receiving a password, where the client is resident at the mobile computing device; decrypting the shared key using the

password; using the shared key to decrypt updated policies and key materials; and replacing policies and key materials at the mobile computing device with the updated and decrypted policies and key materials.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of an embodiment of a system for use in providing security policy distribution and mobile device management.

FIG. 2 is a block diagram of an embodiment of a server within the system of FIG. 1.

FIG. 3 is a general diagram that illustrates software layers within the server of FIG. 2.

FIG. 4 is an illustrative screen shot of an administrative user interface for use with the server of FIG. 2.

FIG. 5 is a block diagram that illustrates functional elements within the gatekeeper of FIG. 1.

FIG. 6 is block diagram that illustrates elements within the shield application of the system of FIG. 1.

FIG. 7 is a flow chart that illustrates installation of the shield security application onto mobile devices.

FIG. 8 is a flow chart that illustrates a method of updating policy information and distributing the updated policy information to a mobile device.

FIG. 9 is a flow chart that illustrates another method of updating policy information and distributing the updated policy information to a mobile device.

FIG. 10 is a diagram that illustrates key materials and specific key field formats for use with encryption of policy information.

The use of the same reference symbols in different drawings indicates similar or identical items.

DETAILED DESCRIPTION OF THE DRAWINGS

Referring to FIG. 1, a system 100 for use in enterprise security management is disclosed. The system 100 includes a server 102, a gatekeeper 104, and a client device module 106. The client device module 106 that is used to provide security functionality is also referred to as a shield. The system 100 is a comprehensive enterprise security management software platform for diverse mobile operating systems, applications and devices. The system 100 enables an organization to secure and manage mobile devices easily and cost effectively. The server 102 integrates with existing security policy management systems and allows administrators to centrally create new mobile security policies by extending existing security policies and to distribute them to a diverse population of mobile devices. The server 102 and gatekeeper 104 work together to automatically and securely push these security policies to a specified mobile device. The shield 106 is a trusted computing environment on the mobile device that enacts and enforces the distributed security policies, controls access to the mobile device, and provides data security.

The server 102 may be implemented as a web-based application server that provides central creation and management of mobile security policies. The server 102 is preferably implemented with portability, scalability and maintainability in mind using industry standards such as Java, XML and other advanced web technologies. To provide easy control and accessibility, an administrative interface to the server 102 is provided through a secure browser interface allowing the simple delegation of responsibilities and access by any workstation or PC on a local network connected to the server 102.

A consolidated LDAP directory (CLD) technique may be used to integrate the server 102 with existing enterprise security infrastructure, such as an existing identity database 108. Existing policy and identity management systems are integrated through a real-time interface to directory resources. A layer in the server 102 provides a consolidated view of the external LDAP services and extends these services through policy inheritance and over-riding. As a result, existing identity directories, such as directory 108, can be used without copying data and without changing the data schemas of the existing enterprise security systems.

The data passed to the gatekeeper 104 and subsequent mobile devices 106 is derived from security role and is protected through a combination of secure socket layer (SSL) and data encryption. Mobile security policies are formed using the administration interface 110, which is coupled to the server 102 via interface 112, to set and extend policies in a consolidated directory (e.g., LDAP). Once policies are set, a policy package is generated for each user within a role, encrypted with the specific users' encryption key, and forwarded to the gatekeeper 104 for installation on the target mobile device 106. Policy package encryption forms a main pillar of system security. Additionally, SSL communication is used for added privacy and authentication between the server 102 and the gatekeeper 104 over the secure interface 114. The system 100 is designed for robust security management to provide many advanced security features including: centralized management of disconnected devices, automatic versioning and distribution of policies, role-based policy creation and management, seamless integration with existing role repositories and security infrastructure, delegated security management, separation of administrative duties, automatic retrieval of device audit logs, consolidation, alerting and reporting, and mobile device management.

The gatekeeper 104 may be implemented as a security management software agent that forms a virtual security layer on existing, third party synchronization systems, such as HotSync, ActiveSycn, and ScoutSync. A function of the gatekeeper 104 is to receive policy packages from the server 102 and install the packages on target mobile devices 106. The gatekeeper 104 operates in two modes to support local and network synchronization. In local mode, the gatekeeper 104 executable operates on desktop and laptop computers forming a security layer on top of personal synchronization tools. In network mode, the gatekeeper 104 executable operates on an enterprise server and forms a security layer on top of a network synchronization application. When the gatekeeper 104 is deployed, mobile devices 106, such as personal digital assistants (PDAs), are required to authenticate and to request permission to synchronize before the third party data synchronization tool is allowed to launch. Additionally, the gatekeeper 104 provides for automatic installation of the mobile shield on specified PDAs, application configuration, update and patch management, mobile device configuration management, monitoring, management, and control access to synchronization application, and distribution of device policies, permissions and configurations.

The mobile device application, i.e., shield, 106, may be implemented as a trusted computing environment operating as a software layer on top of the mobile device operating system. Security policies are received from the gatekeeper 104 using a two-way authentication process. The policies are used by agent software at the mobile device to encrypt data, and to monitor and control device access, device peripherals, and device software and hardware operations. The mobile device trusted environment approach provides many security features, including: on-device policy enforcement whether connected or disconnected, mandatory access control, data encryption with secure recovery, mandatory synchronization authentication, controlled application access and use, control over hardware ports – infrared (IR), compact flash (CF), universal serial bus (USB), secure digital (SD), multiple profiles – personal and business, and secure audit logs. Sample devices that may accept shield software include personal devices made by Palm, Handspring, Sony, Compaq iPaq, and the HP Jornada 500 series.

To summarize, all three major components of the system 100 interoperate substantially seamlessly and transparently to the user to enable a secure mobile environment without materially deterring from the user's experience. The server 102 virtually consolidates external LDAP identity and policy data to integrate to existing security infrastructure. The administrative tools on the server 102 allow policy packages to be automatically formed and distributed to each mobile device 106. The gatekeeper 104 monitors synchronization and installs the shield software and policy packages on targeted devices. Finally, the shield forms a trusted computing environment by forming a security layer on the mobile operating system to enforce the policies originating from the server 102. The complete system 100 forms a comprehensive, enterprise scale mobile security management system.

The system 100 includes components that integrate to external systems. To support a large customer base, multiple platforms are supported for each component. The following sample list identifies illustrative devices and software platforms for integration. At the server 102, the windows2000 operating system, an LDAP of MS Active Directory System (ADS), Critical Path, or iPlanet flat files, and the Explorer version 5.0+ browser. At the gatekeeper 104, compatible operating systems include Win98, WinNT 4.0, Win2000, WinXP, compatible data synchronization software includes HotSync, ActiveSync version 3.1+, server operating system of Win2000, and the network synchronization of ScoutSync

version 3.5+. For the shield, the supported operating systems include PocketPC 2000, PocketPC 2002, and device OS version 3.5+.

The server 102 is constructed using enterprise scale server technology, such as federated webservices to provide scalability servers and portability of functions, model-view-controller (MVC) web interface techniques to provide maintainability and speed, and consolidated LDAP Directory (CLD) technology to provide compatibility and reduce installation and administrative costs in existing security infrastructures.

The server 102 architecture is integrated through a web service paradigm, as illustrated in FIG. 2. This paradigm is an industry recognized best practice for developing and integrating enterprise web applications. The web service paradigm is a loosely coupled architecture of processes that is flexible, allows additional functions, and allows replacement of servers as well as increased scale through load balancing and additional servers.

The core of the web services approach is in the ability to expose or advertise services through a consolidating interface. Referring to FIG 2 many of the key functions of the server 102 such as access control, audit log and security policy management are implemented as individual Java "applications" and advertised or exposed to the internal local area network (LAN) as services. These "applications" operate as web services. Each service can be run as a process or thread on a shared server, on separate servers or in combinations on fewer servers. Scalability and load balancing is achieved by running multiple threads of a service on a single server or on a cluster of servers. Maintenance is simplified by supporting the ability to move services between servers and to replace servers dynamically.

The federating web service in FIG. 2 is a proxy type of service that consolidates the internally advertised services and provides the corresponding service to an external user through a hyper-text transfer protocol (HTTP) interface. The federated web service consolidates internal services by proxying the functionality to external users. The location of the services is specified in a service table or configuration file formatted with eXtensible markup language (XML). Service management is an advantage to the federated services approach. Only a single URL needs to be maintained to provide service to a scalable cluster of servers and services. The federating service has the ability to route application calls

dynamically to perform load balancing. Scalability of the federating service is achieved using multiple federating service servers and standard load balancing routers such as Cisco's LocalDirector router.

The federating services and external users may be integrated through industry standard scripting protocols XML (eXtensible Markup Language) and SOAP (Simple Object Access Protocol). XML is a markup language similar to HTML for web pages, while SOAP is composed with structures or sentences written in XML. With web services, XML is the alphabet that represents data while SOAP is the grammar that defines the service call similar to a remote function call. Specifically, XML provides a tagged markup language that allows portable data representation between services. SOAP is an industry standard structure of XML tags that define calling sequences, parameter structures and result variables. These protocols are supported over the ubiquitous HTTP communication channels of the web.

As a result, XML/SOAP allows an external application, such as the gatekeeper 104, to request a service as a single federated web service URL, to proxy the result to the actual web service and to provide the result back to the gatekeeper 104. Privacy and authentication of the gatekeeper 104 can be achieved using SSL services by using the standard HTTPS protocol in place of HTTP.

The administrator interface 112 is provided through use of a lightweight HTTP or web interface. Benefits of this configuration includes wide availability of access from anywhere in the LAN, secure usage through SSL protocol, as well as simple delegation of responsibilities and separation of duties through authentication and access control.

The server 102 uses the industry recognized best practice of MVC programming model to implement the graphical user interfaces (GUI) of the administrator console. Model View Controller (MVC) is similar to web service in that it is a method of providing remote function calls. MVC leverages the federating web service to manage resources. However, MVC provides an additional capability to graphically represent the results of the service to provide a web page representation and a GUI.

MVC is the modern evolution of CGI for calling functions from web pages. The CGI approach used a myriad of println() calls to return HTTP data back to the browser for

display. Servlets are a server side Java application that perform a specific task and that do not have GUI capabilities. The servlets were used to manage flow while JSP managed the HTML formatting. The MVC model separates servlets into logic (or model) servlets and control servlets resulting in the acronym MVC.

The server 102 uses MVC to implement the GUI. A view component is used to format and represent GUI to the browser. JSP and HTML are used to implement the view component. A controller component is used to consolidate, delegate and manage control flow and may be implemented with a Java servlet controller using HTTPS with the federated web service. Finally, the controller delegates work to an appropriate model within the server 102. The model may be implemented as a servlet in Java. The models are used to control setting of policies, accessing roles stored in the LDAP and forming policy packages for distribution. The entire GUI including operation and logic is controlled and managed by the MVC framework. The framework is quickly implemented, and is easily modified, expanded and maintained.

Simplifying and lowering the total cost of ownership of the mobile security management system is a goal in the design of system 100. A challenge and cost of installation is integration with existing identity data management systems. LDAP is data directory structure that is commonly used to store identity information and security policies to support authentication and authorization systems. It is understandable that customers want to reuse existing LDAP repositories after investing the time and effort to create an LDAP role-based policy system and populate the system with every user in the company. Furthermore, customers may desire future security systems to use the existing LDAP repositories without compromising the integrity of the system by modifying any database schemas.

The server 102 uses a consolidated LDAP directory (CLD) technology to address this integration challenge. The server 102 uses a layering approach and places a virtual layer above external and internal LDAP systems to provide a federated view of LDAP repositories. FIG. 3 illustrates this approach.

The federation works with three layers. The bottom layer 302 is an adapter layer that is specific to a data store format and converts the store representation to a portable format. The middle layer 304 is a core directory engine that performs on-the-fly mapping to

transform top-level client requests into the context of each repository and results into federated representations. The top level 306 is a front-end listener that converts the directory engine results into proper LDAP format. The result is a powerful method for integrating disparate customer identity data stores into a unified view for simplified server installations.

An access control service provides authentication for administrator logins and for gatekeeper 104 communications. This service interfaces to the LDAP repository of identities and permissions to provide control for system and data access. Administrators are authenticated through a login screen presented by a browser with JSP. The JSP requests authentication with the user name and password through the servlet interface of the federated service. The request is proxied to the access control service for completion. The authentication may be performed with LDAP version 3 operations through the CLD and may alternatively be performed using private key encryption type authentication systems.

The gatekeeper 104 is authenticated using SSL server certificates and realm authentication. An SSL connection is created to provide communications between the server 102 and gatekeeper 104. Initially, the server 102 is authenticated to the gatekeeper 104 through SSL certificate authentication. Next, an SSL channel is constructed for privacy. Finally, a name/password pair (per realm authentication) is passed to through the federated service to the access control service for authentication. Successful match of name and password provides authentication of the gatekeeper 104 to the server 102.

A policy service provides management of the role-based policies as well as creation of the policy files. The policy management service is provided to the administration console and allows definition of the policy values for both roles (or groups) and individual users. Once the policies have been defined for a population of users, the administrator can select to publish the policies. The publication process is the act of forming the secure policy files and automatically pushing the policy files out to the individual shield application 106. An example screen shot of the policy management service is shown in FIG. 4.

The system 100 provides a key management service that generates and archives password keys for encryption operations in the shield 106. Symmetric encryption keys are generated using techniques such as industry standard X9.17. Symmetric keys are used to protect data on the mobile device. These data encryption keys are generated uniquely for

each mobile device and are stored on both the server 102 and the shield 106 to enable data protection while allowing secure data recovery with administrator intervention. Asymmetric or public/private key pairs are created with the elliptical curve cryptography (ECC) key algorithm and are used to encrypt policy files and audit log files. Separate key pairs are generated for each device and individually for the policy files and the audit logs. The key pairs are stored on the server 102 for secure data recovery through administrator intervention. The private audit log key is stored on the shield 106 to encrypt audit log information to support transference off of the device. The public policy file key is stored on the shield 106 to allow the software to authenticate and extract the policy items from the encrypted policy files. The opposite keys are used on the server 102 to decrypt audit log files and to encrypt policy files in support of the device.

A policy file is a collection of policy items combined into a single data package and formatted with XML. The policy file is transferred from the server 102 to the mobile device for security configuration and enforcement. The policy file is actually a number of files; one main index file and another for each category of policies defined. Each category file contains a series of policies that define the permissions and behavior of the shield 106. Three items define each policy: category, key and value name. A key may have zero or more name/value pairs associated with it.

The server 102 encodes the policy file with ECC asymmetric encryption and transfers the file to the mobile device. The key pair corresponding to the policy management of an individual mobile device is created and managed by the server 102. The private key is stored on the server 102 and used to encrypt the policy file. The public key is stored on the mobile device by the shield application 106. The policy file is transferred to the mobile device during synchronization, after authentication is performed. The public key stored in the shield is used to open the policy file. The public key is passed to the shield application in a secure manner. This method of policy file management provides private transfer to specific shield deployments, provides policy authentication and management, and is tamper resistant to enable consistent policy enforcement.

Policy data falls into the following categories: I/O, storage, applications, and authentication.

The following tables specify sample types of policy data:

Permission Policies

Name	ID (Category)	Value	Type	ReadOnly	Affects
IR_Enable	I/O	True/False	Boolean	True	Palm: Exchange Manager, IR Library CE:
TCPIP_Enable	I/O	True/False	Boolean	True	Palm: Network, INet Library CE:
NetBios_Enable	I/O	True/False	Boolean	True	Palm: N/A CE:
SyncAuthenticated_Required	I/O	True/False	Boolean	True	Palm: CE:
VolumeMount_Enable	Storage	True/False	Boolean	True	Palm: DB, VFS Manager (File system mounting) CE:
DateBook_Enable	Applications	True/False	Boolean	True	Palm: DateBook CE: Calendar
AddressBook_Enable	Applications	True/False	Boolean	True	Palm: AddressBook CE: Contacts
Todo_Enable	Applications	True/False	Boolean	True	Palm: Todo CE: Tasks
Memo_Enable	Applications	True/False	Boolean	True	Palm: Memo CE: Notes
Expense_Enable	Applications	True/False	Boolean	True	Palm: Expense CE: Money
Mail_Enable	Applications	True/False	Boolean	True	Palm: Mail CE: Inbox
Prefs_Enable	Applications	True/False	Boolean	True	Palm: Prefs CE: Settings
Security_Enable	Applications	True/False	Boolean	True	Palm: Security CE: N/A
FileExplorer_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: File Explorer
InternetExplorer_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Internet Explorer
PocketWord_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Pocket Word
PocketExcel_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Pocket Excel
WindowsMedia_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: Windows Media
Reader_Enable	Applications	True/False	Boolean	True	Palm: N/A CE: MS Reader

Rule Policies

Name	ID (Category)	Value	Type	ReadOnly	Description
PINEnable	Authentication	True/False	Boolean	True	Whether to include PIN authentication in the password hierarchy
PasswordEnable	Authentication	True/False	Boolean	True	Whether to include Password authentication in the password hierarchy
PassPhraseEnable	Authentication	True/False	Boolean	True	Whether to include Pass Phase authentication in the password hierarchy
ManAuthEnable	Authentication	True/False	Boolean	True	Whether to include PIN authentication in the password hierarchy
PasswordNumChars	Authentication	8-16 characters	Number	True	
PasswordAlphasRequired	Authentication	True/False	Boolean	True	
PasswordNumericRequired	Authentication	True/False	Boolean	True	
PasswordSpecialRequired	Authentication	True/False	Boolean	True	
PasswordUpperCaseRequired	Authentication	True/False	Boolean	True	
PassPhraseNumChars	Authentication	16-32 characters	Number	True	
NumPINAttempts	Authentication	1-4	Number	True	
NumPasswordAttempts	Authentication	1-4	Number	True	
NumPassPhraseAttempts	Authentication	1-4	Number	True	
NumManAuthAttempts	Authentication	1-4	Number	True	
UserSessionTimeout	Authentication	1-120 minutes	Number	True	Inactive time till user must re-authenticate
PowerOffTimeoutEnable	Authentication	True/False	Boolean	True	Requires user to re-authenticate after device has been turned off
AuthDataExpires	Authentication	1-365 days	Number	True	Time till user must reset authentication information

The system 100 also provides a logging service. Each event defined in the logging service has a corresponding registered policy. This will enable the administrator to control which events are written to the audit logs.

A log file is a record of events that is generated by the shield software 106. The shield 106 initially stores the file locally. During synchronization, the log file is automatically transferred through the gatekeeper 104 to the server 102. After synchronization, the shield 106 initializes a new file. The server 102 automatically appends the new log to the previous synchronized logs to form a consolidated log. Server access to the log is provided through an open database connectivity (ODBC) interface to allow custom or third party reporting tools to be used.

The log files are locally protected against tampering with elliptical curve algorithm asymmetric encryption. The key pair corresponding to the on-device audit logs of an individual mobile device is created and managed by the server 102. The public key is stored on the server and used to open the audit log after synchronization. The private key is stored on the mobile device by the shield application 106 and is used to add new event records to the event log. An initial value or seed is transferred from the server 102 to the mobile device in a secure mode during synchronization. This seed is updated through the encryption process as records are added to the audit log. This forms an encryption thread through the event recording process. Additionally, a time stamp from the server is used to initialize the file. The initial time stamp combined with periodic time events in the file allows monitoring of the mobile device clock to prevent time tampering. This method of on-device audit logging provides a secure and private audit log that is easily maintained by the server, detects gaps in time and in logging sequence, and is tamper resistant to provide a robust, on-device monitoring system.

Referring to FIG. 5, an illustrative functional diagram for the gatekeeper 104 is disclosed. The gatekeeper 104 includes a persistence network 502, a server interface 504, a client interface 506, an encryption module 508, an audit module 510, a synchronization plug-in module 512, and an authentication module 514. The gatekeeper 104 communicates with the server 102 using HTTPS and XML over the interface 114 and communicates with the mobile device 106 via the synchronization interface 116, such as with SKID3 and XML.

Referring to FIG. 6, an illustrative block diagram for the shield application 106 on a representative mobile device is shown. The shield application 106 includes a communication module 602, a storage area 604, a user interface 606, encryption module 608, audit and log module 610, policy rule engine 612, and system interface 614.

The communication module 602 communicates with external systems such as the gatekeeper. The communication module receives application data, personal information data (PIM), new key materials and policy data from the gatekeeper 104. The application data and PIM data are stored in the general device storage 604. This general storage may be encrypted by the encryption module 608. The new key materials are decrypted by the encryption module 608 and stored in the key data store in 608. The policy data is decrypted by the encryption module 608 and stored in the rules engine store 612.

The user interface module 606 communicates with the device user to authenticate the user and unlock the device. The user interface may retrieve any of a plurality of data such as PIN (personal identification number), password, answer to a question or response to a challenge. Authentication is tested by decrypting data in the encryption module 608 with the retrieved data. Upon successful decryption, authentication is approved. A similar authentication test can be hashing the retrieved information and comparing the information with data stored in the encryption module 608. The user interface 606 also displays alerts such as sync in progress or device is locked.

The audit log module 610 stores system event data, such as successful or unsuccessful authentication attempts, in the encrypted log store of 610. The events are encrypted by the encryption module 608 and transferred to the gatekeeper 104 by the communications module 602.

The rules engine 612 provides authorization based on the policy data in its store. The policies are retrieved from the communications module 602 during connectivity to the gatekeeper 104 and enforces the policies at all times whether connected or disconnected. The policy data is retrieved from the gatekeeper 104 by the communications module 602 in an encrypted form. The encryption module 608 decrypts the data prior to storage on the policy data store in 612. The rules engine receives authorization requests from a plurality of modules and responds with authorization based on the policies stored within. The policy engine can signal the user interface 606 to lock the device if a user action is denied or an unauthorized event occurs.

The rules engine 612 can enforce which devices to which the communications module 602 can communicate. The policy database may contain a list of devices that can be communicated with, a list of devices that cannot be communicated with or a list of keys

stored in the encryption module 608 with which can be used to authenticate devices. If an external device is included in the list of approved devices to communicate with, the rules engine 612 grants authorization to the communication module 602 to communicate with the external device. If an external device is included in the list of disapproved devices to communicate with, the rules engine denies authorization to the communications module 602 to communicate with the external device. If a plurality of keys is listed in the policy database, then the rules engine can request the encryption module 608 to perform a challenge response with an external device to determine authentication. If the authentication is successful, the rules engine 612 may grant authorization to the communications module 602 to communicate with the external device. Otherwise, the rules engine may deny authorization to the communications module 602 to communicate with an external device.

The rules engine 612 and user interface 606 can enforce a personal or business mode. The user interface 606 can authenticate a user in either personal mode or business mode. The mode is determined from the data retrieved from the user interface indicating which mode the user requests. The rules engine authorizes what actions can be performed in each mode. Additionally, the rules engine can authorize which data items in the general data store 604 can be displayed by the user interface 606, can be accessed by a plurality of modules, or can be transferred by the communications module 602.

The system interface 614 communicates using intercepted events with an external event handler, such as OS event handler 630 and communicates, by intercepting system calls, with external operating systems, such as OS 632. The system interface 614 authorizes system calls and events by intercepting the system calls and events, requesting authorization from the policy engine 612, and granting or denying the system calls or events.

Referring to FIG. 7, a method of distributing security software from the server 102 to a mobile computing device is illustrated. First, gatekeeper software 104, including network scripts, policies, and key materials, is installed from the server 102 to a desktop computer, or other suitable gatekeeper platform, at 702. When the mobile computing device connects to the gatekeeper 104 during a data synchronization event, the shield software application 106, i.e., security software for the mobile computing device, is installed from the gatekeeper 104 to the mobile computing device, at 704. The gatekeeper 104 requests a one-

time use password from the server 102, at 706. The server 102 emails the one-time use password to the user of the mobile computing device, at 708. The mobile computing device user can then use the one-time password to complete installation of the security shield application.

At this point, the root key for the key pack is decrypted using the one-time password, allowing access for the user to enter a new password, a personal identification number (PIN), and a password phrase, and optionally other user identification information, such as the user's mothers maiden name or pet name, at 710. The root key is then encrypted using each of the above user information entries, including the new password, the PIN, the phrase, and the user's answers to key questions, at 712. The above process of having a mobile computing device user initiate security operations may be accomplished using user interface software, such as by providing prompting screens to facilitate entry of the user information.

Referring to FIG. 8, a method for distributing a new or modified security policy information to a mobile device is illustrated. At 802, a policy change or a new policy is added by an administrator connected to the server 102 and the server 102, in response to the administrator request, creates a new policy package. The policy package contains the new or modified policy. To distribute the new policy package to the mobile computing device, the server 102 authenticates a connection with the gatekeeper 104 and upon successful authentication, sends the policy package to the gatekeeper 104, at 804.

The authentication between the device and gatekeeper may be implemented using a mutual challenge-response algorithm that uses a shared key as a shared secret for determining authentication. The process is a two step challenge-response that may begin with ether the device or the gatekeeper. Consider an example where the device initiates the challenge. A random number is calculated by the device and sent to the gatekeeper as a challenge. The gatekeeper and the device compute the expected answer in parallel and in private. The answer can be calculated by any one way function of the shared key and challenge value. For example, the key can be appended to the challenge and input to a hashing algorithm such as MD5 for calculation of a message digest. The gatekeeper responds to the device by returning the computed response. If the response matches the expected answer, the first step or phase of the mutual challenge response is completed successfully and the gatekeeper calculates a random number for the return challenge. The

next step repeats the first step but in reverse roles. The gatekeeper challenges the device with the random number. Each computes the expected response privately. The device returns the calculated value as the response. If the values match, then the second phase is passed. If either phase fails, then the entire process is failed. Both steps must pass in order to be successful.

The gatekeeper 104 receives the policy package and waits for the next data synchronization communication with the mobile computing device, at 806. When the mobile computing device initiates data synchronization, at 808, the gatekeeper 104 authenticates the mobile computing device. The gatekeeper 104, upon successful authentication of the mobile computing device, pushes the policy package to the mobile computing device, at 810. The mobile computing device then decrypts the policies and activates the new or modified security policies, at 812. If authentication of either the gatekeeper 104, from the server 102, or the mobile computing device from the gatekeeper 104 fails, then the updated policy package is not distributed and the administrator may be notified.

Referring to FIG. 9, a method where a mobile computing device requests policy updates is shown. In this method, the mobile computing device initiates synchronization with the gatekeeper 104, at 902. The connections between the mobile computing device and the gatekeeper 104 and between the gatekeeper 104 and the server 102 is authenticated, at 904. After successful authentication, the gatekeeper 104 checks the server 102 for new policies, at 906. The server 102 creates a policy package based on new and modified policies and sends the policy package to the gatekeeper 104, at 908. The gatekeeper 104 installs the new and/or modified policies onto the mobile computing device, at 910. At the mobile computing device, the security application (i.e., the shield application 106) decrypts the policy package and activates the new or modified policies on the mobile computing device, at 912.

Referring to FIG. 10, the key materials and the use of the key materials to provide for security applications is illustrated. A sample key 1002 with a plurality of fields, including the software field 1004, the date field 1006, the owner field 1008, the length field 1010, the key ID 1012, and a cyclic redundancy check field 1014 is shown. Also shown is a root key 1016. The root key 1016 is encrypted using a user's PIN 1018, password 1020,

phrase 1022, and challenge 1024 (i.e., answer to key questions). The root key 1016 is then used to encrypt a set of operating keys 1036 referred to as a key ring. The operating keys 1036 include a data key 1038, a policy key 1040, a log key 1042, a gatekeeper authentication element 1044, an updating key 1046, and a heartbeat log key 1048. The data key 1038 is linked to unlock data storage 1054 within the mobile computing device. The policy key 1040 is used to access policies 1050 and the log key 1042 is used to access log files 1052 that track historical mobile device user activities.

The log key is the public key used with a public key encryption algorithm to encrypt data into the event log that tracks historical mobile device user activities.

The gatekeeper authentication key is used by the device in a challenge-response algorithm to prove its identity with the gatekeeper. The key is used as a shared secret to compute the response to a challenge. The update key is used to decrypt new keys sent by the server to the device as replacements to any of the plurality of keys. The heartbeat key is used similar to the gatekeeper authentication key for authenticating between the device and the server. The challenge and response between the device and server is used as a heartbeat to monitor the device.

Also illustrated, is the policy package that includes the policy pack 1056, encrypted using the policy key, and a key material pack 1058 that has been encrypted using the root key 1016. The policy package may be pushed from the server 102, via the gatekeeper 104, to the mobile computing device 106 or may be pulled from the mobile computing device from the server 102, via the gatekeeper 104. Methods for distributing the policy package were described above with respect to FIGs. 8 and 9.

The above disclosed subject matter is to be considered illustrative and the appended claims are intended to cover all such modifications and other embodiments which fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.

WHAT IS CLAIMED IS

1. A server module deployed on a server that is connected to a wireless network access node, comprising:

a database containing user information for multiple wireless devices, each element in the database attributable to at least one authorized wireless device and containing at least one type of data file from the group consisting of: (i) wireless connectivity permissions, (ii) authorized wireless device identification, and (iii) authorized network access node information.

2. A computer memory comprising:

a plurality of operating keys for use in connection with security features of a mobile computing device; and

a root key, the root key to encrypt the plurality of operating keys.

3. A method of enforcing security policies at a mobile computing device, the method comprising:

receiving a policy at the mobile computing device, the policy including at least one device use limitation;

enforcing the policy at the mobile computing device by disallowing a user of the mobile computing device from engaging in the use precluded by the use limitation.

4. A security method comprising:

receiving a password from a user of a mobile computing device;

deriving a security code from the password by applying a non-linear function; and

encrypting the security code using the password as an encryption key.

5. A method of selectively providing a mobile computing device with access to a software application on a server, the method comprising:

receiving a request to access the software application from the mobile computing device;

determining whether to grant access to the software application by checking whether the mobile computing device has an installed security program.

6. A method of updating policies and key materials, the method comprising:

providing a shared encryption key that is shared by a server and a client module;

encrypting data on the client using the shared encryption key;

authenticating a user of a mobile computing device by receiving a password, the client resident at the mobile computing device;

decrypting the shared key using the password;

using the shared key to decrypt updated policies and key materials; and

replacing policies and key materials at the mobile computing device with the updated and decrypted policies and key materials.

7. A wireless security system, comprising:

a client module deployed on a wireless device;

a network module selectively coupled to the client module during synchronization; and

a server module coupled to the network module,

wherein the client module is adapted to authenticate use of a wireless computing device independent of the network module and the server module.

8. A method of installing a security software application from a network module to a mobile computing device, the method comprising:

providing a network module, the network module including security policies and key material, the security policies and key material communicated to the network module from a server;

when the mobile device is synchronizing with the network module, initiating installation of a security software program onto the mobile security device;

requesting a one-time password;

receiving the one-time password at the mobile computing device; and

using the one-time password to decrypt a root key associated with the key materials.

9. A method of distributing security policy information from a server to a mobile computing device, the method comprising:

authenticating a connection between the server and a gatekeeper;

sending a policy package to the gatekeeper;

initiating data synchronization between the mobile computing device and the gatekeeper;

authenticating the mobile computing device; and

sending the policy package from the gatekeeper to the mobile computing device.

10. A client module deployed on a wireless device, comprising:

a policy database including a list of authorized devices to which the wireless device may communicate.

11. A client module deployed on a wireless device, comprising:

a policy database containing at least two user profiles on the wireless device.

12. A client module deployed on a wireless device, comprising:
a policy database including rules related to wireless connectivity permissions; and
an intelligent agent for enforcing the policy database rules.

13. A client module deployed on a wireless device, comprising:
a policy database; and
an agent responsive to the policy database, the agent configured to monitor unauthorized use of the wireless device.

14. A client module deployed on a wireless device, comprising:
a policy database including at least one type of data file from the group consisting of: (i) multiple profile data, (ii) connectivity permissions, (iii) authorized wireless device identification, and (iv) authorized network access node information;
an intelligent agent for enforcing rules of the policy database; and
an activity log containing wireless connectivity history information.

15. A network module deployed at a wireless network access node, comprising:
a policy database including a list of authorized wireless mobile devices; and
an agent for enforcing rules of the policy database.

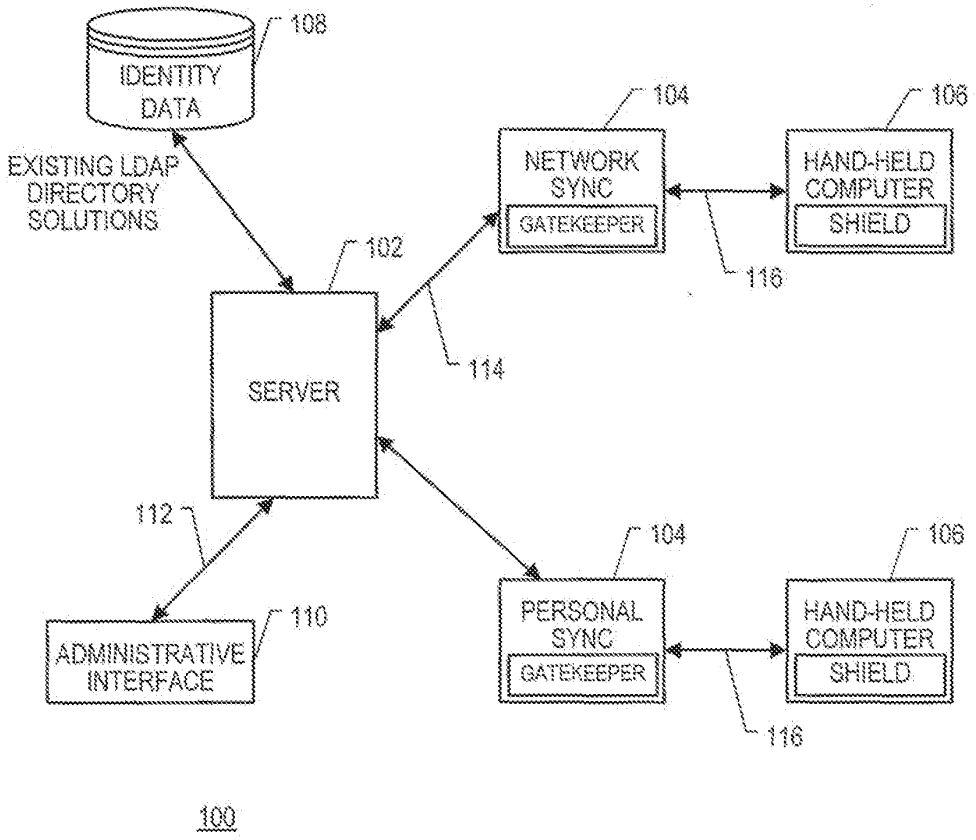

108
IDENTITY DATA
EXISTING LDAP DIRECTORY SOLUTIONS
104
NETWORK SYNC
GATEKEEPER
106
HAND-HELD COMPUTER
SHIELD
116
102
SERVER
114
112
ADMINISTRATIVE INTERFACE
110
104
PERSONAL SYNC
GATEKEEPER
106
HAND-HELD COMPUTER
SHIELD
116
100

FIG. 1

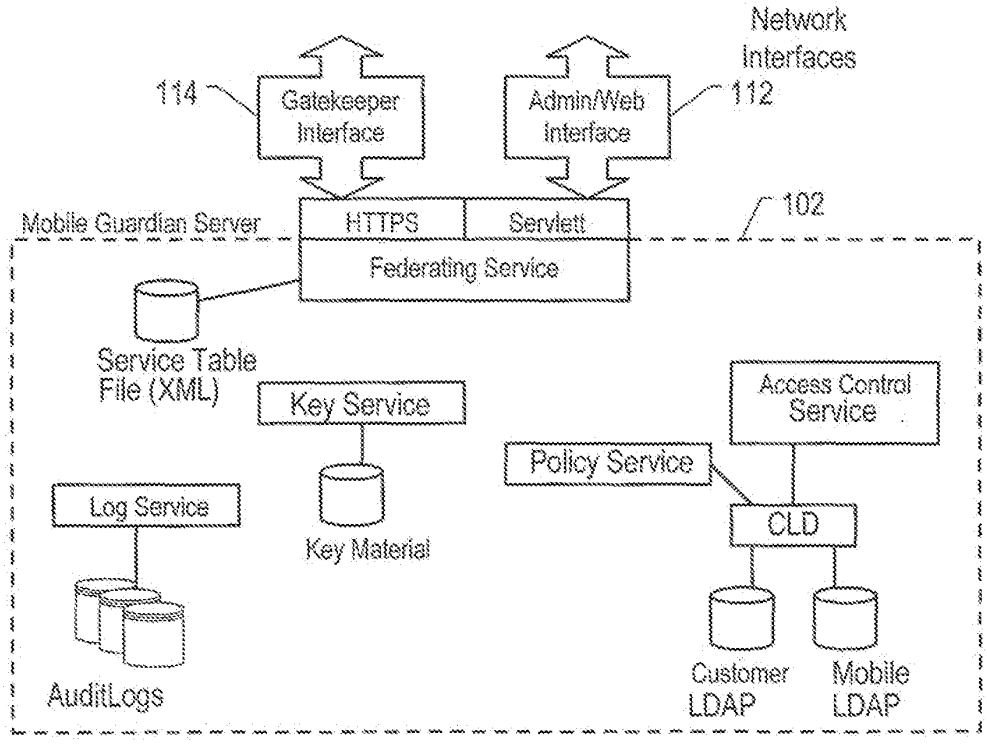

Network
Interfaces
112
114
Gatekeeper
Interface
Admin/Web
Interface
102
Mobile Guardian Server
HTTPS
Servlett
Federating Service
Service Table
File (XML)
Key Service
Access Control
Service
Policy Service
Log Service
Key Material
CLD
AuditLogs
Customer
LDAP
Mobile
LDAP

FIG. 2

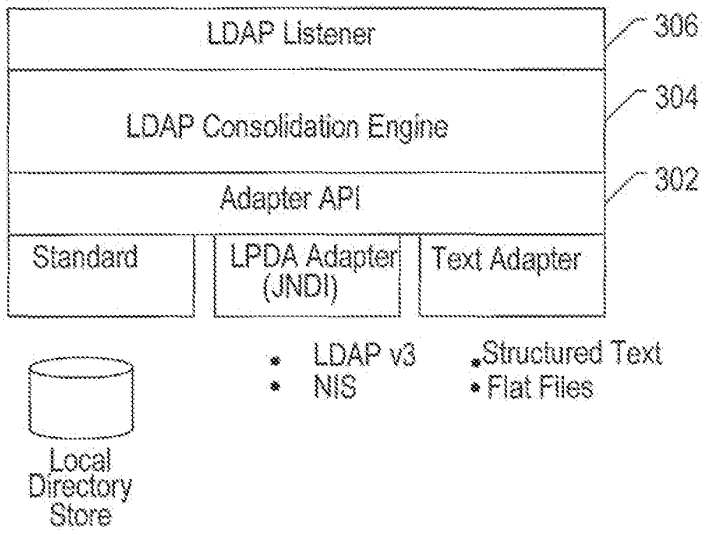

LDAP Listener
306
LDAP Consolidation Engine
304
Adapter API
302
Standard
LPDA Adapter (JNDI)
Text Adapter
LDAP v3
NIS
Structured Text
Flat Files
Local Directory Store

FIG. 3

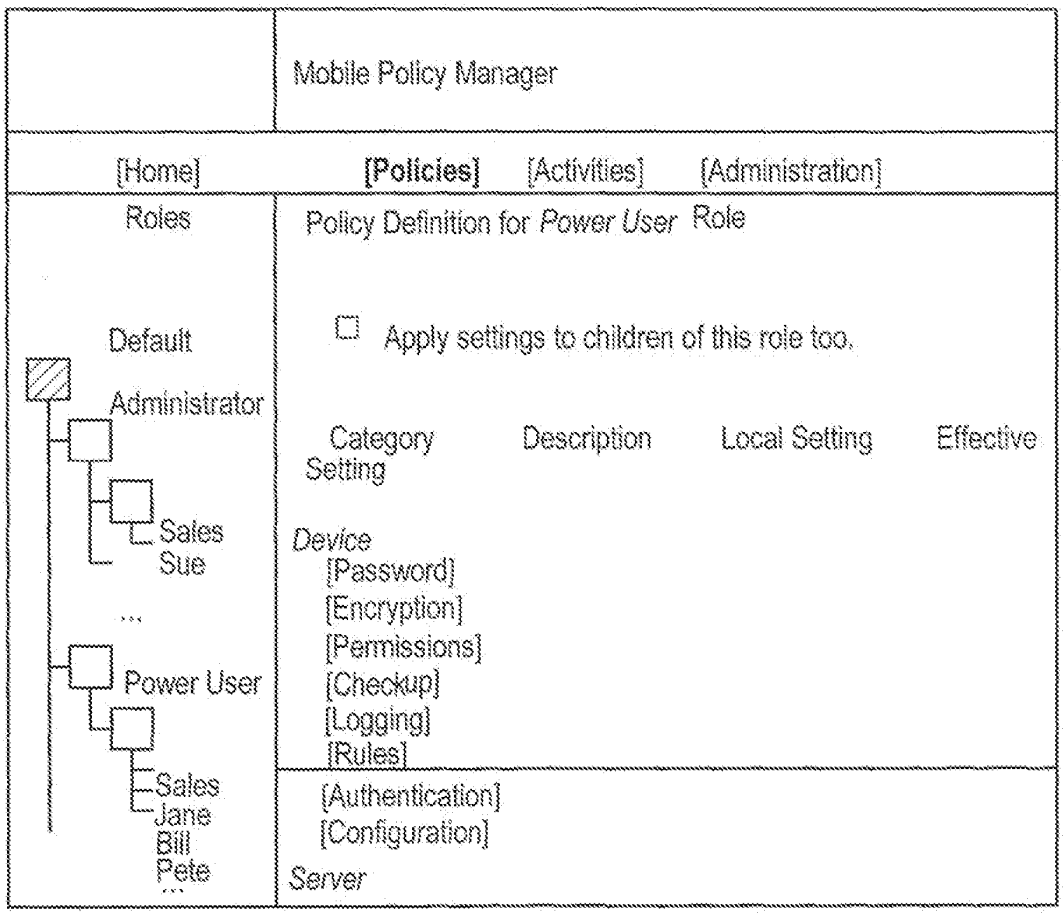

Mobile Policy Manager
[Home]
[Policies]
[Activities]
[Administration]
Roles
Default
Administrator
Sales
Sue
...
Power User
Sales
Jane
Bill
Pete
...
Policy Definition for Power User Role
Apply settings to children of this role too.
Category Setting
Description
Local Setting
Effective
Device
[Password]
[Encryption]
[Permissions]
[Checkup]
[Logging]
[Rules]
[Authentication]
[Configuration]
Server

FIG. 4

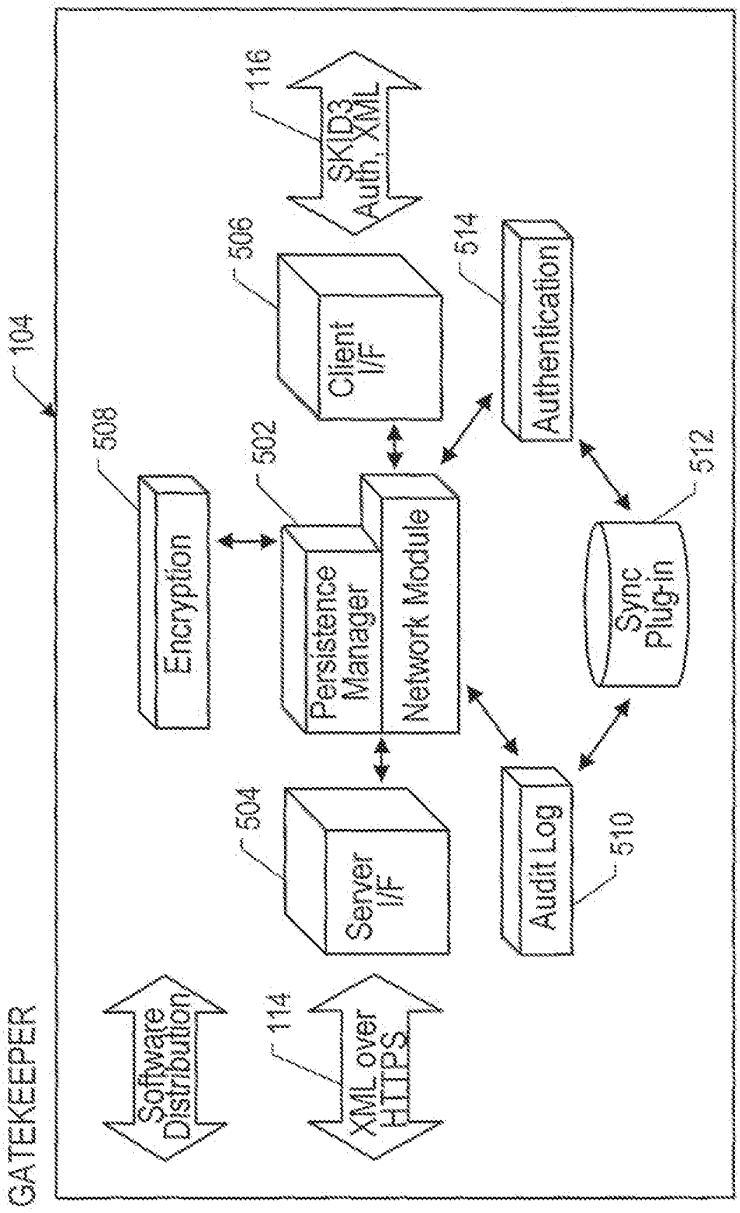

GATEKEEPER
104
Software Distribution
XML over HTTPS
114
Server I/F
504
Persistence Manager
Network Module
502
Encryption
508
Client I/F
506
SKID3 Auth, XML
116
Audit Log
510
Sync Plug-in
512
Authentication
514

FIG. 5

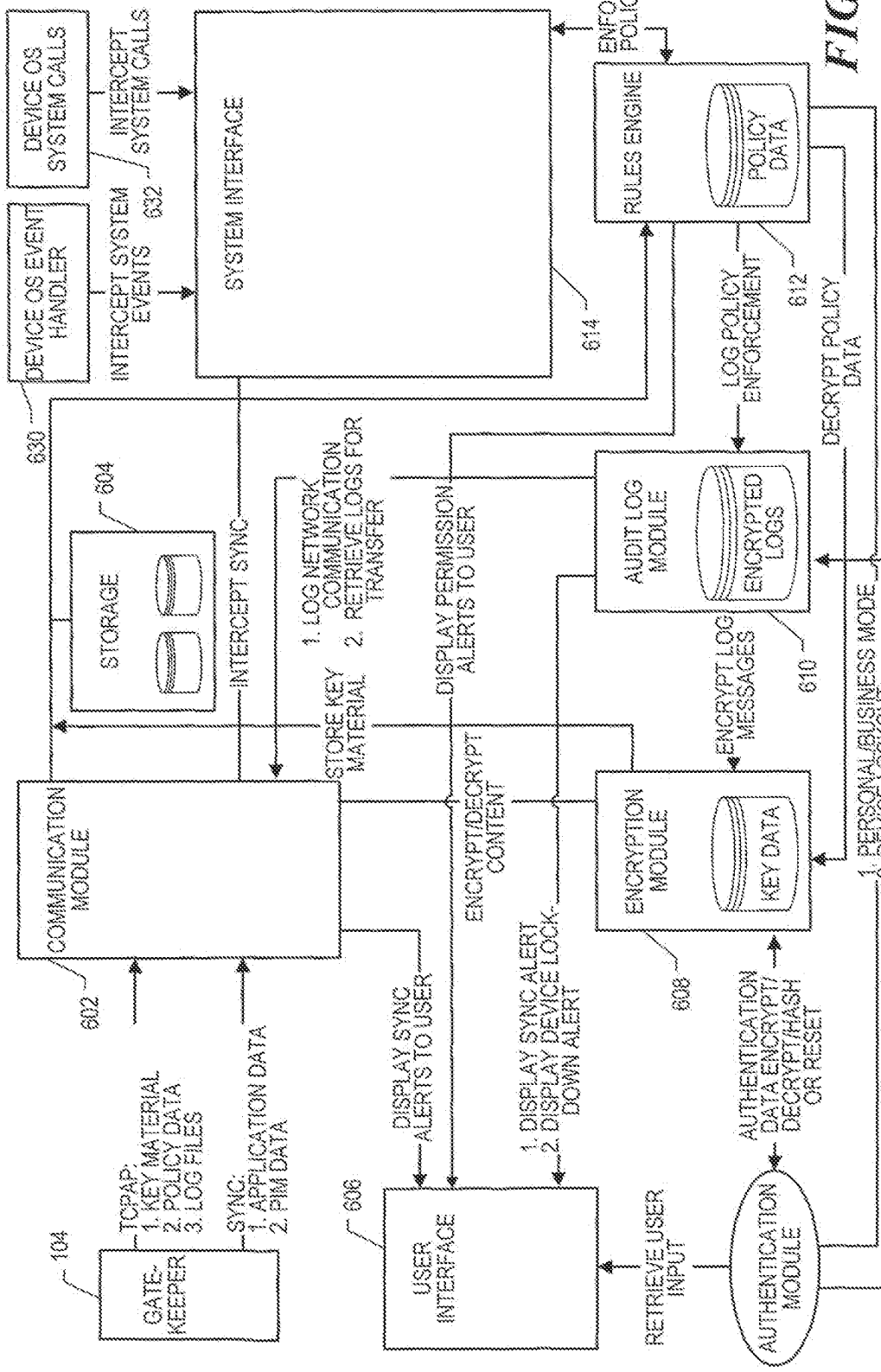

DEVICE OS SYSTEM CALLS
INTERCEPT SYSTEM CALLS
DEVICE OS EVENT HANDLER
INTERCEPT SYSTEM EVENTS
632
SYSTEM INTERFACE
614
ENFORCE POLICIES
RULES ENGINE
POLICY DATA
630
604
STORAGE
INTERCEPT SYNC
1. LOG NETWORK COMMUNICATION 2. RETRIEVE LOGS FOR TRANSFER
STORE KEY MATERIAL
DISPLAY PERMISSION ALERTS TO USER
AUDIT LOG MODULE
ENCRYPTED LOGS
LOG POLICY ENFORCEMENT
612
DECRYPT POLICY DATA
ENCRYPT LOG MESSAGES
610
COMMUNICATION MODULE
602
ENCRYPT/DECRYPT CONTENT
ENCRYPTION MODULE
KEY DATA
608
1. PERSONAL/BUSINESS MODE 2. DEVICE LOCKOUT
TCPAP: 1. KEY MATERIAL 2. POLICY DATA 3. LOG FILES
SYNC: 1. APPLICATION DATA 2. PIM DATA
DISPLAY SYNC ALERTS TO USER
1. DISPLAY SYNC ALERT 2. DISPLAY DEVICE LOCK-DOWN ALERT
AUTHENTICATION DATA ENCRYPT/ DECRYPT/HASH OR RESET
104
GATE-KEEPER
606
USER INTERFACE
RETRIEVE USER INPUT
AUTHENTICATION MODULE
LOG USER AUTHENTICATION

FIG. 6

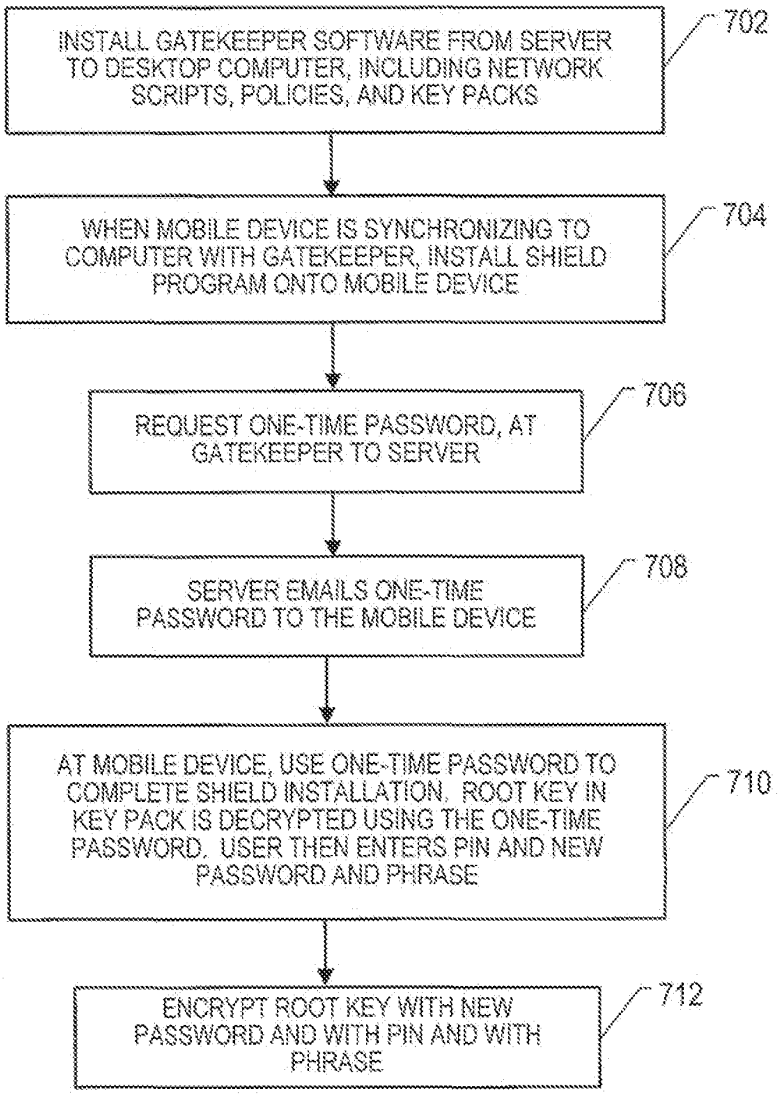

INSTALL GATEKEEPER SOFTWARE FROM SERVER TO DESKTOP COMPUTER, INCLUDING NETWORK SCRIPTS, POLICIES, AND KEY PACKS
702
WHEN MOBILE DEVICE IS SYNCHRONIZING TO COMPUTER WITH GATEKEEPER, INSTALL SHIELD PROGRAM ONTO MOBILE DEVICE
704
REQUEST ONE-TIME PASSWORD, AT GATEKEEPER TO SERVER
706
SERVER EMAILS ONE-TIME PASSWORD TO THE MOBILE DEVICE
708
AT MOBILE DEVICE, USE ONE-TIME PASSWORD TO COMPLETE SHIELD INSTALLATION. ROOT KEY IN KEY PACK IS DECRYPTED USING THE ONE-TIME PASSWORD. USER THEN ENTERS PIN AND NEW PASSWORD AND PHRASE
710
ENCRYPT ROOT KEY WITH NEW PASSWORD AND WITH PIN AND WITH PHRASE
712

FIG. 7

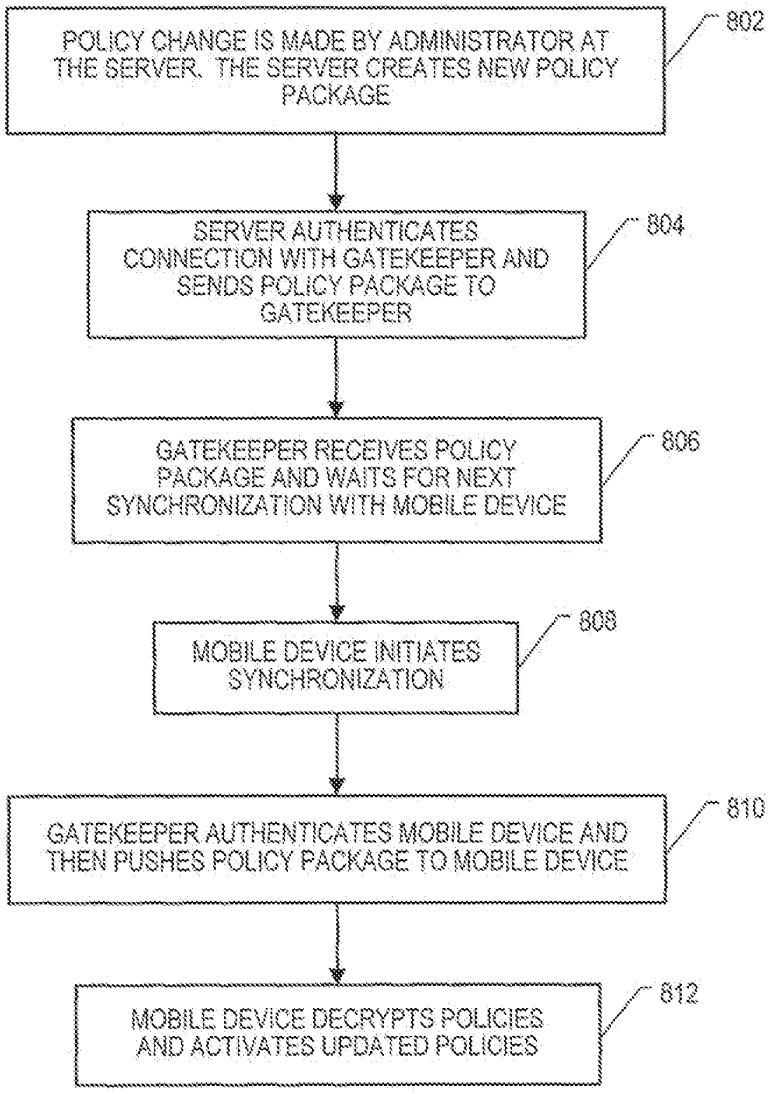

POLICY CHANGE IS MADE BY ADMINISTRATOR AT THE SERVER. THE SERVER CREATES NEW POLICY PACKAGE
802
SERVER AUTHENTICATES CONNECTION WITH GATEKEEPER AND SENDS POLICY PACKAGE TO GATEKEEPER
804
GATEKEEPER RECEIVES POLICY PACKAGE AND WAITS FOR NEXT SYNCHRONIZATION WITH MOBILE DEVICE
806
MOBILE DEVICE INITIATES SYNCHRONIZATION
808
GATEKEEPER AUTHENTICATES MOBILE DEVICE AND THEN PUSHES POLICY PACKAGE TO MOBILE DEVICE
810
MOBILE DEVICE DECRYPTS POLICIES AND ACTIVATES UPDATED POLICIES
812

FIG. 8

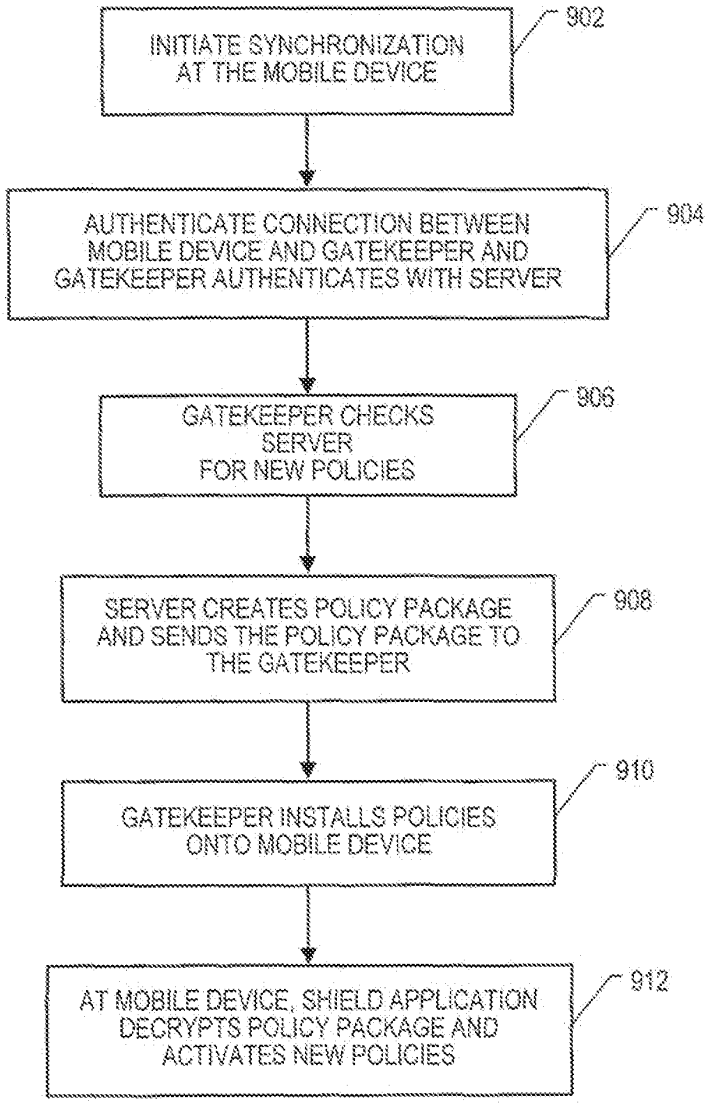

INITIATE SYNCHRONIZATION AT THE MOBILE DEVICE
902
AUTHENTICATE CONNECTION BETWEEN MOBILE DEVICE AND GATEKEEPER AND GATEKEEPER AUTHENTICATES WITH SERVER
904
GATEKEEPER CHECKS SERVER FOR NEW POLICIES
906
SERVER CREATES POLICY PACKAGE AND SENDS THE POLICY PACKAGE TO THE GATEKEEPER
908
GATEKEEPER INSTALLS POLICIES ONTO MOBILE DEVICE
910
AT MOBILE DEVICE, SHIELD APPLICATION DECRYPTS POLICY PACKAGE AND ACTIVATES NEW POLICIES
912

FIG. 9

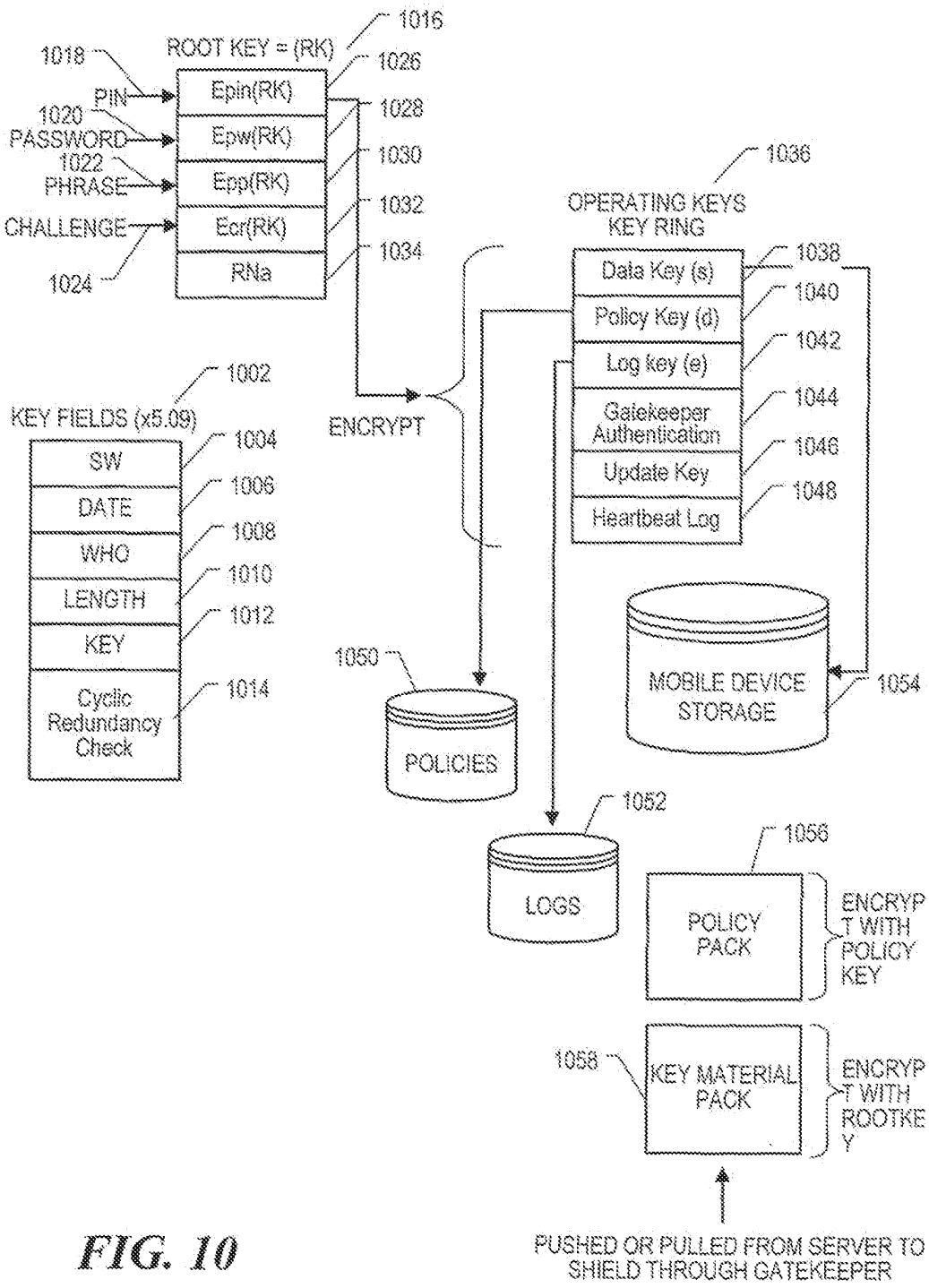

1016
ROOT KEY = (RK)
1018
PIN
1020
PASSWORD
1022
PHRASE
CHALLENGE
1024
Epin(RK)
Epw(RK)
Epp(RK)
Eor(RK)
RNa
1026
1028
1030
1032
1034
1036
OPERATING KEYS
KEY RING
Data Key (s)
Policy Key (d)
Log key (e)
Gatekeeper Authentication
Update Key
Heartbeat Log
1038
1040
1042
1044
1046
1048
1002
KEY FIELDS (x5.09)
SW
DATE
WHO
LENGTH
KEY
Cyclic Redundancy Check
1004
1006
1008
1010
1012
1014
ENCRYPT
1050
POLICIES
MOBILE DEVICE STORAGE
1054
1052
LOGS
1056
POLICY PACK
ENCRYPT WITH POLICY KEY
1058
KEY MATERIAL PACK
ENCRYPT WITH ROOTKEY
PUSHED OR PULLED FROM SERVER TO SHIELD THROUGH GATEKEEPER

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/29347

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00, 9/32
US CL : 713/150, 200-202; 380/255, 270, 277, 278, 279, 281, 283, 284
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. : 713/150, 200-202; 380/255, 270, 277, 278, 279, 281, 283, 284

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,236,852 B1 (VEERASAMY et al) 22 May 2001, see abstract, col. 2, lines 4-36, col. 5, lines 14-40, col. 8, lines 19-55, col. 9, lines 23-46, col. 11, lines 5-11	1,3,5,9-15
X	US 5,850,444 A (RUNE) 15 December 1998, see abstract, col. 3, lines 12-50, col. 4, lines 16-38, col. 5, lines 54-61	2,8
X	US 6,178,506 B1 (QUICK, JR.) 23 January 2001, see col. 2, lines 46-60, col. 4, line 45-col. 5, line 8, col. 6, lines 11-40	4,6

☐ 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
04 December 2003 (04.12.2003)	23 DEC 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Nasser Moazzami Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US03/29347

Continuation of B. FIELDS SEARCHED Item 3:
BRS TEXT SEARCH (files: USPAT, DERWENT, JPO, EPO, IBM TDB, US PGPUB)

search terms: wireless, cell, cellular, policy, root, key, encrypt, encrypting, password, authentic, authenticate, authentication, authenticating, authenticated, authorize, authorizing, authorization, authorized

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
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number
WO 2004/095753 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US2004/010070

(22) International Filing Date: 30 March 2004 (30.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/418,457 17 April 2003 (17.04.2003) US

(71) Applicant (*for all designated States except US*): **MOTOROLA INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **ADWANKAR, Sandeep, M.** [IN/US]; 1224 East Algonquin Road, #SS, Schaumburg, IL 60173 (US). **NARASIMHAN, Nitya** [IN/US]; 1919 Prairie Square, #304, Schaumburg, IL 60173 (US). **VASUDEVAN, Venugopal** [US/US]; 4741 Fairfax Avenue, Palatine, IL 60067 (US).

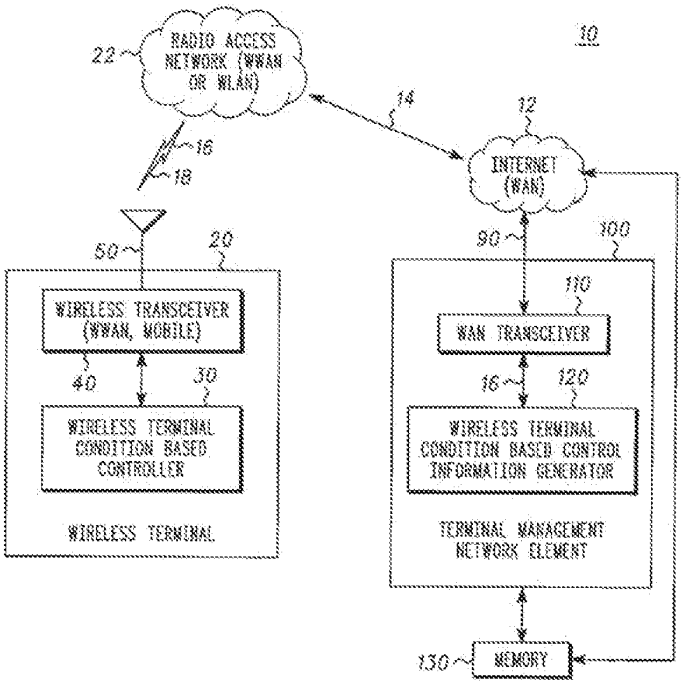
(74) Agents: **WATANABE, Hisashi, David** et al.; 600 North US Highway 45, Libertyville, IL 60048 (US).

(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, 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, 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, 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, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: A METHOD AND APPARATUS FOR MANAGING WIRELESS MOBILE TERMINALS



(57) Abstract: A method and system for managing a terminal management system including a terminal management network element (100) and at least one wireless terminal (20). The terminal management network element (100) includes a wireless terminal condition based control information generator (120) that generates wireless terminal condition based control information (20) represented by extensible markup language code. The wireless terminal condition based control information (20) includes selected action data (46) based on selectable action data (820) associated with a terminal management action to execute on at least one wireless mobile terminal (22), selected condition data (42) based on selectable condition data (840) wherein the selected condition data (42) is associated with the selected action data (46), and selected attribute data (44) based on selectable attribute data wherein the selected attribute data (44) is associated with the selected action data (46). A wireless terminal condition based controller (30) executes the terminal management action if the selected condition (42) data associated with the terminal management action is satisfied.

WO 2004/095753 A2

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.

A METHOD AND APPARATUS FOR MANAGING WIRELESS MOBILE TERMINALS

FIELD OF THE INVENTION

[0001] The invention relates generally to wireless communication systems, wireless terminals, and network elements, and more particularly, to the control and management of wireless terminals, and related methods.

BACKGROUND OF THE INVENTION

[0002] With the growth of wireless terminals, there is a concurrent growth with managing wireless terminal operations. Wireless terminals, such as hand-held wireless devices, including but not limited to a PDAs, cellular phone, a pager, a smart phone, and other suitable devices, are known to employ limited protocols for managing terminal operations. Wireless terminal operations include operations such as diagnostic testing and the reporting of wireless terminal functions, such as, for example, the reporting of the battery level on the wireless terminal to a network element.

[0003] For example, the Synchronization Markup Language (Synch ML) protocol allows a wireless system operator to perform single terminal management actions for immediate execution on a given wireless terminal. However, the Synch ML protocol does not allow for the performance of multiple terminal management actions at any given time, or for the conditional execution of terminal management actions, or for the delayed execution of terminal management actions. For example, the Synch ML protocol does not allow for an operator to schedule execution of wireless terminal management actions at a predetermined time or upon a condition of a terminal or network to suit different conditions relating to different attributes of a mobile terminal or a condition of the network. As a result, the Synch ML protocol does not support scheduling or conditional management control of the wireless terminal.

[0004] As another example of wireless terminal management technology, J2ME is a Java based technology providing limited management of wireless terminal operations for wireless devices and other resource-constrained devices. However, J2ME technology does not support dynamic class loading which prevents Java from being a viable solution for managing wireless mobile terminals.

[0005] Another system proposes a policy-based management network that enforces a management policy through routers in a wired network. However this system permits only "one-time" enforcement of the policy. Further, the policy in the management network addresses only one criterion. As a result, the policy is not dynamically enforceable or adaptable. Additionally, this policy-based management network executes within a router in a wired network and not in a wireless end-user device.

[0006] Other proposed systems, such as the "Simple Network Management Protocol" (SNMP), allow execution of an application based on a time of day. For example, the "cron" command in a Unix system permits the execution of a command at a particular time of day. These systems, however, are typically limited to wired networks and, additionally, require high levels of bandwidth to operate.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention is illustrated by way of example and not limitation in the accompanying figures, in which like reference numerals indicate similar elements, and in which:

FIG. 1 is a block diagram of a terminal management system in accordance with one exemplary embodiment;

FIG. 2 is a block diagram of the terminal management system shown in Fig. 1 according to another exemplary embodiment;

FIG. 3 is a flow chart of a method for managing at least one wireless mobile terminal;

FIG. 4 is a block diagram of the wireless terminal of FIG. 1 shown in more detail;

FIG. 5 is a flow chart for a method of receiving data according to one exemplary embodiment;

FIG. 6 is a flow chart of a wireless terminal processing termination information and attribute data according to one exemplary embodiment;

FIG. 7 is a flow chart of a method of processing a plurality of terminal management actions according to one exemplary embodiment;

FIG. 8 illustrates a user interface for a terminal management network element according to one exemplary embodiment;

FIG. 9 is a flow chart for updating software on a wireless terminal according to one exemplary embodiment; and

FIG. 10 is a flow chart of a method for managing a terminal management network element.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0008] A communication system and method employs wireless terminals, such as wireless mobile terminals, determine that a condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition based control information. The wireless terminal condition based control information includes at least terminal condition information and action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal. The wireless terminal, in response to determining that a condition associated with the terminal management action is satisfied based on the received terminal condition

information, conditionally executes the terminal management action identified by the received action data.

[0009] FIG. 1 illustrates one exemplary embodiment of a communication system 10 that includes, in this example, at least one wireless terminal 20, and a terminal management network element 100. The wireless terminal 20 is coupled to the terminal management network element 100 through a radio access network such as a "wireless wide area network" or "wireless local access network" (WWAN or WLAN) 22, and a wide area network (WAN) 12, such as the internet or other suitable network. Radio access network 22 and WAN 12 are operably coupled through a suitable communication link 14, such as an Ethernet link. Radio access network 22 may be any conventional communication network for transmitting wireless terminal condition-based control information 16, such as a CDMA wireless network, 802.11(b) wireless network, 3G telecommunications system, or any suitable wireless network. Wireless terminal condition based control information 16 includes condition data for conditionally executing terminal management actions.

[00010] The wireless terminal 20 may be a mobile telephone, a personal data assistant ("PDA"), WIFI device, blue tooth compliant device, personal computer, end device, or any other suitable communication device. Wireless mobile transceiver 20 includes wireless terminal condition-based controller 30 suitably coupled to wireless transceiver 40 for communication with radio access network 22. Wireless terminal condition-based controller 30 communicates with radio access network 22 via wireless transceiver 40, antenna 50, and radio communication link 18. Wireless terminal condition-based controller 30 identifies and executes the terminal management action and the condition associated with the terminal management action. The wireless terminal condition-based controller 30 may be one or more suitably programmed

processors, such as a microprocessor, a microcontrolloer, a digital signal processor, and therefore includes associated memory that contains executable instructions that when executed causes the wireless terminal condition-based controller 30 to carry out the operations described herein. In addition, controller as used herein includes discreet logic, state machines or any other suitable combination of hardware, software and firmware.

[00011] Terminal management network element 100 includes wireless terminal condition-based control information generator 120 and WAN tranaceiver 110. WAN transceiver 110 couples wireless terminal condition-based control information generator 120 to wide area network 12 via WAN interface 90. Terminal management network element 100 may be any suitable network element, such as but not limited to a computer, such as a personal computer, server, or plurality of computers or servers.

[00012] FIG. 2 illustrates the communication system 100 as shown in the embodiment of FIG. 1 in more detail. Wireless terminal 20 receives wireless terminal condition-based control information 16 that includes at least terminal condition information 26 and action data 46 associated with a terminal management action. Terminal condition information 26 includes condition data 42 and attribute data 44. Wireless terminal condition-based controller 30 is coupled to input/output "I/O" interface 32 and memory 34. Input/output interface 32 is coupled to exemplary wireless terminal interface battery 36, exemplary action data for terminal management action 28, and an other 38 wireless terminal attribute interface data.

[00013] FIG. 3 illustrates one example of a method 300 for managing the operation of wireless terminal 20 in FIG. 1. At block 310, the wireless terminal 22 determining that a condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition-based control

information 24 that includes at least terminal condition information 26 and action data 46, wherein the action data 46 identifies at least one terminal management action. The terminal management action performs terminal management operations on the wireless terminal 22, such as asset management, configuration management, fault management, and performance management. As shown in block 320, the wireless terminal conditionally executes, the terminal management action identified by the received action data 46. The condition associated with the terminal management action may be an attribute and a condition associated with the wireless mobile terminal, such as a 25% battery level or an 847 area code.

[00014] Referring to memory 130 as shown in FIG. 2, instructions executable by a processor may be stored in memory 130 in order to cause the processor to perform the method 200 described in FIG. 3. These instructions executable by a processor include receiving the extensible markup language code that includes at least wireless terminal condition-based control information. As previously stated, the wireless terminal condition-based control information includes at least terminal condition information and action data where the action data identifies at least one terminal management action associated with the wireless mobile terminal. The instructions executable by the processor may conditionally execute the terminal management action identified by the action data in response to determining that a condition associated with the terminal management action is satisfied, based on the terminal condition information.

[00015] FIG. 4 illustrates the wireless terminal condition-based terminal controller 30, including a synch engine 410, and including a command parser 400, coupled to a policy engine 420, and GUI 416. Command parser 400 is coupled to the wireless transceiver 40 to receive the wireless terminal condition-based control information 16. Command parser 400 parses the terminal condition information 16, and action data 46 associated with the wireless terminal

action and identifies attribute data 44 associated with the action data 46 and condition data 42. In one embodiment, the condition data 42 includes a condition associated with an attribute such as less than, greater than, and equal to. The attribute field may be a threshold level for performing a comparison.

[00016] Command parser 400 is coupled to GUI 416 (Graphical User Interface) via sync engine adapter 412 to send and receive information to a user. Information sent to the user may include, for example, queries, prompts and messages sent to the user via a display on the GUI 416 of wireless terminal 22. The GUI 416 may also provide information to the wireless terminal 20 via the sync engine adapter 412 by providing information input by the user, such as a message, and data input via a keyboard on the wireless terminal 22.

[00017] As shown in FIG. 4, wireless terminal condition-based controller 30 includes a policy reader 430 coupled to the command parser 400 to read the action data 46, attribute data 44 and condition data 42 associated with the terminal management action 410. An attribute monitor 440 is coupled to the policy reader 430 to receive attribute data 44. Attribute monitor 440 is also coupled to input/output interface 32 to monitor current terminal attribute values 460 in response to the attribute monitor 440 receiving attribute data 44. Task manager 450 is coupled to the policy reader 430 and to the attribute monitor 440 to compare the current terminal attribute values 44 from the attribute monitor 440 with the received condition data 42 from the policy reader 430 to determine if the condition data 42 is satisfied. In order to perform this comparison, the attribute monitor 440 may receive current terminal attribute values 460 through: a polling event, an interrupt event, a predetermined time of day trigger event, or a predetermined period of elapsed time trigger event. For example, wireless terminal condition-based controller 30 may include one or more processors to, for example, poll the input/output interface 32 in order to

obtain the received current terminal attribute values 460. Alternatively, an interrupt event may be used to obtain current terminal attribute values 460 from input/output interface 32.

[00018] In one embodiment, the task manager 450 schedules a current terminal management action to execute, according to whether a previous terminal management action is completed. For example, the terminal management action may be a timed terminal management type of action wherein execution of the terminal management action is scheduled for a particular time of day. Alternatively, the current terminal management action schedule may be a periodic type of task. According to one exemplary embodiment, a current terminal management action is started only after a previous terminal management action is completed similar to a cron function on a UNIX operating system.

[00019] FIG. 5 is a block diagram for receiving a payload at block 510 with wireless terminal condition-based control information 16 represented by extensible markup language code for a terminal management action. Command parser 400 reads wireless terminal condition-based control information 24 from a payload at block 520, for identifying the terminal condition information 26 and action data 46 associated with the terminal management action. In this embodiment, the parser 400 of wireless terminal condition-based controller 30 reads attribute data 44 associated with the action data 46 from the terminal condition information 26, as shown in block 530. Additionally, at block 540, parser 400 reads condition data 42, associated with the attribute data 44.

[00020] In one embodiment, a terminal management action may be a battery-level guard operation that specifies a command for fetching an attribute such as the battery level from the wireless terminal 22. For example, the battery-level guard command may prevent execution of the terminal management action specified by the action data if the battery level on the terminal is

below 25%. In this embodiment, the attribute of the terminal management action is the battery level, the condition is greater than 25%, and the action data represents a terminal management action for fetching a current terminal attribute value for the battery level.

[00021] Examples of the terminal condition information associated with the terminal management action include a wireless terminal state (i.e., battery level as previously described) or a network state. For example, a network operator may want to run an automated test where all phones in the 847 area code receive a terminal management action, such as a test of wireless terminal functions. The operator may further want to execute the test on the first 100 mobiles to respond during off-peak hours so as not to drain terminals that are running low on batteries. Therefore, the network state may be the number of cell phones in the 847 area code running the requested terminal management action. The attribute therefore may be the test represented by the terminal management action. Other examples of terminal condition information include a duration since the last terminal management action occurred, a number of action repetitions, a completion of a terminal management action, a software upgrade, a time of day, a terminal management action schedule, a wireless application protocol (WAP) configuration, a user setting, a signal level, a battery level, and terminal location coordinates.

[00022] The wireless terminal condition-based control information 16, as shown in FIGs. 1 and 2, may be transmitted using extensible markup language code. In one embodiment, for example, the extensible markup language code may be based on the Sync ML communications protocol described at www.syncml.org. However, any extensible markup language code may be used such as SMG, HTTP and XML.

[00023] Further, the extensible markup language code may include an assert command, a schedule command, and a perform command. The assert command may associate the terminal

condition information 16 (condition data 42, and attribute data 44) with the received action data 46, and may also associate the terminal condition information 26 with exception action data if the condition data is not satisfied. For example, the assert command may cause the terminal management action to execute in the event the condition data is not satisfied. In another example of the assert command, the terminal management action may be a diagnostic test such as a test to determine if the browser is functioning properly. If the test results indicate that the browser is not functioning, then the browser may be automatically configured by, for example, configuring the WAP settings on the browser.

[00024] The schedule command may associate the terminal condition information with data such as a time of day, a time interval between successive executions of the terminal management action, a number of repetitions to execute the terminal management action, a repetition rate for executing the terminal management action, and a first run of a scheduled execution of a terminal management action. In one example, a terminal management action may be postponed for execution at a particular time. In another example, scheduling may take the form of monitoring, measuring and reporting an elapsed period of time to perform a terminal management action, such as downloading a web page. The wireless terminal may measure the amount of time a web page takes to download over a period of time and for a number of occurrences and report these measurements to the operator for statistical analysis.

[00025] The perform command associates an attribute value such as a network attribute value, or a locally obtained attribute value associated with the wireless mobile terminal, and action data. For example, the perform command performs a non-local service action, such as a "get" terminal attribute value. Accordingly, an operator may use this command to measure service performance on a wireless mobile terminal.

[00026] FIG. 6 is a block diagram for one embodiment of a method 600 to manage at least one wireless mobile terminal. The wireless terminal 20 receives attribute data 44 (i.e., via the command parser 400) associated with the action data at block 610. Condition data 42 associated with the attribute data 44 is received at block 620. The attribute monitor 440 receives locally obtained current terminal attribute values 460 (i.e., via the input/output interface 32) at block 630. As previously stated, the task manager 450 compares the locally obtained current terminal attribute values 460 with the received condition data 42 to determine if the condition data 42 is met at block 640. Optionally, for example, task manager 450 schedules a current terminal management action to conditionally execute, according to whether a previous terminal management action is completed. In this embodiment, the task manager 450 conditionally executes the current terminal management action if the condition data associated with the terminal management action is met. In one exemplary embodiment, the condition data 42 requires that a previous terminal management action is executed at step 670 before the current terminal management action is executed. Since in this embodiment a current terminal management action may be scheduled to perform at a time in the future, the condition of the current terminal attribute values 460 may change by the time the current terminal management action is executed. Accordingly, the current terminal attribute values 460 may be updated at step 660 in order to determine if the condition data is still satisfied at that time.

[00027] FIG. 7 is a block diagram of a method for managing multiple terminal management actions on a wireless terminal 22. The parser 400 at block 710 receives terminal condition information and action data associated with multiple corresponding terminal management actions. Accordingly, each of the multiple action data 46 identifies a corresponding terminal management action. As shown in block 720, the multiple terminal condition

information includes multiple attribute data 44 associated with corresponding action data 46. The terminal condition information includes condition data 42 associated with corresponding attribute data 44.

[00028] Attribute monitor 440 receives current terminal attribute values 460 at block 740 in response to the attribute monitor 440 receiving the multiple attributes for each corresponding terminal management action. At block 750, in one embodiment, the task manager 450 schedules each terminal management action for execution in accordance with the condition data 42. At step 760, task manager 450 compares each current terminal attribute value with the corresponding received-condition data 42 to determine if the condition data 42 is met. If the terminal management action is executed at a later time, then the current terminal attribute values 460 may be updated, if necessary at block 760, to determine whether the current terminal attribute value 460 reflects the state of the attribute. The task manager 450 at block 770 conditionally executes each of the multiple terminal management actions if the condition data 42 associated with the corresponding terminal management action is satisfied. In one embodiment, the condition data 42 requires that a previous terminal management action is executed.

[00029] FIG. 8 illustrates a selectable terminal management action window 800 for the terminal management network element 100, as shown in FIG. 1. As previously stated, the wireless terminal condition-based control information generator 120 generates extensible markup language code that includes wireless terminal condition-based control information 16. This may be generated by an operator through the selectable terminal management action window 800, as shown in FIG. 8. For example, a user may select a type of terminal management action from options displayed on a window menu, as shown in FIG. 8, to perform terminal management operations within the terminal management categories such as (i) performance management,

(ii) asset management, (iii) configuration management, and (iv) fault management. Accordingly, an operator may select one of these terminal management actions from the selectable terminal management action window. As a result, the wireless terminal condition-based control information generator 120 generates selected action data 820 based on the selectable action data associated with a terminal management action for at least one wireless mobile terminal.

[00030] Once a selection is made from the selectable terminal management action window 810, in one embodiment, a selectable condition pull-down window may then be presented to the user for selection of the desired condition associated with the selected action. The wireless terminal condition-based control information generator 120 then generates selected condition data based on the selectable condition data where the selected condition data is associated with the selectable action data. Similarly, a user may select an attribute associated with the desired action through a selectable device attribute pull-down menu window 850. Accordingly, the wireless terminal condition-based control information generator 120 produces selected attribute data based on the selectable attribute data wherein the selected attribute data is associated with the selectable action data. Once the selected action data, selected condition data, and the selected attribute data are identified through, for example, an operator making appropriate selections through the user interface, as shown in FIG. 8, then the wireless terminal condition-based control information generator 120 may generate the extensible markup language code for identifying the wireless terminal base control information.

[00031] In another embodiment, the wireless terminal condition-based control information generator 120 generates multiple terminal management actions defined by corresponding action data. As previously discussed with respect to the execution of multiple terminal management actions in a wireless terminal 22, the execution of a first terminal management action may be

conditioned on the execution of a second terminal management action. In another embodiment, as previously discussed with regards to running tests on wireless terminal devices within the 847 area code, the operator may desire to stop execution of the test when, for example, the first 100 mobile terminals have responded with test results to the terminal management network element 100. In this example, the terminal management network element 100 may transmit a network attribute value to the wireless terminal 22 in order to allow the task manager in each respective wireless terminal 22 to compare the network attribute value with the selected condition data to determine if the selected condition is met. For example, the network attribute value may be a current number of responses under 100, such as 82. The task manager will then compare the network attribute value 82 with the condition data 100 in order to determine if the first 100 wireless mobile telephone devices have completed the test in this example. Since in this example the network attribute value 82 is less than the condition data 100, the condition data is not satisfied, and the terminal management action continues execution.

[00032] In another embodiment, as shown in FIG. 9, during session setup as shown in block 910, the wireless terminal determines if multiple terminal management actions are in operation. At block 920, the wireless terminal determines if a terminal management action is currently pending. If the wireless terminal has a pending terminal management action, then the terminal management network element 100 sends the wireless terminal condition-based control information to the wireless terminal at block 930. If there is no pending task at block 940, then the wireless terminal condition-based control information is not sent to the wireless mobile terminal. In this way, the terminal management network element 100 can determine if the wireless terminal condition-based control information is required to be sent to the wireless mobile terminal.

[00033] FIG. 10 illustrates a method 1000 for managing at least one wireless terminal on a terminal management network element. At block 1010 the terminal management network element 100 presents selectable action data associated with a terminal management action for selection by a user, such as through the selectable terminal management action window 810 of FIG. 8. The wireless terminal condition-based control information generator 120 presents selectable condition data associated with a terminal management action at block 1020 where the selected condition data is associated with the selected action data. At block 1030, the terminal management network element 100 presents selectable attribute data associated with the selectable action data where the selected attribute data is associated with the selected action data. The selected condition data, selected action data, and selected device attribute data is received by the wireless terminal condition-based control information generator 120 at block 1040.

[00034] Optionally, if the operator desires that the terminal management actions are executed according to a schedule, the operator selects the condition data to reflect the desired schedule at step 1050. The wireless terminal condition-based control information generator 120 generates the wireless terminal condition-based control information according to the selected action data, the selected condition data, and the selected attribute data, wherein the wireless terminal condition-based control information is represented by extensible markup language code for at least one wireless terminal at block 1060. According to one embodiment, the wireless terminal for the extensible markup language code for at least one wireless mobile terminal, including the wireless terminal condition-based control information, may be stored into a storage medium such as a CD rom, magnetic tape, any optical type of storage medium at step 1070.

[00035] Although, for purposes of illustration, the wireless terminal condition-based control information was described with reference to the Sync ML protocol, any appropriate

communication protocol or extension of protocol, such as J2ME or SNMP may be used. In addition, terminal management operation of a wireless terminal may be performed in any other way, so that terminal management actions may be associated with conditions such as condition data. Other advantages will be recognized by those with ordinary skill in the art.

[00036] In one embodiment, the system and method described may be incorporated as an extension of the existing SyncML terminal management protocol in a non-invasive manner. For example, the extension information, such as the condition data, attribute data, and action data (i.e. wireless terminal based condition based control information) may be incorporated into the existing SyncML payload. These extensions to the existing SyncML payload are completely transparent to existing SyncML systems. As a result, systems capable of receiving the extension information will extract and interpret the extension information, while older systems will merely discard the extension information without error. Additionally, the extension to the existing SyncML protocol is extensible, and can therefore be easily customized or enhanced to address new requirements and criteria.

[00037] The system and method allows an operator to control the management functions of wireless mobile terminals individually on a per-terminal basis rather than by enforcing a management function on all terminals. Additionally, since the responsibility for terminal management execution and for the execution of multitasking multiple terminal management actions occurs within the wireless terminal 20 rather than in the terminal management network element 100, execution of a terminal management action is more likely to execute successfully. Since execution of the terminal management action on the terminal management network element 100 may be interrupted or aborted if the radio access network 22 becomes unavailable, processing of the terminal management actions by the wireless terminal 20 would be

independent of the radio access network 22. As a result, reliability is improved because the wireless terminal executes the terminal management actions independently from the terminal management network element 100, even if access to the radio access network 16 is unavailable (i.e. in an area without signal).

[00038] Another advantage includes the ability of the wireless terminal 22 to be self-adaptive to reflect changes on the specific terminal. Other advantages include a reduction in bandwidth for performing terminal management actions on the wireless terminal 20 rather than on the terminal management network element 100. As a result, high data rate communication over the radio access network 22 for performing the terminal management operation is not required, and therefore, a reduction in communication bandwidth is realized. Consequently, the cost and effort associated with wireless terminal management is reduced.

[00039] It should be understood that the implementation of other variations and modifications of this invention and its various aspects will be apparent to those of ordinary skill in the art, and that the invention is not limited by specific embodiments described. It is therefore contemplated to cover by the present invention, any and all modifications, variations, or equivalents that fall within the spirit and scope of the basic underlying principles disclosed and claimed herein.

WE CLAIM:

1. A method in a wireless terminal comprising:

determining that a condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition based control information that includes at least terminal condition information and action data wherein the action data identifies the at least one terminal management action associated with the wireless terminal; and

executing conditionally, by the wireless terminal, the terminal management action identified by the received action data.

2. The method of claim 1 wherein determining that the condition associated with at least one terminal management action is satisfied based on extensible markup language code that includes at least wireless terminal condition based control information includes: attribute data associated with the action data; and condition data associated with the attribute data.

3. The method of claim 2 comprising:

obtaining current terminal attribute values in response to the received attribute data at the wireless terminal; and

comparing the obtained current terminal attribute values to the condition data to determine if the condition data is met.

4. The method of claim 2 comprising:

scheduling a current terminal management action to conditionally execute according to whether a previous terminal management action is completed; and

conditionally executing the current terminal management action if the condition data associated with the current terminal management action is met wherein the condition data requires that the previous terminal management action is executed.

5. The method of claim 1 comprising:

obtaining wirelessly received wireless terminal based control information including a plurality of action data corresponding to a plurality of terminal management actions, a plurality of corresponding attribute data associated with the corresponding plurality of action data, a plurality of corresponding condition data associated with the corresponding plurality of attribute data, and

obtaining a plurality of current terminal attribute values in response to obtaining the plurality of corresponding attribute data associated with the corresponding plurality of action data;

comparing the plurality of current terminal attribute values to the corresponding condition data to determine if the condition data is met; and

conditionally executing the plurality of terminal management actions if the condition data associated with the corresponding terminal management action is satisfied wherein the condition data requires that a previous terminal management action is executed.

6. The method of claim 1 wherein, the terminal condition information associated with the terminal management action includes data representing at least one of: a wireless terminal state, a network state, a duration since a last terminal management action occurred, a number of action repetitions, a completion of a terminal management action, a software upgrade, a time of day, a terminal management action schedule, a wireless application protocol (WAP) configuration, a user setting, a signal level, a battery level, and terminal location coordinates.

7. The method of claim 1 where the wireless terminal condition based control information includes at least one of an, assert command, schedule command, and perform command, wherein:

the assert command associates the terminal condition information with the received action data and with exception action data if the condition data is not satisfied,

the schedule command associates the terminal condition information with data including at least one of a time of day, a time interval between successive executions of the terminal management action, number of repetitions to execute the terminal management action, repetition rate of executing the terminal management action, monitoring, measuring and reporting an elapsed period of time to perform a terminal management action, and a first run of a scheduled execution of a terminal management action, and

the perform command associates action data with an attribute value including at least one of a network attribute value, and a wireless mobile terminal attribute value.

8. A wireless terminal comprising:

a wireless transceiver that receives extensible markup language code that includes at least wireless terminal condition based control information that includes at least terminal condition information and action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal; and

a wireless terminal condition based controller, coupled to the wireless transceiver,

the wireless terminal condition based controller for:

determining whether a condition associated with the terminal management action is satisfied, based on the terminal condition information, and

executing, the terminal management action identified by the action data if the condition associated with the terminal management action is satisfied.

9. The wireless terminal condition based controller of claim 8 comprising:

a command parser coupled to the wireless transceiver to parse the wireless terminal condition based control information to identify the terminal condition information and the action data associated with the terminal management action.

10. The wireless terminal of claim 9 wherein the wireless terminal condition based controller comprises:

a policy reader coupled to the command parser to read the action data, attribute data, and condition data associated with the terminal management action;

an attribute monitor coupled to the policy reader to receive attribute data from the policy reader and to obtain current terminal attribute values in response to the received attribute data; and

a task manager coupled to the policy reader and to the attribute monitor to compare the current terminal attribute values from the attribute monitor, with the received condition data to determine if the condition data is satisfied.

11. The wireless terminal of claim 10 wherein the task manager:

schedules a current terminal management action to execute according to whether a previous terminal management action is completed; and

conditionally executes the current terminal management action in accordance with the condition data associated with the current terminal management action, wherein the condition data requires that a previous terminal management action is executed.

12. The wireless terminal of claim 8 wherein the wireless terminal condition based controller comprises:

a processing device;

memory containing executable instructions that causes the processing devices to:

identify the at least wireless terminal condition based control information that includes the at least terminal condition information and the

action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal; and

in response to determining that the condition associated with the terminal management action is satisfied based on the terminal condition information, conditionally execute, the terminal management action identified by the action data.

13. The wireless terminal of claim 8 wherein the terminal condition information associated with the terminal management action is determined at an event selected from the group consisting of a polling event, an interrupt event, a predetermined time of day, and a predetermined period of elapsed time.

14. The wireless terminal of claim 8 where the extensible markup language code includes at least one of an assert command, a schedule command, and a perform command, wherein:

the assert command associates the terminal condition information with the received action data and associates the terminal condition information with exception action data if the condition data is not satisfied,

the schedule command associates the terminal condition information with data including at least one of a time of day, time interval between successive executions of the terminal management action, number of repetitions to execute the terminal management action, repetition rate of executing the terminal management action, monitoring, measuring and reporting an elapsed period of time to execute the terminal

management action, and a first run of a scheduled execution of a terminal management action, and

the perform command associates the action data with an attribute value including at least one of a network attribute value and an attribute value associated with the wireless mobile terminal.

15. The wireless terminal of claim 8 wherein the wireless terminal based control information identifies a plurality of terminal management actions, wherein the wireless terminal executes the plurality of terminal management actions in accordance with the corresponding terminal condition information wherein the terminal condition information requires that a previous terminal management action is executed.

16. A storage medium having stored therein instructions executable by a processor that causes the processor to:

receive, extensible markup language code that includes at least wireless terminal condition based control information that includes at least terminal condition information and action data wherein the action data identifies at least one terminal management action associated with the wireless mobile terminal; and

in response to determining that a condition associated with the terminal management action is satisfied based on the terminal condition information, conditionally execute, by the processor, the terminal management action identified by the action data.

17. A wireless terminal comprising:

a wireless transceiver that receives extensible mark-up language code that includes a payload, including at least wireless terminal condition based control information; and

a wireless terminal condition based controller comprising:

a command parser coupled to the wireless transceiver that parses the wireless terminal condition based control information wherein the terminal condition information comprises:

action data associated with at least one terminal management action;

attribute data associated with the action data; and

condition data associated with the attribute data,

a policy reader coupled to the command parser operative to read the action data, attribute data and condition data associated with the least one terminal management action;

an attribute monitor coupled to the policy reader to receive the attribute data from the policy reader and to locally obtain current terminal attribute values in response to the received attribute data; and

a task manager coupled to the policy reader to compare the current terminal attribute values to the received condition data to:

determine if the condition data is met, and

conditionally execute the terminal management action identified by the action data.

18. A terminal management network element comprising:

a wireless terminal condition based control information generator that generates extensible markup language code that includes wireless terminal condition based control information that includes:

selected action data based on selectable action data associated with a terminal management action for at least one wireless mobile terminal;

selected condition data based on selectable condition data wherein the selected condition data is associated with the selectable action data; and

selected attribute data based on selectable attribute data wherein the selected attribute data is associated with the selectable action data,

wherein the wireless terminal condition based control information is generated according to the selected action data, the selected condition data and the selected attribute data; and

a transceiver coupled to the wireless terminal control based control information generator to transmit the wireless terminal control based information.

19. The terminal management network element of claim 18 wherein the wireless terminal condition based control information generator generates a plurality of terminal management actions defined by a plurality of action data, and

wherein the terminal management network element defines condition data associated with a first terminal management action to conditionally execute according to whether a second terminal management action completes execution.

20. The terminal management network element of claim 18 wherein the wireless management terminal network element generator:

generates wireless terminal condition based control information to conditionally execute a plurality of terminal management actions each associated with corresponding selected condition data on a plurality of wireless mobile terminals, and

sends network attribute values to the plurality of wireless mobile terminals to compare the network attribute values with the selected condition data to determine if the selected condition data is met.

21. A method for managing a terminal management network element comprising:

presenting selectable action data associated with a terminal management action;

receiving selected action data in response to presenting the selectable action data;

presenting selectable condition data associated with the selectable action data wherein the selected condition data is associated with the selected action data;

receiving selected condition data in response to presenting the selectable condition data;

presenting selectable attribute data associated with the selectable action data wherein the selected attribute data is associated with the selected action data;

receiving selected attribute data in response to presenting the selectable attribute data, and

generating wireless terminal condition based control information according to the selected action data, the selected condition data, and the selected attribute data wherein the wireless terminal condition based control information is represented by extensible markup language code for at least one wireless mobile terminal.

22. The method of claim 21 wherein the selected action data identifies a plurality of terminal management actions, the method comprising;

associating selected condition data with a first terminal management action to conditionally execute the first terminal management actions on a single wireless terminal according to whether a second terminal management action is completed; and

generating the plurality of current terminal management actions associated with the selected condition data.

23. The method of claim 21 comprising;

generating wireless terminal condition based control information for a plurality of wireless mobile terminals; and

sending network attribute values to the plurality of wireless mobile terminals to allow comparing the network attribute values with the selected condition data by each of the plurality of wireless mobile terminals to determine if the selected condition data is met.

24. A terminal management system comprising:

a terminal management network element comprising:

a wireless terminal condition based control information generator that generates wireless terminal condition based control information comprising:

selected action data based on selectable action data associated with a terminal management action to execute on at least one wireless mobile terminal;

selected condition data based on selectable condition data wherein the selected condition data is associated with the selected action data;

selected attribute data based on selectable attribute data wherein the selected attribute data is associated with the selected action data,

wherein the wireless terminal condition based control information is generated according to the selected action data, the selected condition data and the selected attribute data, wherein the wireless terminal condition based control information is represented by extensible markup language code;

at least one wireless terminal comprising:

a wireless transceiver that receives the at least wireless terminal condition based control information, the selected attribute data, the selected condition data, the selected action data and the terminal management action associated with the wireless mobile terminal; and

a wireless terminal condition based controller, operatively coupled to the wireless transceiver, and operative to

determine that the selected condition data associated with the terminal management action is satisfied, and

conditionally execute the terminal management action identified by the selected action data if the selected condition data associated with the terminal management action is satisfied.

25. The terminal management system of claim 24 wherein the wireless terminal condition based control information generator generates a plurality of terminal management actions defined by the selected action data and the associated selected condition data, and defines the selected condition data associated with each terminal management action to conditionally execute in accordance with the selected condition data associated with each respective terminal management action.

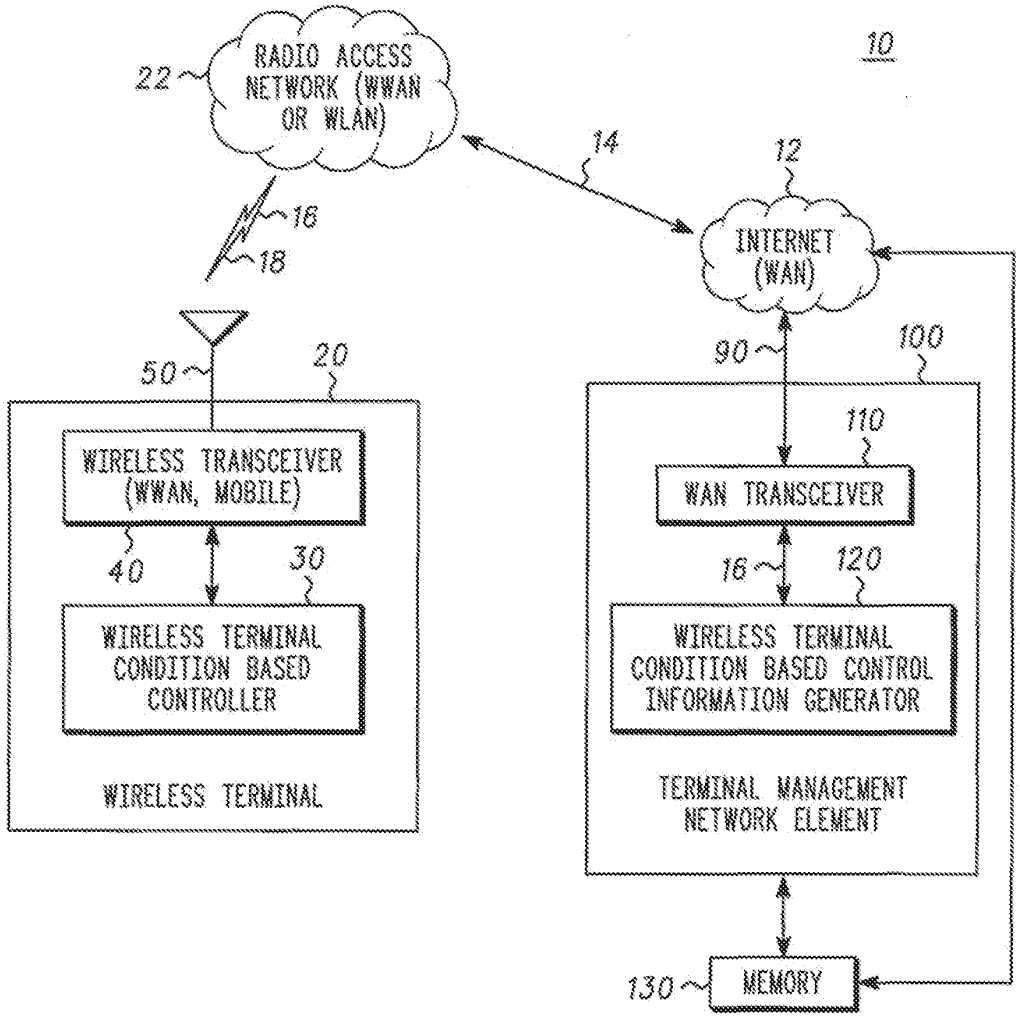

RADIO ACCESS NETWORK (WWAN OR WLAN)
22
10
14
12
16
18
INTERNET (WAN)
50
20
90
100
110
WIRELESS TRANSCEIVER (WWAN, MOBILE)
WAN TRANSCEIVER
40
30
16
120
WIRELESS TERMINAL CONDITION BASED CONTROLLER
WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION GENERATOR
WIRELESS TERMINAL
TERMINAL MANAGEMENT NETWORK ELEMENT
130
MEMORY

FIG. 1

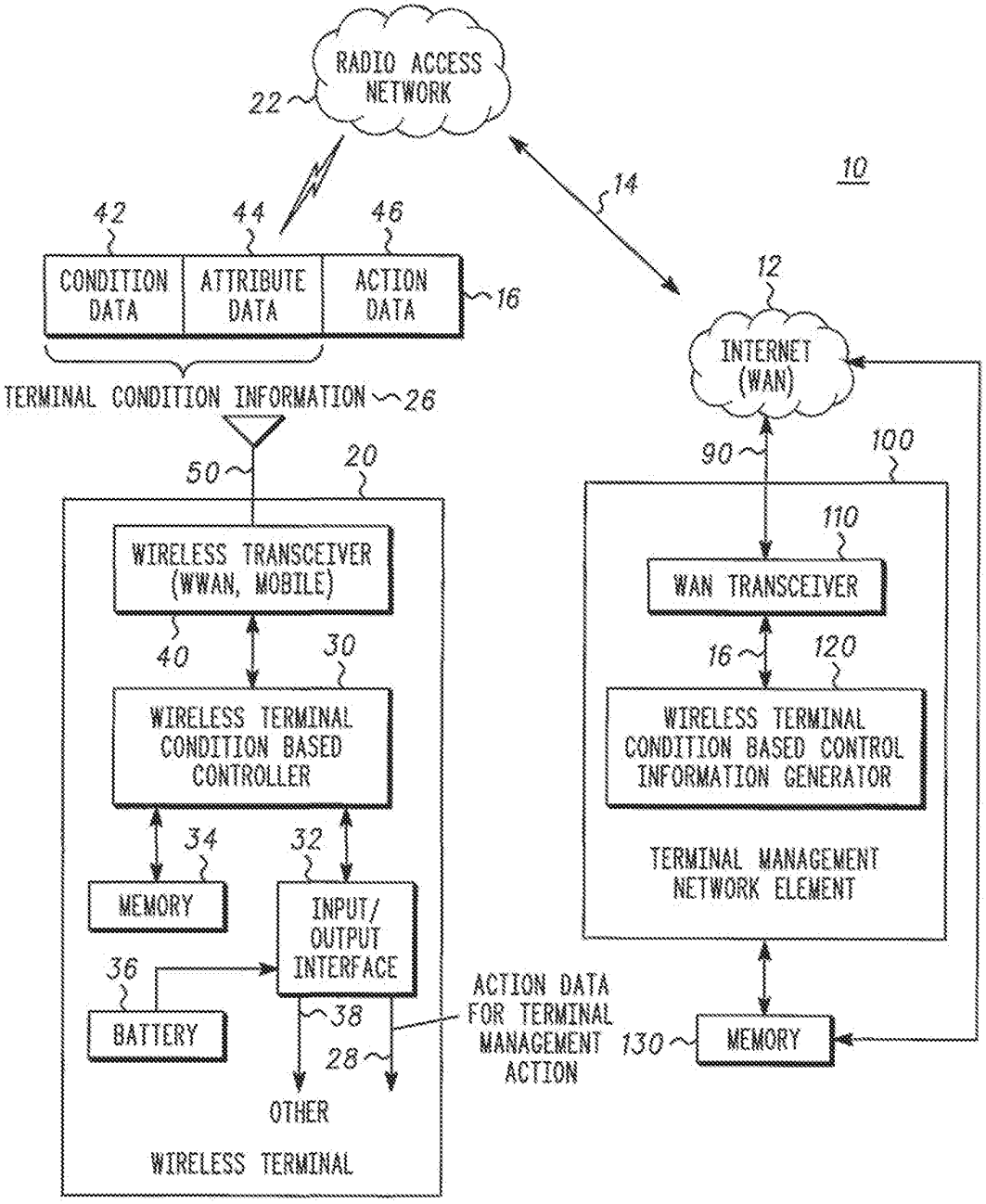

RADIO ACCESS NETWORK
22
14
10
42
44
46
CONDITION DATA
ATTRIBUTE DATA
ACTION DATA
16
12
INTERNET (WAN)
TERMINAL CONDITION INFORMATION
26
50
20
90
100
WIRELESS TRANSCEIVER (WWAN, MOBILE)
110
WAN TRANSCEIVER
40
30
16
120
WIRELESS TERMINAL CONDITION BASED CONTROLLER
WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION GENERATOR
34
32
TERMINAL MANAGEMENT NETWORK ELEMENT
MEMORY
INPUT/ OUTPUT INTERFACE
36
ACTION DATA FOR TERMINAL MANAGEMENT ACTION
38
BATTERY
28
130
MEMORY
OTHER
WIRELESS TERMINAL

FIG. 2

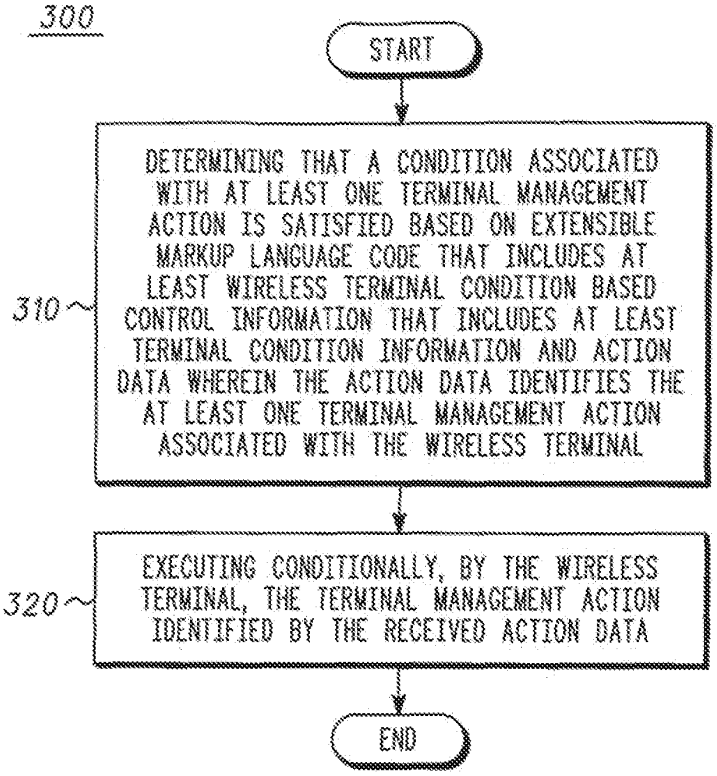

300
START
DETERMINING THAT A CONDITION ASSOCIATED WITH AT LEAST ONE TERMINAL MANAGEMENT ACTION IS SATISFIED BASED ON EXTENSIBLE MARKUP LANGUAGE CODE THAT INCLUDES AT LEAST WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION THAT INCLUDES AT LEAST TERMINAL CONDITION INFORMATION AND ACTION DATA WHEREIN THE ACTION DATA IDENTIFIES THE AT LEAST ONE TERMINAL MANAGEMENT ACTION ASSOCIATED WITH THE WIRELESS TERMINAL
310
EXECUTING CONDITIONALLY, BY THE WIRELESS TERMINAL, THE TERMINAL MANAGEMENT ACTION IDENTIFIED BY THE RECEIVED ACTION DATA
320
END

FIG. 3

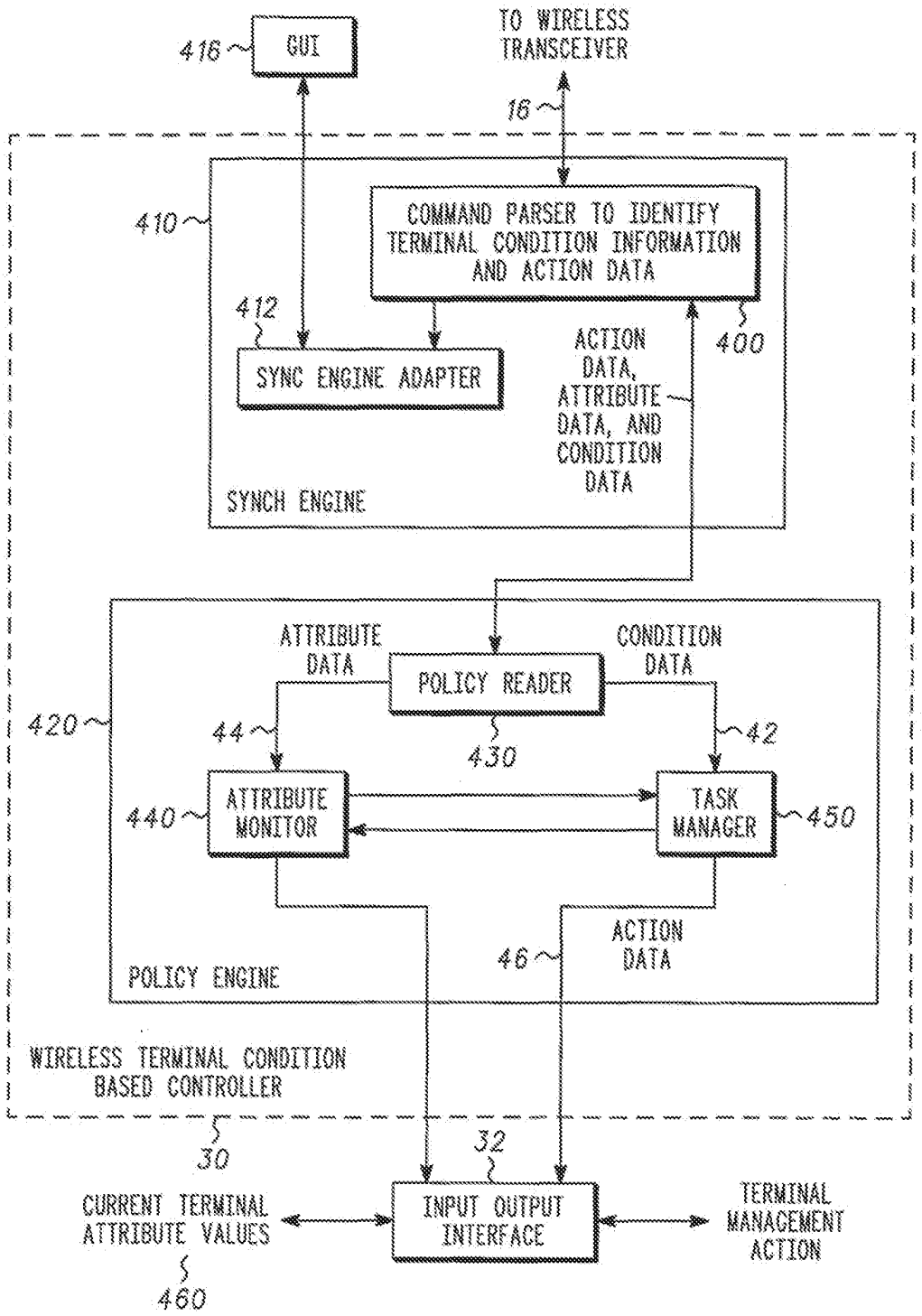

416
GUI
TO WIRELESS TRANSCEIVER
16
410
COMMAND PARSER TO IDENTIFY TERMINAL CONDITION INFORMATION AND ACTION DATA
412
400
SYNC ENGINE ADAPTER
ACTION DATA, ATTRIBUTE DATA, AND CONDITION DATA
SYNCH ENGINE
ATTRIBUTE DATA
CONDITION DATA
POLICY READER
420
44
42
430
440
ATTRIBUTE MONITOR
TASK MANAGER
450
46
ACTION DATA
POLICY ENGINE
WIRELESS TERMINAL CONDITION BASED CONTROLLER
30
32
CURRENT TERMINAL ATTRIBUTE VALUES
460
INPUT OUTPUT INTERFACE
TERMINAL MANAGEMENT ACTION

FIG. 4

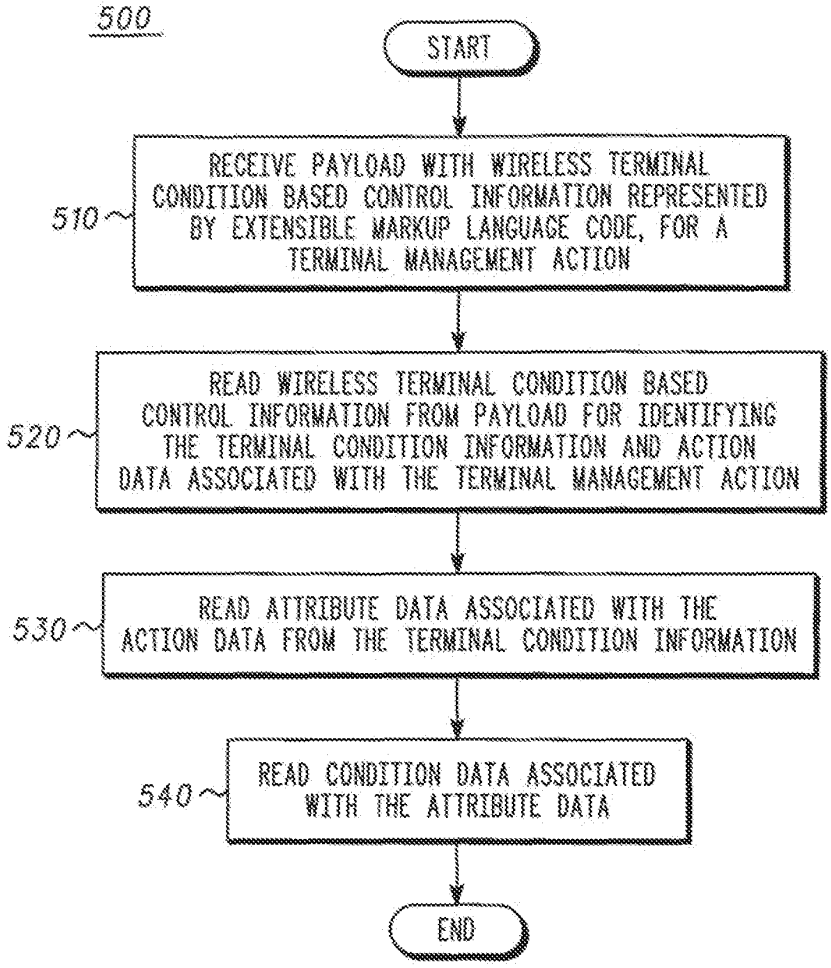

500
START
510
RECEIVE PAYLOAD WITH WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION REPRESENTED BY EXTENSIBLE MARKUP LANGUAGE CODE, FOR A TERMINAL MANAGEMENT ACTION
520
READ WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION FROM PAYLOAD FOR IDENTIFYING THE TERMINAL CONDITION INFORMATION AND ACTION DATA ASSOCIATED WITH THE TERMINAL MANAGEMENT ACTION
530
READ ATTRIBUTE DATA ASSOCIATED WITH THE ACTION DATA FROM THE TERMINAL CONDITION INFORMATION
540
READ CONDITION DATA ASSOCIATED WITH THE ATTRIBUTE DATA
END

FIG. 5

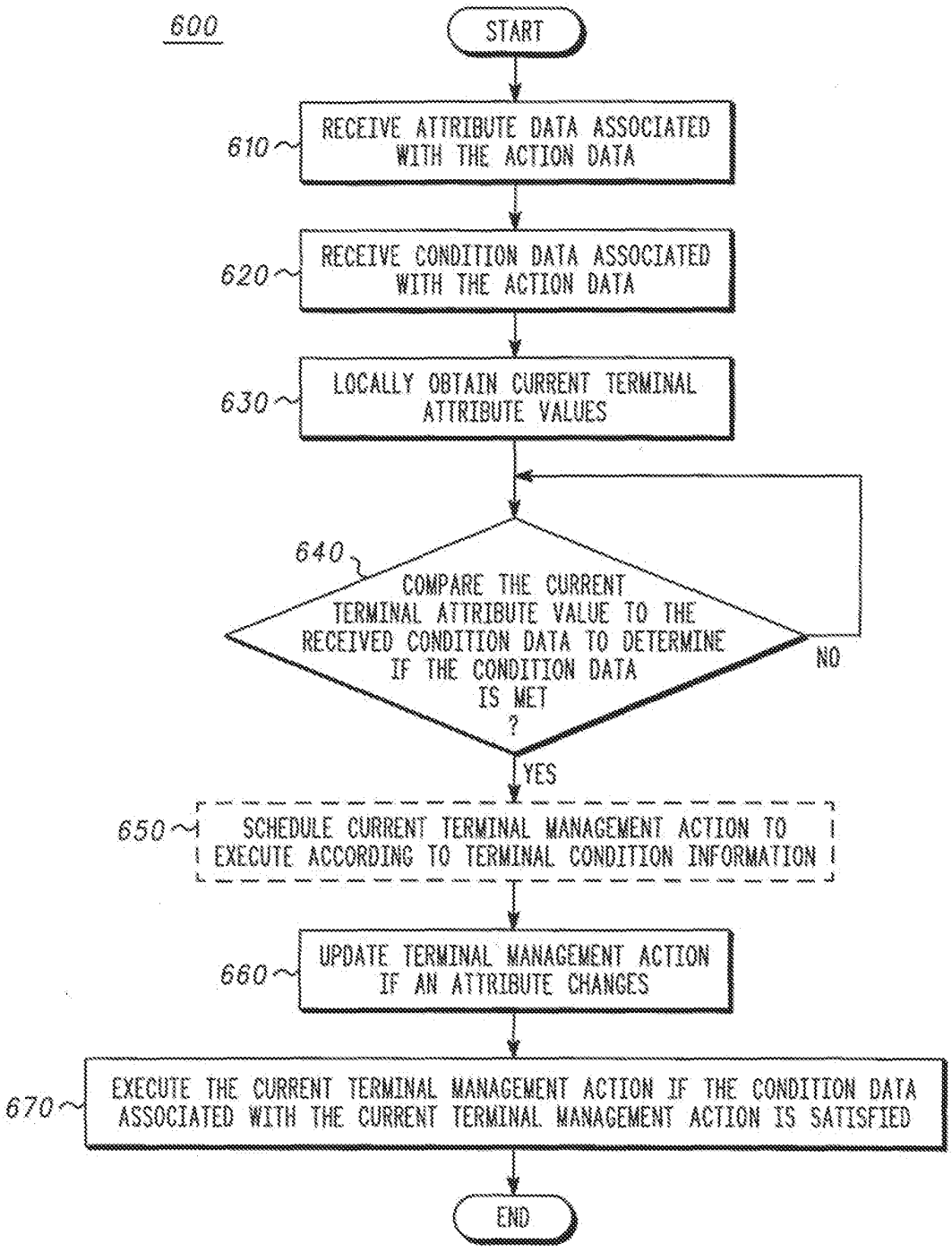

600
START
610
RECEIVE ATTRIBUTE DATA ASSOCIATED WITH THE ACTION DATA
620
RECEIVE CONDITION DATA ASSOCIATED WITH THE ACTION DATA
630
LOCALLY OBTAIN CURRENT TERMINAL ATTRIBUTE VALUES
640
COMPARE THE CURRENT TERMINAL ATTRIBUTE VALUE TO THE RECEIVED CONDITION DATA TO DETERMINE IF THE CONDITION DATA IS MET ?
NO
YES
650
SCHEDULE CURRENT TERMINAL MANAGEMENT ACTION TO EXECUTE ACCORDING TO TERMINAL CONDITION INFORMATION
660
UPDATE TERMINAL MANAGEMENT ACTION IF AN ATTRIBUTE CHANGES
670
EXECUTE THE CURRENT TERMINAL MANAGEMENT ACTION IF THE CONDITION DATA ASSOCIATED WITH THE CURRENT TERMINAL MANAGEMENT ACTION IS SATISFIED
END

FIG. 6

7/10

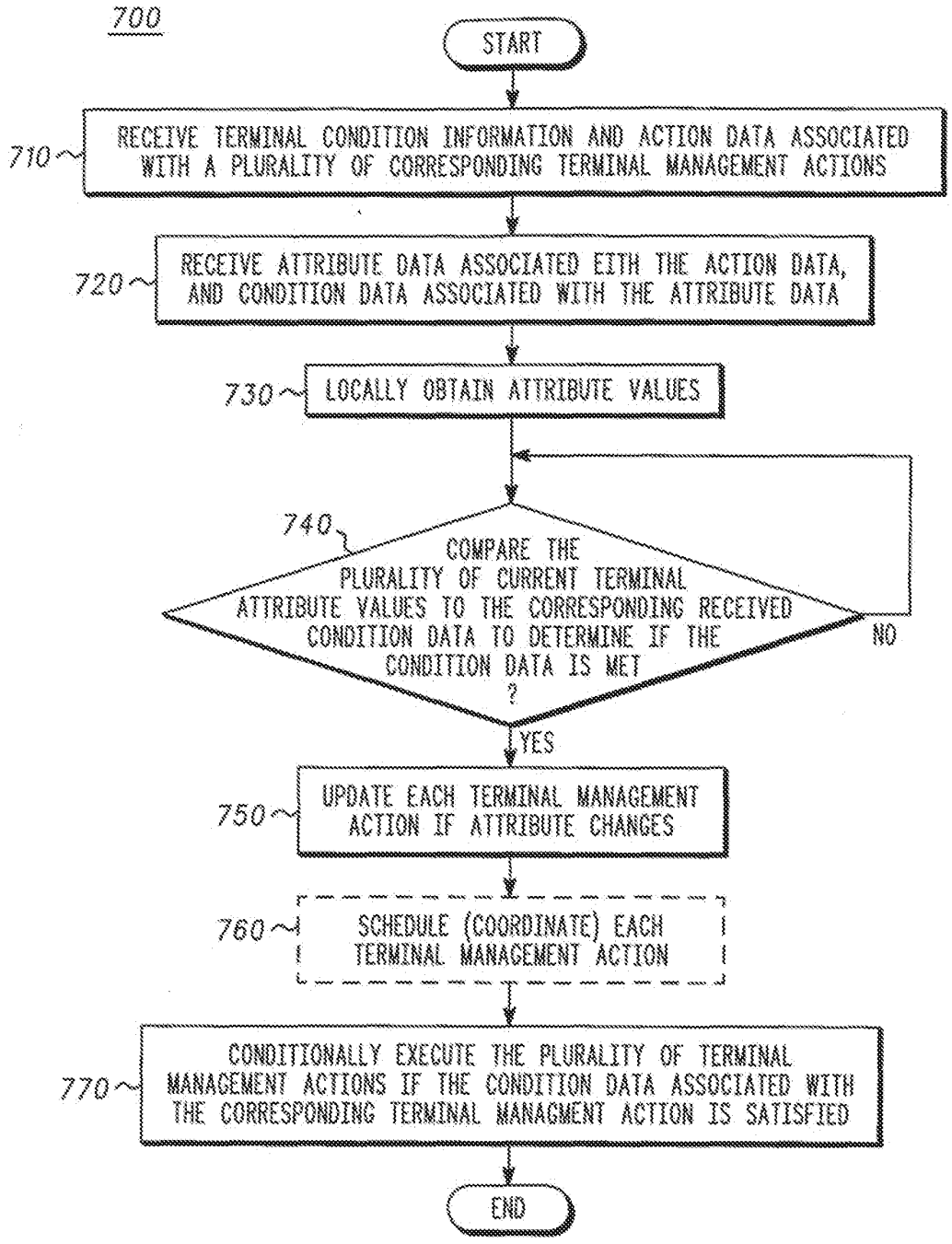

700
START
710
RECEIVE TERMINAL CONDITION INFORMATION AND ACTION DATA ASSOCIATED WITH A PLURALITY OF CORRESPONDING TERMINAL MANAGEMENT ACTIONS
720
RECEIVE ATTRIBUTE DATA ASSOCIATED EITH THE ACTION DATA, AND CONDITION DATA ASSOCIATED WITH THE ATTRIBUTE DATA
730
LOCALLY OBTAIN ATTRIBUTE VALUES
740
COMPARE THE PLURALITY OF CURRENT TERMINAL ATTRIBUTE VALUES TO THE CORRESPONDING RECEIVED CONDITION DATA TO DETERMINE IF THE CONDITION DATA IS MET ?
NO
YES
750
UPDATE EACH TERMINAL MANAGEMENT ACTION IF ATTRIBUTE CHANGES
760
SCHEDULE (COORDINATE) EACH TERMINAL MANAGEMENT ACTION
770
CONDITIONALLY EXECUTE THE PLURALITY OF TERMINAL MANAGEMENT ACTIONS IF THE CONDITION DATA ASSOCIATED WITH THE CORRESPONDING TERMINAL MANAGMENT ACTION IS SATISFIED
END

FIG. 7

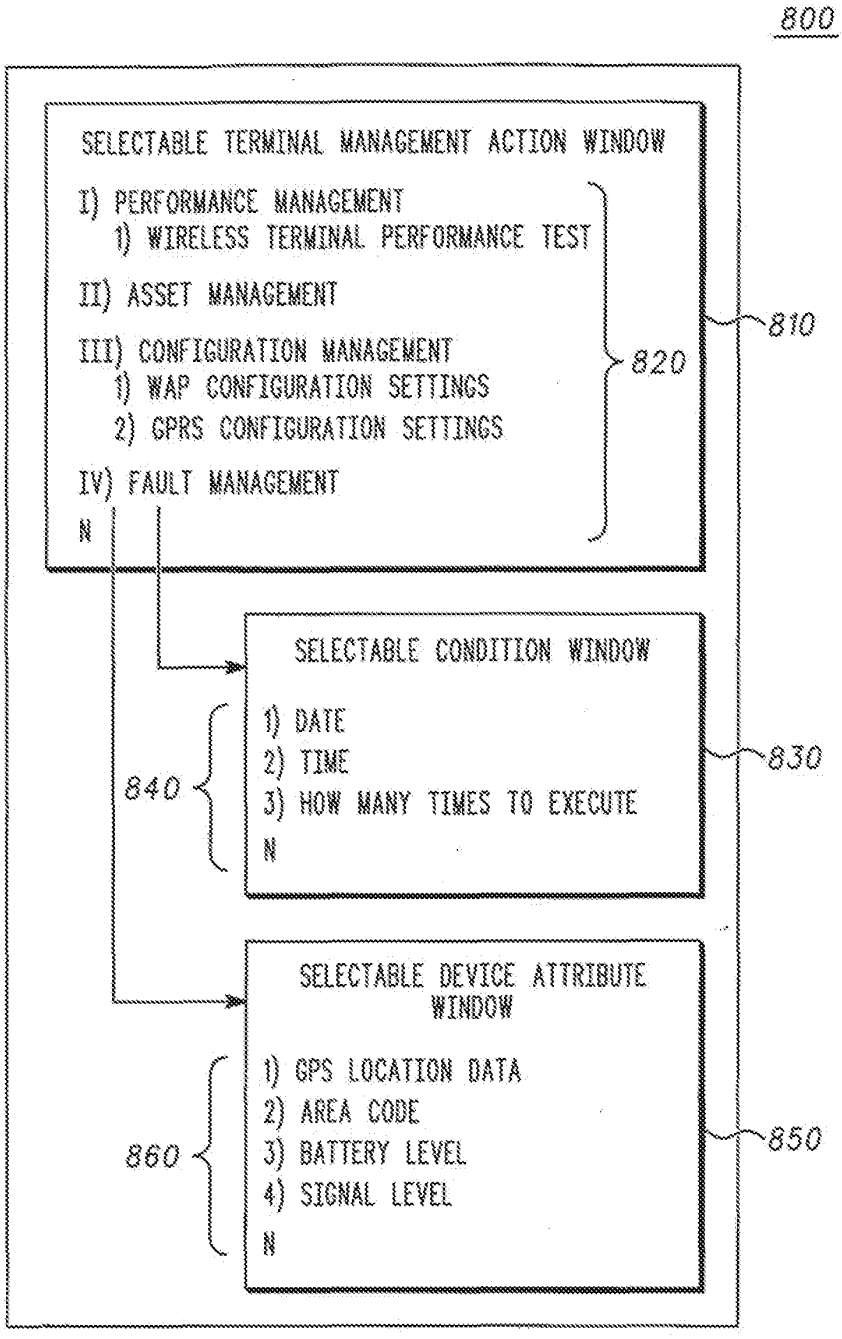

800
SELECTABLE TERMINAL MANAGEMENT ACTION WINDOW
I) PERFORMANCE MANAGEMENT
1) WIRELESS TERMINAL PERFORMANCE TEST
II) ASSET MANAGEMENT
III) CONFIGURATION MANAGEMENT
1) WAP CONFIGURATION SETTINGS
2) GPRS CONFIGURATION SETTINGS
IV) FAULT MANAGEMENT
N
820
810
SELECTABLE CONDITION WINDOW
1) DATE
2) TIME
3) HOW MANY TIMES TO EXECUTE
N
840
830
SELECTABLE DEVICE ATTRIBUTE WINDOW
1) GPS LOCATION DATA
2) AREA CODE
3) BATTERY LEVEL
4) SIGNAL LEVEL
N
860
850

FIG. 8

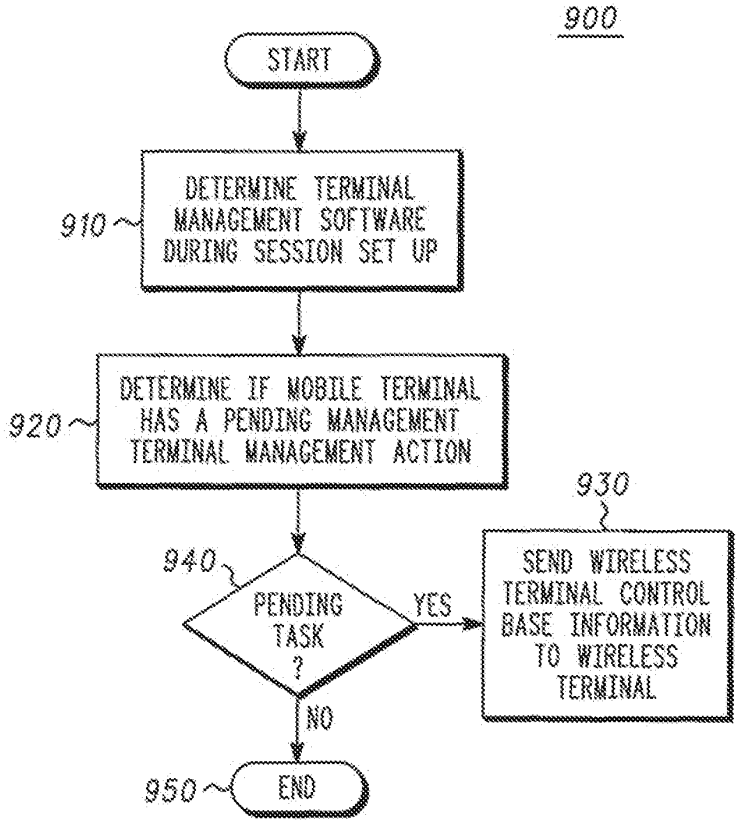

900
START
910
DETERMINE TERMINAL MANAGEMENT SOFTWARE DURING SESSION SET UP
920
DETERMINE IF MOBILE TERMINAL HAS A PENDING MANAGEMENT TERMINAL MANAGEMENT ACTION
930
940
PENDING TASK ?
YES
SEND WIRELESS TERMINAL CONTROL BASE INFORMATION TO WIRELESS TERMINAL
NO
950
END

FIG. 9

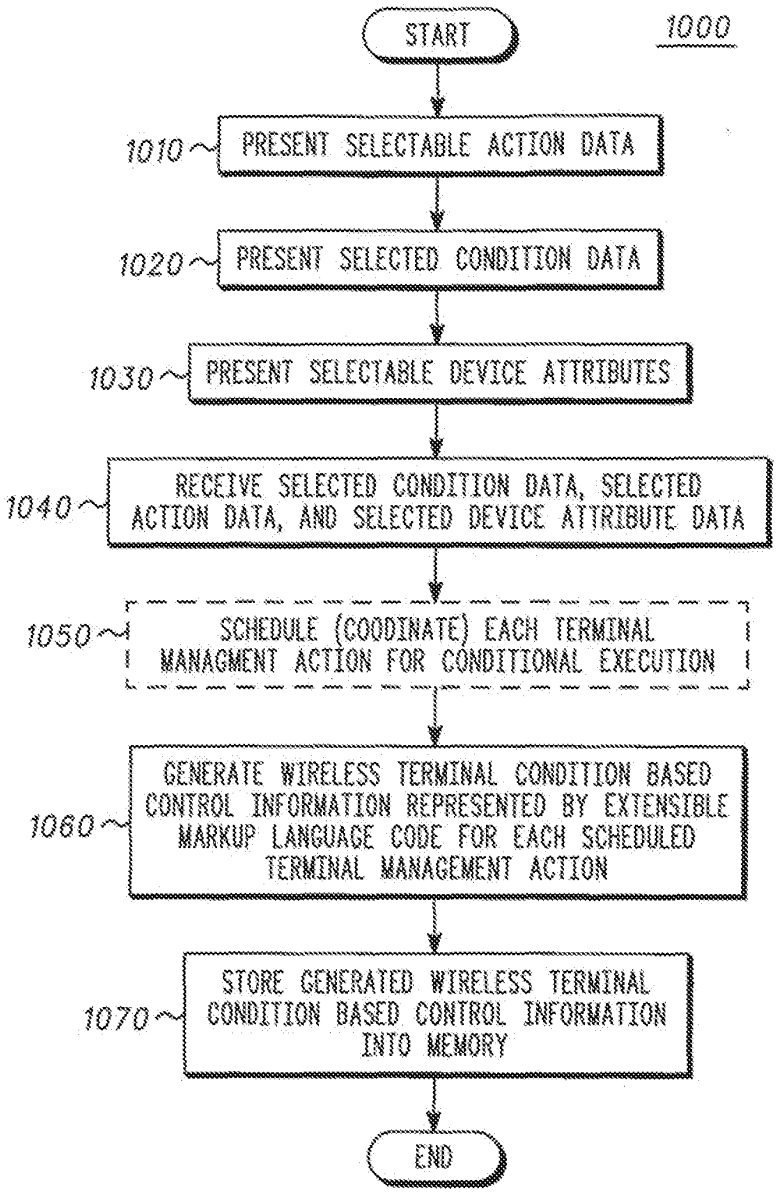

START
1000
1010
PRESENT SELECTABLE ACTION DATA
1020
PRESENT SELECTED CONDITION DATA
1030
PRESENT SELECTABLE DEVICE ATTRIBUTES
1040
RECEIVE SELECTED CONDITION DATA, SELECTED ACTION DATA, AND SELECTED DEVICE ATTRIBUTE DATA
1050
SCHEDULE (COODINATE) EACH TERMINAL MANAGMENT ACTION FOR CONDITIONAL EXECUTION
1060
GENERATE WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION REPRESENTED BY EXTENSIBLE MARKUP LANGUAGE CODE FOR EACH SCHEDULED TERMINAL MANAGEMENT ACTION
1070
STORE GENERATED WIRELESS TERMINAL CONDITION BASED CONTROL INFORMATION INTO MEMORY
END

FIG. 10

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/014891 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/23226

(22) International Filing Date: 19 July 2002 (19.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/309,862 3 August 2001 (03.08.2001) US
09/992,310 19 November 2001 (19.11.2001) US

(71) Applicant: THE BOEING COMPANY [US/US]; P.O. Box 3707, M/S 13-08, Seattle, WA 98124-2207 (US).

(72) Inventor: ROCKWELL, Lawrence, L.; 8018-146th Avenue NE, Redmond, WA 98052 (US).

(74) Agent: GALBRAITH, Ann, K.; The Boeing Company, P.O. Box 3707, M/S 13-08, Seattle, WA 98124-2207 (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, 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*

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.

WO 03/014891 A2

(54) Title: AN AIRBORNE SECURITY MANAGER

(57) Abstract: An airborne security management system is provided for monitoring security activities in a mobile network platform. The airborne security management system includes a mobile network that is interconnected via an unreliable communication link to a terrestrial-based network security management system; an intrusion detection system connected to the mobile network and operable to detect a security intrusion event whose origination is associated with the mobile network; and a mobile security manager adapted to receive the security intrusion events from the intrusion detection system. The mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system. The mobile security manager is further operable to command security response activities on the mobile network platform, when the mobile network platform is not connected with network security management system.

AN AIRBORNE SECURITY MANAGER

[0001] This application claims priority under 35 U.S.C. §119(e) to United States Provisional Application No. 60/309,862 filed on August 3, 2001, and entitled "An Airborne Security Manager" the specification and drawings of which are hereby expressly incorporated by reference.

TECHNICAL FIELD

[0002] The present invention relates generally to an airborne security management system for monitoring security activities in a mobile network platform, and more particularly to an autonomous airborne security manager for responding to detected security intrusion events when the mobile network platform is or is not in communication with a terrestrial-based network security management system.

BACKGROUND OF THE INVENTION

[0003] Broadband data and video services, on which our society and economy have grown to depend, have heretofore generally not been readily available to users onboard mobile network platforms such as aircraft, ships, trains, automobiles, etc. While the technology exists to deliver such services to most forms of mobile network platforms, past solutions have been generally quite expensive, with low data rates and/or available to only very limited markets of government/military users and some high-end maritime markets (i.e., cruise ships).

[0004] Previously developed systems which have attempted to provide data and video services to mobile network platforms have done so with only limited success. One major obstacle has been the high cost of access to such broadband data and video services. Another problem is the limited capacity of previously developed systems, which is insufficient for mobile network platforms carrying dozens, or even hundreds, of passengers who each may be simultaneously requesting different channels of programming or different data services. Furthermore, presently existing systems are generally not readily scalable to address the demands of the traveling public.

[0005] Of particular interest, presently existing systems also have not comprehensively addressed security issues relating to the mobile network platform. Therefore, it is desirable to provide a network security architecture for monitoring, reporting and responding to onboard security activities in a mobile network platform. It is envisioned that such a network security architecture should be designed to (a) secure computing resources to which passengers may have access on the mobile platform; (b) communicate reliably with terrestrial-based system components over an unreliable communication link; (c) provide a policy mediated response to detected security intrusion events occurring on the mobile platform; and (d) scale the management of the system to hundreds or thousands of mobile platforms.

SUMMARY OF THE INVENTION

[0006] In accordance with the present invention, an airborne security management system is provided for monitoring security activities in a mobile network platform. The security management system includes a mobile network that is interconnected via an unreliable communication link to a terrestrial-based network security management system; an intrusion detection system connected to the mobile network and operable to detect a security intrusion event whose origination is associated with the mobile network; and a mobile security manager adapted to receive the security intrusion events from the intrusion detection system. The mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system. The mobile security manager is further operable to command security response activities on the mobile network platform, when the mobile network platform is not connected with network security management system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The various advantages of the present invention will become apparent to one skilled in the art by reading the following specification and subjoined claims and by referencing the following drawings in which:

[0008] Figure 1 is a block diagram depicting a network security

architecture for a mobile network platform in accordance with the present invention;

[0009] Figures 2A and 2B are state machine diagrams illustrating a security policy for a given user access point on the mobile network platform in accordance with the present invention;

[0010] Figure 3 is a diagram of an exemplary data structure for implementing the security policies of the present invention;

[0011] Figure 4 is a diagram depicting the primary software components of the network security architecture of the present invention;

[0012] Figure 5 is a block diagram depicting the functional software modules which comprise the airborne security manager in accordance with the present invention;

[0013] Figure 6 is a block diagram depicting the functional components implementing the terrestrial control and data storage functions of a terrestrial-based network security system in accordance with the present invention;

[0014] Figure 7 is an exemplary aircraft browser window used to implement the monitoring and manual control functions of a terrestrial-based network security system in accordance with the present invention; and

[0015] Figure 8 is an exemplary aircraft status window used to implement the monitoring and manual control functions of a terrestrial-based network security system in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Figure 1 illustrates a network security architecture 10 for

monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform 12. In a preferred embodiment, the network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based communication system16, including a terrestrial-based network security management system 18. While the following description is provide with reference to an airborne application, it is readily understood that the broad aspects of the network security architecture are applicable to mobile network platforms which may reside in passenger buses, cruise ships, etc.

[0017] It is envisioned that the mobile network platform 12 provides aircraft passengers a suite of broadband two-way data and video communication services. The infrastructure allows information to be transferred to and from the aircraft at high enough data rates to support a variety of services. To do so, the mobile network platform 12 is primarily comprised of four subsystems: an antenna subsystem 22, a receive and transmit subsystem (RTS) 24, a control subsystem 26, and a cabin distribution subsystem 28. Each of these four subsystems will be further described below.

[0018] The antenna subsystem 22 provides two-way broadband data connectivity and direct broadcast television reception capability to the aircraft. Although the invention is not limited thereto, the antenna subsystem 22 is generally designed to provide this connectivity during cruise conditions (limited roll

and pitch angles) of the aircraft. Connectivity with the aircraft is most commonly achieved via a K band Fixed Satellite Service (FSS) satellite, a Broadcast Satellite Service (BSS) satellites, and/or a direct broadcast television service (DBS) satellite.

[0019] For illustration purposes, additional description is provided for the processing associated with Ku band satellite broadcast signals. The antenna subsystem 22 may receive and/or transmit Ku band satellite broadcast signals. The antenna system 22 down-converts an incoming Ku-band signal, amplifies, and outputs the L-band signals to the RTS 24. The antenna system may also provide a broadband downlink capability. In this case, the antenna system 22 receives an L-band data signal from an on-aircraft modem, up-converts this signal, amplifies it and then broadcasts as a Ku band signal to selected satellite transponders.

[0020] The receive and transmit subsystem (RTS) 24 operates in receive and transmit modes. In receive mode, the RTS 24 may receive rebroadcast video signals, rebroadcast audio signals and/or IP data embedded in an L-band carrier. The RTS 24 in turn demodulates, de-spreads, decodes, and routes the received signals to the cabin distribution subsystem 28. In transmit mode, the RTS 24 sends IP data modulated into an L-band signal. The RTS 24 encodes, spreads, and modulates the signal the IP data it receives from the cabin distribution subsystem 28.

[0021] The control subsystem 26 controls the operation of the mobile security platform 12 and each of its four subsystems. Of particular interest, the control subsystem 26 includes one or more intrusion detection subsystems 32 and

an airborne security manager 34. An intrusion detection subsystem 32 is operable to detect security intrusion activities which may occur on or in relation to the mobile network platform. To do so, an intrusion detection subsystem 32 inspects all of the data packets entering a computing device on which it is hosted and, upon detection of a security intrusion activity, transmits a security intrusion event to the airborne security manager 34. As will be apparent to one skilled in the art, the intrusion detection subsystem 32 may be implemented using one of many commercially available software products.

[0022] The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. Exemplary responses may include warnings one or more passengers on the aircraft, alerting terrestrial-based security administrators, and/or disconnecting a passenger's network access.

[0023] The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. In a preferred embodiment, the cabin distribution system may be composed of either a series of 802.3 Ethernet switches or 802.11X wireless access points. It should be noted that the current 802.11B standard only allows

for a shared secret between all users of a wireless access point and thus is not suitable for providing the desired level of communication privacy in the passenger cabin. In contrast, next generation wireless standards, such as 802.11X ("X" denotes a revision of 802.11 beyond "B") will support "channelized" or individual user level encryption. It is envisioned that such wireless standards are within the scope of the present invention.

[0024] Each user access point preferably has the properties of a managed layer 3 switch. First, each user access point must enforce the association of IP address and MAC address with a particular port. This requirement his applicable to either a wired and wireless cabin environment. A second requirement for each user access point is to accept a command to shut off its access port. In the case of a wireless access device, a communication channel consisting of a particular frequency, time division or sub-frame substitutes for the physical access port. A third requirement for each user access point is to preclude passengers from eavesdropping or receiving Ethernet packets not directly addressed to them. In a wired cabin distribution system, this can be accomplished through the use of a switched Ethernet architecture. In a wireless cabin distribution system, this can be accomplished through the use of "channel level encryption" specific to a particular user.

[0025] The design of a security policy mechanism is the most fundamental element of the network security architecture 10. In accordance with the present invention, it is envisioned that the security policy will be designed within the following design constraints. First, the security policy mechanism should map different security intrusion events to different responses. It should be

appreciated that the severity of response is based on the danger of the detected activities. Second, the automated response policy has to be enforced at all times (subject to over-ride conditions), regardless of whether airborne to terrestrial communications are available or not. If the automated responses are disabled during periods of connectivity, the connectivity might fail before a security administrator has a chance to take action in which case the system reverts to the automated policy in effect prior to the override. The security administrator can retract the response if they desire. Third, the policy mechanism has to arbitrate between automated responses from the airborne security manager and manual commands received from terrestrial-based security administrators. If the automated system mistakenly blocks a passenger's network address, and the terrestrial administrator overrides that action, the security policy mechanism needs to know about that action and not try to enforce the block.

[0026] State machines are a flexible, yet intuitively appealing, mechanism for modeling complex behaviors. Therefore, state-machines have been chosen to represent the security policies of the present invention. Figures 2A and 2B illustrates basic UML state machines which model the security policy associated with an user access point in the mobile network platform.

[0027] In Figure 2A, each user access point can be in one of three defined states. By default, all user access points begin in a normal state 42. A security intrusion event of any kind will result in a transition to either a suspected state 44 or a disconnected state 46 for the applicable user access point. Each transition is in the form of "event/response" where events are the external triggers that cause the state transition and responses are external actions that the system

initiates when making the transition. For instance, a low or medium priority event 48 occurring in a normal state will cause the system to log the event and/or attempt to provide a warning to the passenger connected at that user access point. The user access point then transitions to the suspected state as shown in Figure 2A.

State machine models may be enhanced to incorporate manual controls. Specific manual control commands enable a terrestrial-based security administrator to explicitly disable or enable a user access point from the ground. By adding a state that indicates that the user access point is under manual control ensures that the automated responses do not override the manual control command received from the security administrator. Therefore, it is envisioned that each state machine may provide an autoresponse disable state 50 as shown in Figure 2B. Transitions to and from the autoresponse disable state are commanded by a terrestrially-based security administrator. While in the autoresponse disable state, the administrator can initiate any one of various predefined security responses. In the event connectivity is lost between the administrator and the aircraft, the state machine model reverts to the normal state or the previous state depending on configuration settings.

State machines models are also used to represent each of the host servers or other types of computing devices which reside on the mobile security platform. In this way, a server that is under attack may respond differently than a user access point. It is also envisioned that each of the state machines can be tied together through synthetic event generation, such that when a server is under attack, the user access points may employ a different security policy that is less

tolerant of suspicious behavior.

[0028] Each state machine can be represented by a data structure 51 as depicted in Figure 3. The data structure includes a current state 52, a possible security event 54, a resulting state 56 and a possible response 58. In this way, each state can be cross-referenced against possible events to produce a resulting state and a list of possible actions. Possible events may include (but are not limited to) a security intrusion event having high priority, a security intrusion event having medium priority, a security intrusion event having a low priority, a reset event, a timer expiration event, a communication link up event, a communication link down event and one or more custom events for supporting manual control commands from the security administrator. Possible responses may include (but are not limited to) setting a timer, installing a filter, resetting a filter, alerting control panel, alerting terrestrial-based security administrator, disconnecting user access point, issuing a passenger warning, and one or more predefined customer responses. One skilled in the art will readily recognize from such discussion how to implement a security policy mechanism in accordance with the present invention.

[0029] Referring to Figure 4, the overall network security architecture 10 may be logically decomposed into five major components. The five major components are airborne policy enforcement 62, air-ground communication 64, terrestrial control and data storage 66, terrestrial monitoring and manual control 68, and terrestrial policy editing and assignment 70. Each of these logical components are also mapped to their physical location within the network security architecture 10 as shown in Figure 4.

[0030] The airborne policy enforcement component 62 is provided by the airborne security manager 34. The primary responsibilities of the airborne security manager include (but are not limited to) managing and monitoring intrusion detection sensors, monitoring other airborne event sources, responding to security events in accordance with the applicable security policy, monitoring the airborne intrusion detection sensors, configuring static network traffic filters at user access points, executing any manual overrides commands from the terrestrial-based network security management system, installing new security policies received from the terrestrial-based network security management system, and reporting events and status of interest to the terrestrial-based network security management system. As will be apparent to one skilled in the art, the airborne security manager 34 is comprised of one or more software applications residing on one or more server(s) on each aircraft. A configuration of redundant airborne security managers provide for fail over in the event of a hardware or software failure.

[0031] With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems.

[0032] In conjunction with the onboard status module 74, the event

response module interprets and executes the state machine representing the active security policy. For instance, upon arrival of a security intrusion event, the event response module determines whether the event is associated with an individual passenger connection, an individual host server, or the airborne security manager as a whole. This module then retrieves the current state of that passenger connection, host server, or airborne security manager from the onboard status module 74 and performs the actions associated with that state and event in accordance with the active security policy. Exemplary actions may include issuing new events, making state transitions, modifying network filters, disabling passenger connections, and/or queuing messages for transmission to the terrestrial-based network security management system.

[0033] The onboard status module 74 maintains the current state of each individual passenger connection, each host server, and of the airborne security manager as a whole for the purpose of directing the state machine event response. The onboard status module 74 also tracks the status of intrusion detection sensors (e.g., signature file, operational/inactive status, sensor configuration) as well as collects status information from the other onboard modules.

[0034] The policy manager 76 is responsible for reacting to commands from the terrestrial-based network security system regarding security policy loading and activation. The policy manager also serves as a repository for configuration information relating to the airborne security manager, including, for instance, general communications parameters that determine frequency of status reports and event reporting.

[0035] The persistent storage manager 78 manages the overall data storage requirements for the onboard network security architecture. Data residing in persistent storage generally falls into one of three categories: (1) communications queue (i.e., messages to be transmitted to the terrestrial-based security management system), (2) onboard status (i.e., per-passenger connection, per-host, and system-wide data requirements), and (3) security policies. The persistent storage manager may rely on various well known, lightweight mechanisms for data storage.

[0036] Referring to Figure 4, the terrestrial control and data storage (C&DS) component 66 is provided by the terrestrial-based network security management system 16. The control and data storage functions include (but are not limited to) storing all event data in persistent storage, tracking the desired and last known configurations for each aircraft, supporting multiple security management consoles having multiple windows, notifying open console windows of any data changes that affect the window contents, providing an interface for effecting manual overrides in security policy, offering a reporting interface for reviewing stored data, and controlling access to all stored data. This component may be implemented using Java-based applications residing on one or more terrestrial servers which constitute the network security management system 16.

[0037] A more detailed description of the terrestrial control and data storage component 66 is provided with reference to Figure 6. This terrestrial component will maintain one aircraft object 90 for each aircraft associated with the security architecture. The aircraft object 90 maintains all state information for a given aircraft as well as keeps track of the last reported and the desired state of

the airborne security manager 34 residing on the given aircraft. The aircraft object 90 is a dynamic object, such that it state is maintained in dynamic memory and can be reconstructed from event histories, if necessary. Any activity that could alter the state of the airborne security manager 34 is performed by invoking a method of the aircraft object. Each method represents an event and is logged in an appropriate event log. In addition, these methods are all synchronized, ensuring that only one thread can be effecting state changes at any given time. In order to eliminate the possibility of deadlock, none of these event operations will block on communication or issue events to other aircraft.

[0038] The aircraft object 90 uses a communication subsystem 100 to exchange information with the airborne security manager 34. The aircraft object 90 issues commands and requests for status reports as well as receives events and status reports. Until an appropriate event or status report is received, any command is considered pending. This does not mean that the command has not yet executed – it may not have been executed, or it may have been and the acknowledging status report has simply not yet been received. Due to this gap in knowledge about what is actually taking place onboard the aircraft, the aircraft object 90 must carefully differentiate between the last known status and the desired status.

[0039] The aircraft object 90 is the controller in a Model-View-Controller architecture as is well known in the art. In this paradigm, the model is the data stored in a database, and the views are the various user interfaces being used to display information about the aircraft. The aircraft object is responsible for updating all of the views any time the model changes. In order to enforce this, all

changes to the model must be performed by the aircraft object and the aircraft object must keep track of those user interfaces that could be affected by the change.

[0040] The aircraft object 90 also maintains a collection of host objects 92 and passenger connection objects 94. The host objects 92 are used to represent the state of each onboard host server that the airborne security manager 34 is responsible for. The passenger connection objects 94 represent the individual passenger connections to the onboard network.

[0041] The terrestrial control and data storage component 66 also includes a single aircraft container object 96. It is envisioned that this object may be implemented as a collection class, such as a hash table. Under this approach, aircraft objects will be created by the aircraft container 96 for every aircraft in the system. By routing incoming communication through the aircraft container 96, we ensure that the communication subsystem 100 will be able to deliver incoming messages to the appropriate aircraft object. In addition, the container concept may be used to facilitate the manner in which aircraft objects are created. For instance, aircraft objects may be created only as they are needed. When an incoming message is received, the aircraft container 96 locates the applicable aircraft object. If the aircraft object is not present in memory, the aircraft container can create the object. Likewise, aircraft objects that are no longer being actively monitored could be deleted until they are needed again.

[0042] The terrestrial control and data storage component 66 will also maintain event histories for each of the aircraft in a central database 98. The database 98 will maintain a record of all the events reported by an aircraft in the

system. In addition, it will maintain a record of all of the commands performed by terrestrial-based security administrator. The former represents the last known state of each aircraft; whereas the latter represents the desired stated of each aircraft. The choice of the term "last known" reflects the time delay between events occurring on board the aircraft which might not have been reflected on the ground.

[0043] Security policy files are also stored within the database 98. As a configuration option, in order to maintain a history of old policies, the policy tables may be append-only. The primary policy table will maintain a mapping of names and version numbers to a series of smaller policy elements. The communication subsystem 100 interfaces with the database 98 in order to retrieve security policy files and update the policy files onboard the aircraft.

[0044] A policy manager 99 will be responsible for any changes to policy files. This object is necessary because policy is the only thing that is not associated with a single aircraft. The policy manager 99 will ensure that any changes to policy files are properly versioned. It will also be responsible for delivering updated policy to one or more aircraft.

[0045] Returning to Figure 4, the terrestrial monitoring and manual control component 68 and the terrestrial policy editing and assignment component 70 also reside at the terrestrial-based network security management system 12. The monitoring and manual control component functions include (but are not limited to) monitoring the state and activities of a group of aircraft and selecting an individual aircraft for closing examination, monitoring the state and activities of a single aircraft and selecting an individual server or passenger connection for

closer examination, monitoring the state and activities of a single airborne server, manually controlling a single airborne server, monitoring the state and activities of a single airborne passenger connection, and manually controlling a single airborne passenger connection. This component may be implemented using a Java-based user interface running on one or more terrestrial servers.

[0046] To support the monitoring and manual control functions, the user interface includes a number of windows that may be monitored by a human network security administrator. For instance, an aircraft browser allows groups of aircraft to be navigated and aggregate/summary information displayed as shown in Figure 7. However, this window does not show the status of the communication link. In order to display such status information, the user can select a specific aircraft from the aircraft browser, thereby navigating to an aircraft status window. An exemplary aircraft status window is shown in Figure 8. The aircraft status window enables the user to view all data relevant to a specific aircraft in a single tree structure view 102. In addition, all logged events and commands are displayed in a lower log panel 104. The tabs 106 along the top of the window permit navigation to other panels which in turn focus on a different specific element associated with the aircraft. For instance, the seat panel 108 will provide status information, log detail, and manual controls for a specific seat. Other exemplary windows used to support the monitoring and manual control functions may include (but is not limited to) a passenger connection status window that focuses on displaying information for a single passenger connection, an onboard host status window that focuses on displaying information on a specific host computing device residing on the aircraft, and an events log window that displays

event information for a given group, aircraft, passenger connection or host device. It is envisioned that the above-described windows are merely representative of some of the functionality and appearance that be used to implement the monitoring and manual control functions of the present invention.

[0047] In addition to monitoring and manual control, services for editing security policy files and distributing security policy updates also reside at the terrestrial-based network security management system 16. The policy editing and application functions include (but are not limited to) editing sensor configuration files, retrieving intrusion detection signature file updates from the applicable vendor website, editing response policy state machines and parameters, editing static security configurations, combining sensor files, signature files, response policies, and static configuration into specific security policies, providing version control over security policy updates, browsing the aircraft in the system by last known policy and desired policy, and distributing a new policy to a selected group of aircraft. The editing of security policy is not intended to be a routine daily activity. For this reason, policy editing and application functions are treated as a separate, distinct logical component from the other functions administered through the user interface running on the terrestrial servers.

[0048] The air-ground communication component 64 is responsible for communication between the airborne security manager and the terrestrial servers. Thus, this component is distributed across these two physical locations. The air-ground communication functions include (but are not limited to) providing non-blocking communications, retrying transmissions until reliable delivery is achieved, queuing up messages during periods of non-connectivity, handling communication

session authentication, utilizing cryptographic integrity checks to protect against tampering and replay, optimizing away redundant or superseded messages where possible, utilizing available bandwidth according to message priorities, minimizing bandwidth consumption, and delivering security policy updates to aircrafts. Logically isolating the communications component helps protect the design of the airborne security manager and the terrestrial servers from unnecessary complexity arising from sporadic connectivity.

[0049] The foregoing discussion discloses and describes preferred embodiments of the invention. One skilled in the art will readily recognize from such discussion, and from the accompanying drawings and claims, that changes and modifications can be made to the invention without departing from the true spirit and fair scope of the invention as defined in the following claims.

What is claimed is:

1. A network security architecture for monitoring security activities in a mobile network platform, comprising

a mobile network residing on the mobile network platform, the mobile network being interconnected via an unreliable communication link to a terrestrial-based network security management system;

an intrusion detection system connected to the mobile network and residing on the mobile network platform, the intrusion detection system operable to detect a security intrusion event that is associated with the mobile network; and

a mobile security manager residing on the mobile network platform and adapted to receive the security intrusion events from the intrusion detection system, the mobile security manager is further operable to perform security response activities in response to the security intrusion events, when the mobile network platform is not connected with network security management system.

2. The network security architecture of Claim 1 wherein the mobile security manager is operable perform security response activities in accordance with a security policy resident on the mobile network platform.

3. The network security architecture of Claim 2 wherein the security policy is defined as a plurality of predefined security intrusion events and a

corresponding security response for each of said plurality of security intrusion events.

4. The network security architecture of Claim 2 wherein the security policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

5. The network security architecture of Claim 1 wherein the mobile network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one of the plurality of user access points.

6. The network security architecture of Claim 5 wherein the security response is selected from the group consisting of logging the security intrusion event received from the intrusion detection system, providing a warning message to at least one of said user access points, providing an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of said user access points, and disconnecting one of said user access points from the mobile network.

7. The network security architecture of Claim 5 wherein the mobile security manager maintains an indicator of the current operational state for each

of the plurality of user access points, such that the security response directed to said one of the plurality of user access points is in part based on the operational state of said one of the plurality of user access points.

8. The network security architecture of Claim 7 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

9. The network security architecture of Claim 7 wherein the mobile security manager is further operable to identify the current operational state for said one of the plurality of user access points and perform security response activities based in part on the identified operational state and the security intrusion event received from the intrusion detection system.

10. The network security architecture of Claim 9 wherein the mobile security manager is further operable to modify the current operational state for said one of the plurality of user access points in accordance with the security policy.

11. The network security architecture of Claim 1 wherein the mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the

network security management system.

12. A method for monitoring security activities associated with a network residing in a mobile network platform, the mobile network platform being interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

detecting a security intrusion event whose origination is associated with the network residing on the mobile network platform;

providing a mobile security manager residing on the mobile network platform, where the mobile security manager is adapted to receive the security intrusion event; and

performing a security response activity in response to the detected security intrusion event, when the mobile network platform is not connected with the network security management system.

13. The method of Claim 12 wherein the step of performing a security response activity further comprises applying the security response activity in accordance with a security policy, where the security policy is defined as a plurality of predefined security intrusion events and a corresponding security response for each of said plurality of security intrusion events.

14. The method of Claim 12 further comprising the steps of applying the security response activity in accordance with a security policy, where the security policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

15. The method of Claim 12 wherein the network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one of the plurality of user access points.

16. The method of Claim 15 wherein the security response activity is selected from the group consisting of logging the security intrusion event, providing a warning message to at least one of the user access points, providing an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of the user access points, and disconnecting one of the user access points from the network.

17. The method of Claim 16 further comprising the steps of maintaining an indicator of the current operational state for each of the plurality of user access points and performing a security response activity in response to the detected security intrusion event, where the security response activity is in part based on the operational state of said one of the plurality of user access points.

18. The method of Claim 17 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

19. An airborne security system for monitoring security activities associated with a network residing on an aircraft, the aircraft being interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

an intrusion detection system connected to the network and operable to detect a security intrusion event that is associated with network; and

an airborne security manager connected to the network and adapted to receive the security intrusion event from the intrusion detection system, the security manager is further operable to perform security response activities in accordance with a security policy, when the aircraft is not connected with the network security management system.

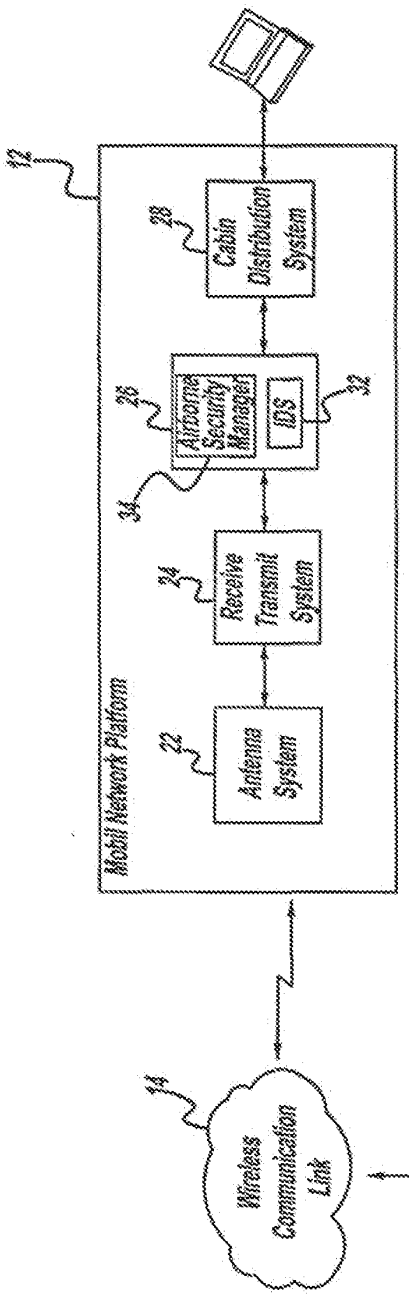

12
Mobil Network Platform
22
Antenna System
24
Receive Transmit System
26
Antenna Security Manager
32
OS
28
Cabin Distribution System
14
Wireless Communication Link
16
Ground Comm System
18
Terrestrial Network Security Management System

Figure - 1

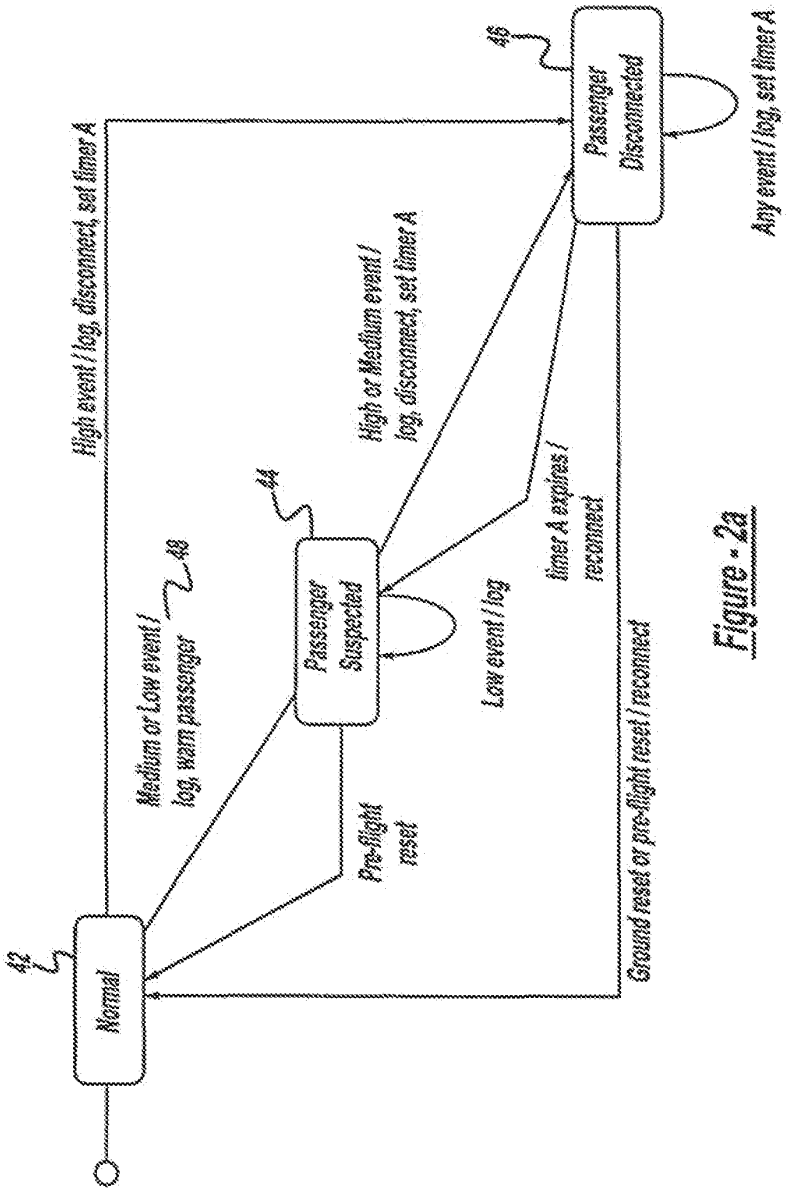

42
Normal
High event / log, disconnect, set timer A
Medium or Low event / log, warn passenger
48
44
Passenger Suspected
Pre-flight reset
High or Medium event / log, disconnect, set timer A
Low event / log
timer A expires / reconnect
46
Passenger Disconnected
Any event / log, set timer A
Ground reset or pre-flight reset / reconnect

Figure - 2a

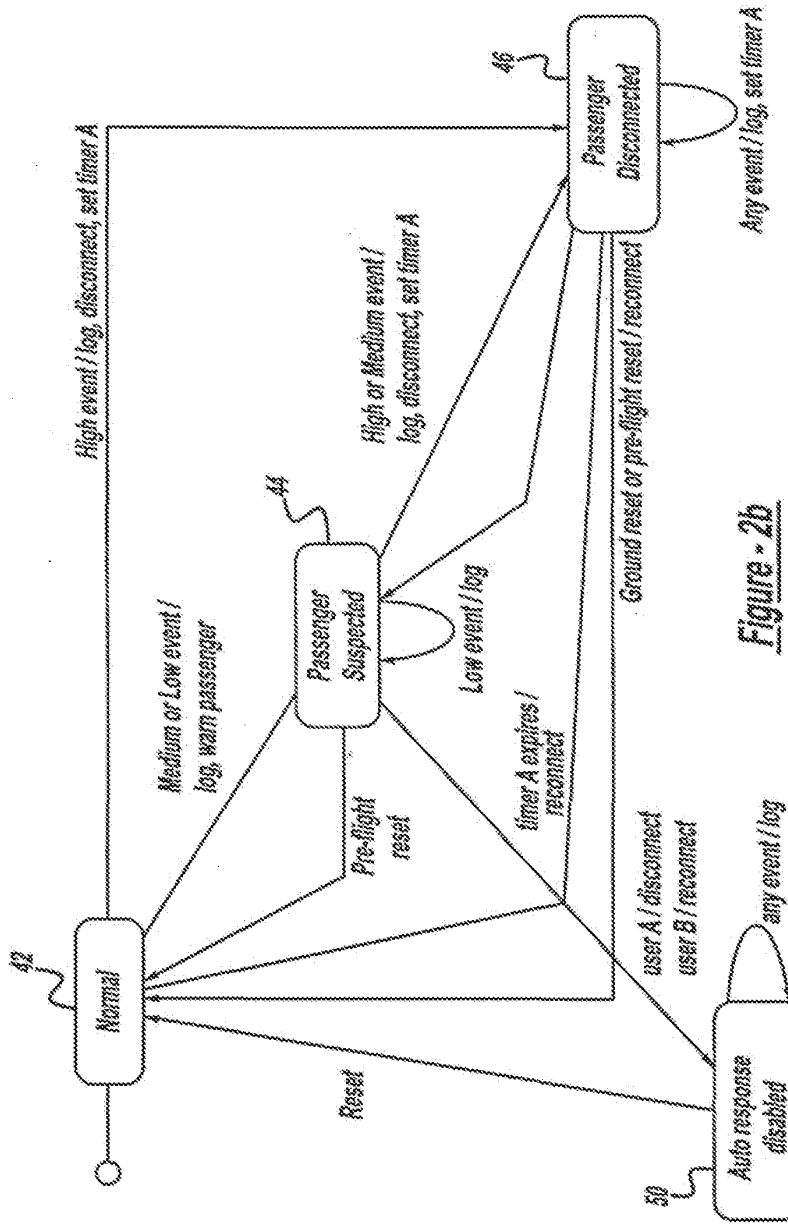

42
Normal
44
Passenger Suspected
46
Passenger Disconnected
50
Auto response disabled
High event / log, disconnect, set timer A
Medium or Low event / log, warn passenger
Pre-flight reset
High or Medium event / log, disconnect, set timer A
Low event / log
timer A expires / reconnect
Ground reset or pre-flight reset / reconnect
Any event / log, set timer A
user A / disconnect user B / reconnect
any event / log
Reset

Figure - 2b

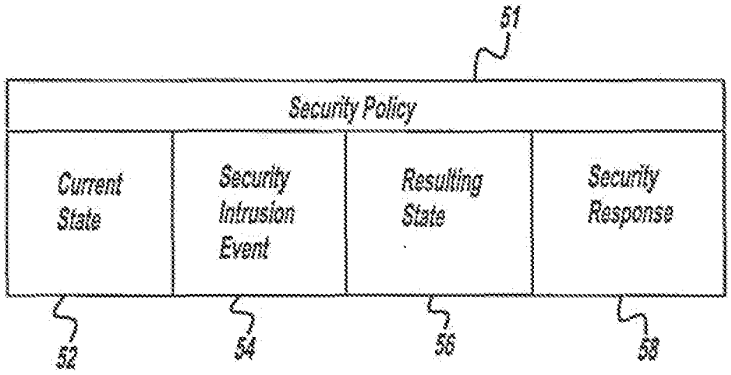

51
Security Policy
Current State
Security Intrusion Event
Resulting State
Security Response
52
54
56
58

Figure - 3

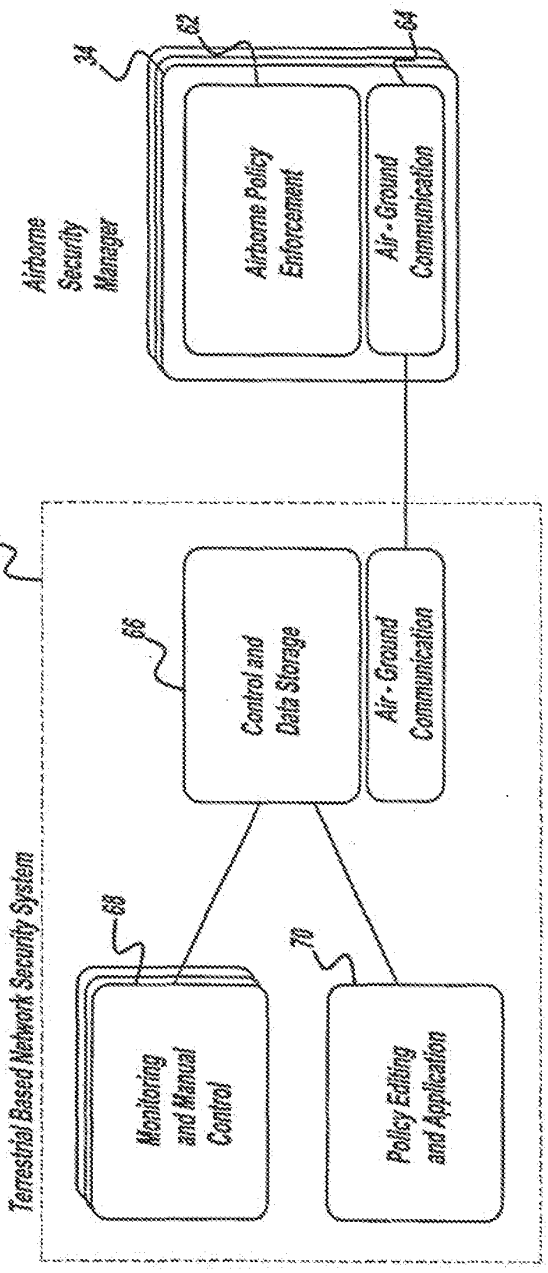

Airborne Security Manager
34
62
64
Airborne Policy Enforcement
Air - Ground Communication
16
Terrestrial Based Network Security System
66
Control and Data Storage
Air - Ground Communication
68
Monitoring and Manual Control
70
Policy Editing and Application

Figure - 4

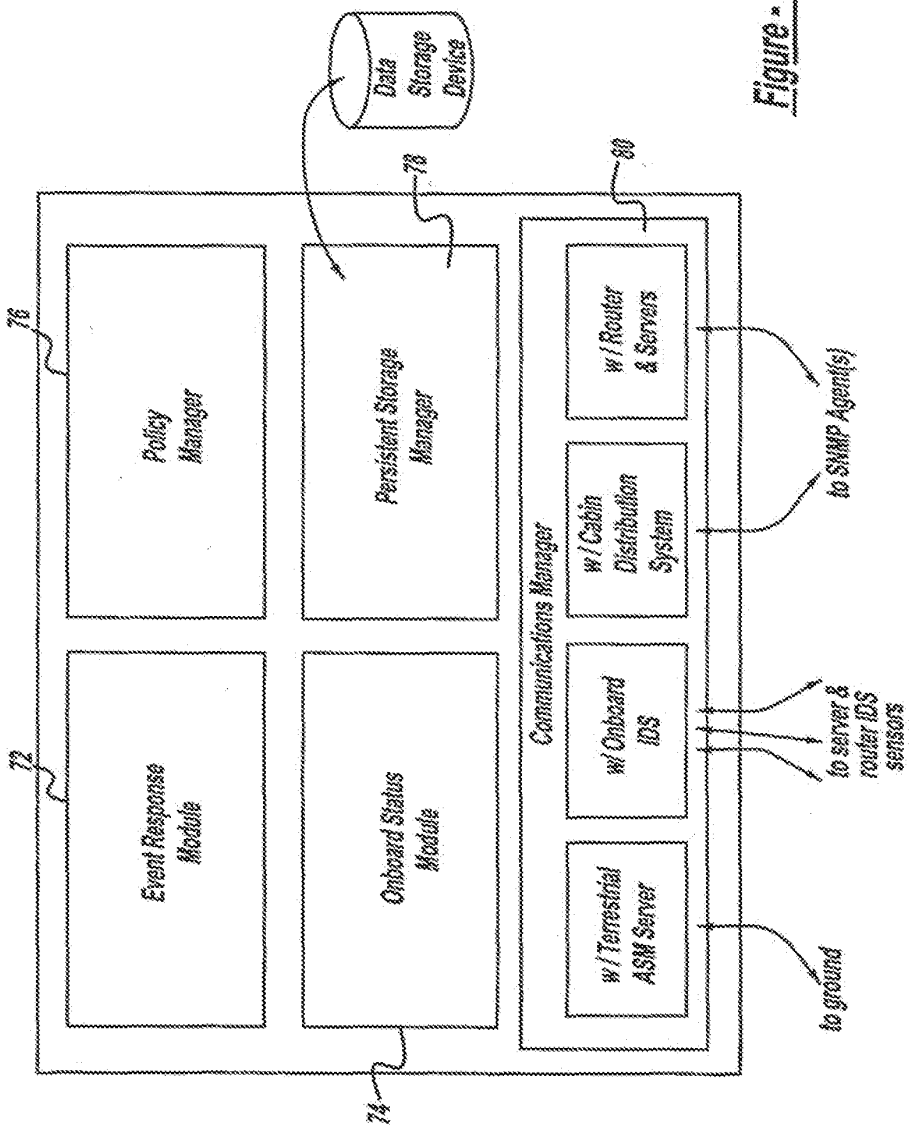

Data Storage Device
78
80
76
Policy Manager
Persistent Storage Manager
w/ Router & Servers
w/ Cabin Distribution System
to SNMP Agent(s)
Communications Manager
72
Event Response Module
Onboard Status Module
w/ Onboard IDS
to server & router IDS sensors
w/ Terrestrial ASM Server
to ground
74

Figure - 5

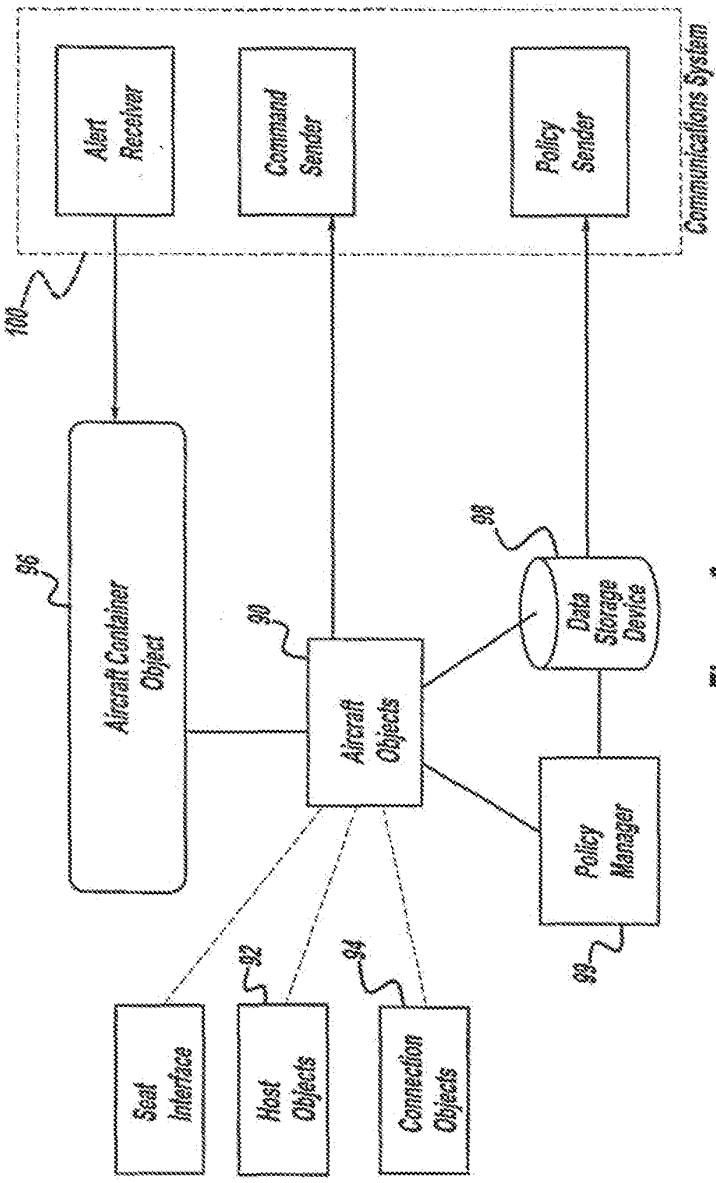

Communications System
Alert Receiver
Command Sender
Policy Sender
100
96
Aircraft Container Object
90
Aircraft Objects
98
Data Storage Device
Policy Manager
99
92
Host Objects
94
Connection Objects
Seat Interface

Figure - 6

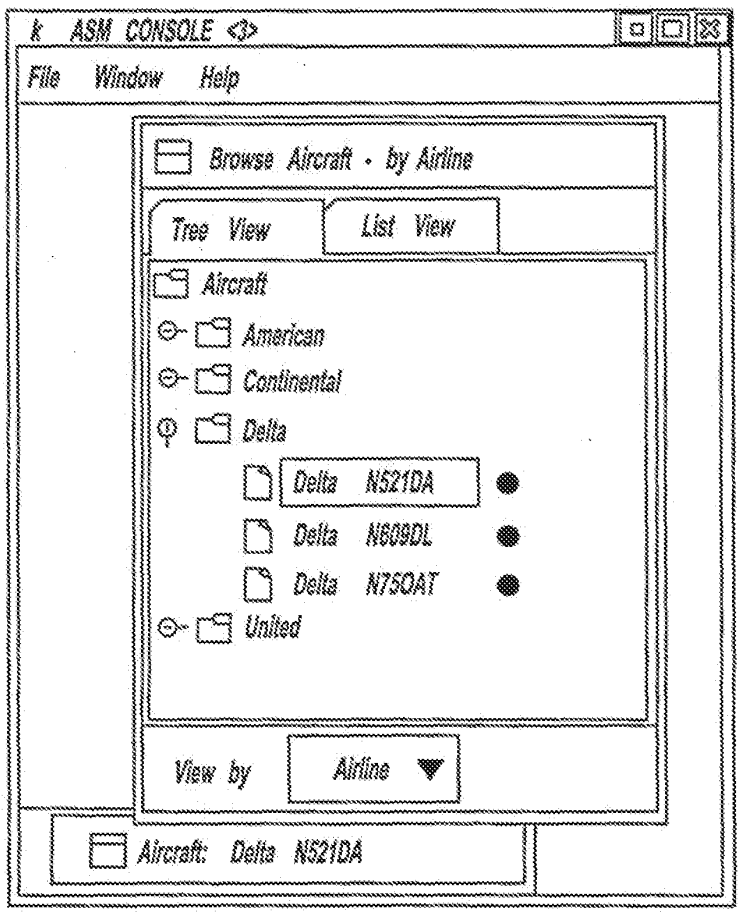

ASM CONSOLE <3>
File Window Help
Browse Aircraft - by Airline
Tree View
List View
Aircraft
American
Continental
Delta
Delta N521DA
Delta N608DL
Delta N750AT
United
View by
Airline
Aircraft: Delta N521DA

Figure - 7

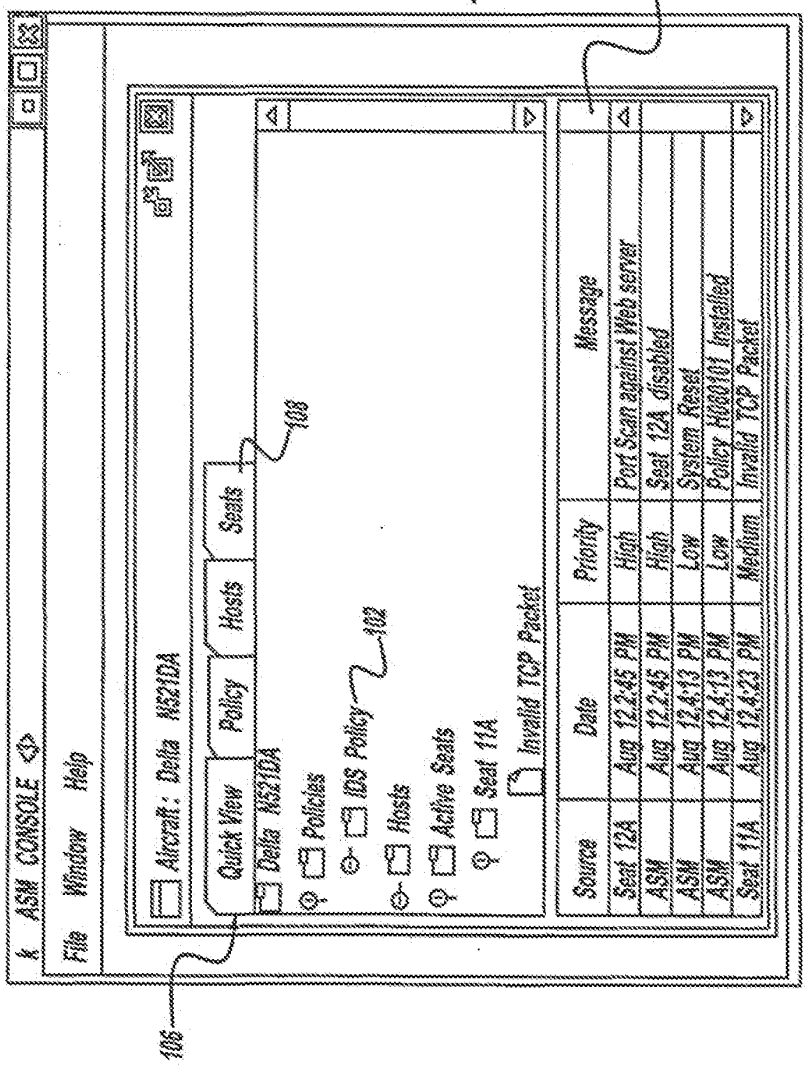

ASM CONSOLE
File Window Help
Aircraft: Delta N521DA
Quick View
Policy
Hosts
Seats
Delta N521DA
Policies
IDS Policy
Hosts
Active Seats
Seat 11A
Invalid TCP Packet
Source
Date
Priority
Message
Seat 12A
Aug 12:2:45 PM
High
Port Scan against Web server
ASM
Aug 12:2:45 PM
High
Seat 12A disabled
ASM
Aug 12:4:13 PM
Low
System Reset
ASM
Aug 12:4:13 PM
Low
Policy H000101 installed
Seat 11A
Aug 12:4:23 PM
Medium
Invalid TCP Packet
106
102
108
104

Figure - 8

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
27 September 2007 (27.09.2007)

(10) International Publication Number
WO 2007/107701 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/GB2007/000859

(22) International Filing Date: 12 March 2007 (12.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
06251528.3 22 March 2006 (22.03.2006) EP

(71) Applicant *(for all designated States except US)*: **BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY** [GB/GB]; 81 Newgate Street, London Greater London EC1A 7AJ (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **COFTA, Piotr Leon** [PL/GB]; 32 Bugsby Way, Kesgrave, Ipswich Suffolk IP5 2WX (GB).

(74) Agent: **WILLIAMSON, Simeon Paul**; BT GROUP LEGAL INTELLECTUAL PROPERTY DEPARTMENT, PPC5A, BT Centre, 81 Newgate Street, London Greater London EC1A 7AJ (GB).

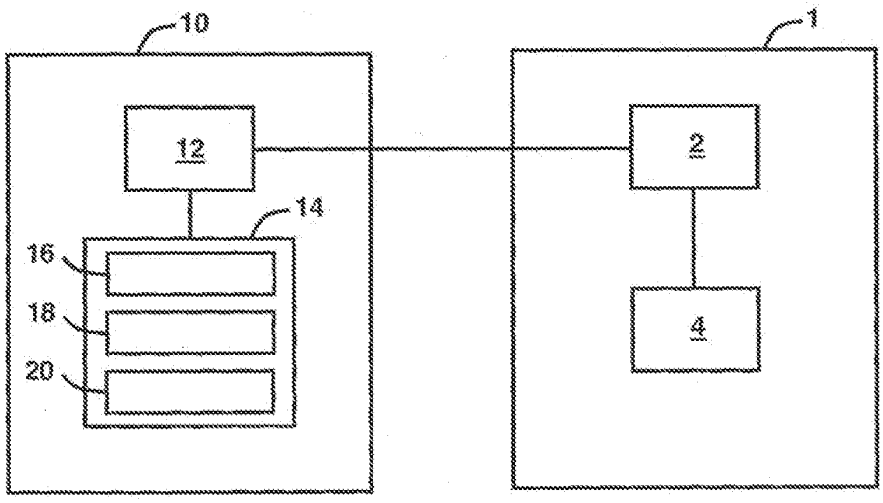
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, ME, 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, MT, 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: COMMUNICATIONS DEVICE MONITORING



(57) Abstract: A method, and devices, for a first communications device (10), e.g. a Subscriber Identity Module (SIM) to monitor a second communications device, e.g. a mobile telephone (1). The method comprises: the SIM (10) sending a program (16) stored at the SIM (10) to the mobile telephone (1); the mobile telephone (1) running the program (16) to provide one or more outcomes; the mobile telephone (1) sending the one or more outcomes to the SIM (10); the SIM (10) comparing the one or more outcomes to one or more correct outcomes (18) stored at the SIM (10); and the SIM (10) evaluating the result of the comparison according to one or more policies (20) stored at the SIM (10).

WO 2007/107701 A2

COMMUNICATIONS DEVICE MONITORING

The present invention relates to monitoring a communications device to verify, determine or otherwise assess the behaviour, condition or integrity of the communications device. The present invention relates in particular, but not exclusively, to monitoring a mobile communications device having a Subscriber Identity Module (SIM) located in the mobile communications device.

In the field of communications devices conventional approaches are provided for a first communications device to monitor a second communications device, in particular so that the first communications device can verify, determine or otherwise assess the behaviour, condition or integrity of the second communications device.

In some conventional approaches, the first communications device observes external signs of activity of the second communications device. In other conventional approaches, the first communications device engages in a pre-defined communications interaction with the second communications device to verify whether the second communications device performs correctly with respect to the interaction. For example, the first communications device may open an Internet connection at set time intervals to determine whether the second communications device is able to accept the Internet connection.

A common type of communication device, the mobile telephone, is becoming increasingly susceptible to outside influences on its integrity, due to increasing use of mobile telephones for data and software download, Internet connection, and so on. For example, mobile telephones are increasingly likely to be subject to malicious influences such as viruses and worms.

US20050033987 describes a mobile terminal that can carry out an integrity check on itself based on a trusted platform concept, for example the Trusted Computing Platform (TCP), using integrity metrics. Data is stored, for example on a SIM in the mobile terminal.

US20040243801 describes a system in which a mobile telephone can perform a self-check, using integrity metrics, in response to a request for verification.

In a first aspect, the present invention provides a method for a first communications device to monitor a second communications device, the method comprising: the first communications device sending a program stored at the first communications device to the second communications device; the second communications device running the program to provide one or more outcomes; the second communications device sending the one or more outcomes to the first communications device; the first communications device comparing the one or more outcomes to one or more correct outcomes stored at the first communications device; and the first communications device evaluating the result of the comparison according to one or more policies stored at the first communications device.

The first communications device may be located in the second communications device.

The first communications device may be a smart card and the second communications device may comprise means for coupling with the smart card.

The first communications device comprises cellular communications system Subscriber Identity Module, SIM, functionality and the second communications device is a mobile communications device that uses the SIM functionality of the first communications device.

The first communications device may not have a capability to run the program.

The first communications device may select the program to send to the second communications device from among a plurality of programs stored at the first communications device.

The first communications device may select randomly or pseudo-randomly the program to send to the second communications device from among a plurality of programs stored at the first communications device.

The method may be such that as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, the first communications device ceases co-operating with the second communications device. Ceasing co-operating may comprise declining to provide cellular communications system authorisation.

The method may be such that as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, the first communications device contacts a network operator of the cellular communications system through the second communications device.

In a further aspect, the present invention provides a first communications device adapted to monitor a second communications device, the first communications device comprising: storage means, the storage means storing a program, correct outcomes of the program, and policies; means adapted to send the program to a second communications device; means adapted to receive one or more outcomes of running the program from the second communications device; means adapted to compare the received one or more outcomes to corresponding correct outcomes of the stored correct outcomes; and means adapted to evaluate the result of the comparison according to one or more of the stored policies.

The first communications device may be adapted to be located in the second communications device.

The first communications device may be a smart card.

The first communications device may comprises cellular communications system Subscriber Identity Module, SIM, functionality.

The first communications device may not have a capability to run the program.

The program may be one of a plurality of programs stored by the storage means; and the first communications device may further comprise means adapted to select the program from among the plurality of programs. The means adapted to select the program from among the plurality of programs may be adapted to perform the selection randomly or pseudo-randomly.

The first communications device may further comprise means for, as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, ceasing co-operating with the second communications device. Ceasing co-operating may comprise declining to provide cellular communications system authorisation.

The first communications device may further comprise means for, as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, contacting a network operator of the cellular communications system through the second communications device.

In a further aspect, the present invention provides a second communications device adapted to be monitored by a first communications device, the second communications device comprising: means adapted to receive a program from a first communications device; means adapted to run the program to provide one or more outcomes; and means adapted to send the one or more outcomes to the first communications device.

The second communications device may further comprise means for locating the first communications device in the second communications device.

The first communications device is a smart card.

The second communications device may be a mobile communications device adapted to use cellular communications system Subscriber Identity Module, SIM, functionality of the first communications device.

In further aspects, the present invention provides a storage medium storing processor-implementable instructions for controlling one or more processors to carry out the method or implement the devices of any of the above aspects.

Thus the present invention provides an active monitoring process in which integrity metrics are not required to be measured.

In certain aspects, the present invention provides an active monitoring process for a mobile device, for example a mobile telephone, by using a SIM, or a card or other module comprising SIM functionality, located in the mobile device, as the monitoring device in the active monitoring process. This advantageously makes use of the SIM's typically greater resistance to outside influences compared to that of the mobile device.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram showing certain functional modules of a mobile device in which a first embodiment of the present invention is implemented;

Figure 2 is a block diagram showing certain functional modules of the mobile device of Figure 1 and certain functional modules of SIM located in the mobile device; and

Figure 3 is a process flowchart showing certain steps carried out by the SIM and the mobile device in an embodiment of a monitoring process.

Figure 1 is a block diagram showing certain functional modules of a mobile device 1 in which a first embodiment of the present invention is implemented. In this embodiment the mobile device 1 is a mobile telephone 1. The mobile telephone 1 comprises a processor 2, hereinafter referred to as the telephone processor 2, and the following modules, each of which are coupled to the processor 2: a radio input/output module 3, a storage medium 4, a user interface 5, a display 6, a loudspeaker 7 and a microphone 8. The storage medium 4 of the mobile telephone 1 is hereinafter referred to

as the telephone storage medium 4. The radio input/output module 3 is further coupled to an antenna 9.

A SIM 10 is shown located in the mobile telephone 1. The SIM 10 is coupled to the telephone processor 2 of the mobile telephone 1. When located in the mobile telephone 1, the SIM 10 is often considered as, or described as, being part of the mobile telephone 1. However, the present embodiment is most readily described by considering the SIM 10 as a separate communications device to the mobile telephone 1. In the present embodiment, the mobile telephone 1 and the SIM 10 operate according to the UMTS specification (Universal Mobile Telecommunication System), as specified in ETSI (European Telecommunications Standards Institute) specifications TS102.221, TS131.101, TS131.102 and other related specifications, except where described otherwise below.

In operation, the mobile telephone 1, under control of the telephone processor 2, and where appropriate using instructions and/or data stored in the telephone storage medium 4, carries out conventional mobile telephone operation according to the UMTS specification, as described in the following overview. Wireless signals are sent to, and received from, base stations of a cellular communications system using the antenna 8, with modulation and demodulation being performed by the radio input/output module 3. The user interface 5, comprising a keyboard and other touch devices enables a user to input instructions and data. The display 6 displays information, such as telephone numbers, network details, images and so on to the user. The loudspeaker 7 and the microphone 8 enable the user to respectively input and hear audio information, e.g. speech during a telephone call. The SIM 10 provides data and cellular communications network connectivity functionality to the mobile telephone 1. This allows the mobile telephone 1 to send and receive short message service (SMS) messages including multi-media messages, partake in telephone calls, access the Internet, download data and software, and so on.

It will be appreciated that the mobile telephone 1 comprises many other conventional components and functions in addition to the functional modules described above. It will also be appreciated that the functional modules described above may exhibit many other conventional functions and details. However, further explanation of any of these additional conventional components, functions and details is not necessary for understanding the present invention, and moreover they are readily implemented by the skilled person.

Figure 2 is a block diagram showing certain of the above described functional modules of the mobile telephone 1 and certain functional modules of the SIM 10. In particular, Figure 2 shows the telephone processor 2 and the telephone storage medium 4 of the mobile telephone 1. As shown in Figure 2, the SIM 10 comprises a processor 12, hereinafter referred to as the SIM processor 12. The SIM processor 12 is coupled to the telephone processor 2. The SIM 12 further comprises a storage medium 14, hereinafter referred to as the SIM storage medium 14. The SIM storage medium 14 is coupled to the SIM processor 12. Operation of the SIM 10 is controlled by the SIM processor 12 in conventional fashion, where appropriate using conventional algorithms, instructions and data (not shown in Figure 2) stored in the SIM storage medium 14.

In this embodiment the SIM storage medium 14 comprises, in addition to the above mentioned conventional algorithms, instructions and data, further algorithms, instructions and data for use in a process of monitoring the mobile telephone 2, which process will be described in more detail below with reference to Figure 3. As shown in Figure 2, the further algorithms, instructions and data for use in the monitoring process comprise test programs 16, correct outcomes 18, and policies 20. In this embodiment the test programs 16 are provided using the SIM Application Toolkit. In particular, proactive commands in the SIM Application Toolkit are used to make the communication between the SIM and the mobile telephone two-way by virtue of the mobile telephone polling the SIM. Further details of the test programs 16, correct outcomes 18, and policies 20 will be described in more detail below.

Figure 3 is a process flowchart showing certain steps carried out by the SIM 10 and the mobile telephone 1 in this embodiment of a monitoring process. At the top of the flowchart, the reference numeral 10 indicates those steps carried out by the SIM 10, and the reference numeral 1indicates those steps carried out by the mobile telephone 1.

At step s2, the SIM 10, more particularly the SIM processor 12, selects one of the test programs 16.

At step s4, the SIM 10 sends the selected test program 16 to the mobile telephone 1.

At step s6, the mobile telephone 1 receives the test program, and under control of the telephone processor 2 stores the test program 16 in the telephone storage medium 4.

At step s8, the SIM 10, more particularly the SIM processor 12, requests the program 16 to be run, by sending a request message to the mobile telephone 1.

A step s10, the mobile telephone 1, more particularly the telephone processor 2, executes the program stored in the telephone storage medium 4.

Meanwhile, at step s12, the SIM 10 awaits the outcomes of the test program 16 being run by the mobile telephone 1.

At step s14, the outcomes of the test program are sent by the mobile telephone 1 to the SIM 10. In this embodiment the outcomes are sent according to instructions contained in the test program 16 itself. This has an advantage that any corrupted program in the mobile telephone need not be involved in the process. Nevertheless, this is not essential, and in other embodiments, the mobile telephone 2 can be pre-programmed with instructions to send any outcomes from test programs to the source of the testing program, i.e. in this case the SIM 10.

At step s16, the SIM 10, more particularly the SIM processor 12, compares the received outcomes with the correct outcomes 18 stored in the SIM storage medium 14.

At step s18, the SIM 10, more particularly the SIM processor 12, determines a decision for the received outcomes, when compared with the correct outcomes 18, according to the policies 20 stored in the SIM storage medium 14. In this embodiment, the policies 20 simply specify that if the comparison step s16 indicates that the received outcomes are the same as the correct outcomes 18 then the SIM 10 continues to co-operate with the mobile telephone 1, whereas if the comparison step s16 indicates that any of the receive outcomes are different to the correct outcomes 18 then the SIM 10 stops co-operating with the mobile telephone 1. Many other policies 20 may be implemented, and other such possibilities will be discussed later below.

At step s20, the SIM 10 implements the decision determined at step s18. Hence, in this embodiment, at step s20, SIM 10 continues to co-operate with the mobile telephone 1 if the received outcomes were the same as the stored correct outcomes 18, whereas SIM 10 stops co-operating with the mobile telephone 1 if the received outcomes were different to the stored correct outcomes 18.

A time out option may be provided such that if the mobile telephone 1 does not return any outcomes within a given time from being instructed to run the test program, then this is in itself considered as a received outcome by the SIM 10, and this outcome is accorded a policy.

It should be noted that certain of the process steps depicted in the flowchart of Figure 3 and described above may be omitted or such process steps may be performed in differing order to that presented above and shown in Figure 3. Furthermore, although all the process steps have, for convenience and ease of understanding, been depicted as

discrete temporally-sequential steps, nevertheless some of the process steps may in fact be performed simultaneously or at least overlapping to some extent temporally. For example, steps s4 and s8 may be performed as one step, i.e. the SIM 10 may send the program to the device and the request to run the program at the same time. Another possibility is omission of the step of the SIM 10 requesting the program to be run, and instead the mobile telephone automatically executing any such received test program.

Thus a process is provided in which a program stored at the SIM 10 is executed by the mobile telephone 1, and the outcome of the program is returned to the SIM to evaluate. Thus a process is provided in which the relatively more secure SIM can effectively probe the status of the relatively less secure mobile telephone. Furthermore, because the test programs are stored at the SIM and not at the mobile telephone (except when due to be executed), any attacker of the mobile telephone cannot ascertain what programs any tampered version of the mobile telephone will need to be able to carry out to mask any changes made to the mobile telephone.

In the above embodiments, the SIM 10 and mobile telephone 1 operate according to the UMTS specification. In other embodiments, the SIM 10 and mobile telephone may instead, or in addition, operate according to other cellular communications specifications, for example Global System for Mobile Communications (GSM).

In the above embodiment the mobile communications device is a mobile telephone. In other embodiments other types of mobile device may be employed, for example a personal digital assistant or other device linked to a mobile radio receiver or module.

Indeed, in other embodiments, the communications device being monitored need not be a mobile device. For example, communications devices which although not portable nevertheless employ a SIM or other smart card, of the type described in the following paragraphs may be the device being monitored.

In the above embodiments, the element performing the monitoring of the mobile telephone is a conventional UMTS SIM adapted by programming using the SIM application toolkit. Also, dual SIM with more than one authentication means can be used. For example, dual SIM with more than one authentication means (for example with two SIM functionalities embedded on the same physical card) can be used. In other embodiments, the SIM functionality used in the above embodiments may be housed and delivered in physical forms other than a conventional SIM card. For example, the functionality may be provided on a Secure Digital (SD) card or a Multi Media Card (MMC). More generally, the device performing the monitoring may be any type of smart card, i.e. a

module comprising processing as well as memory, with the device being monitored being any communications device with means for coupling with the smart card. In each such embodiment, due to the physical location of the SIM or e.g. other smart card in the device being monitored, it can be typically assumed that a required level of trust between the monitoring device and the device being monitored is present. Nevertheless, as a further generalisation, in other embodiments coupling between the SIM or e.g. other smart card with the device being monitored may instead be provided remotely, for example over a Bluetooth wireless link or other local wireless link.

The test programs may be written in any suitable programming language, with the device being monitored being provided with processing means for executing programs in the chosen language. However, preferably the test programs are in a conveniently portable language such as Java. Mobile telephones meeting the UMTS specification typically comprise a Java capability therein. Therefore, such conventional mobile telephones may be simply adapted for use in the above embodiments by providing them with a Java-SIM connection. This may be provided consistent with the JCP (Java Community Process) specification of JSR177 (SATSA): Security and Trust which enables integration of these, and by incorporating a CLDC (Connected Limited Device Configuration) platform. The use of Java is beneficial as it guarantees high portability of the test program between different mobile telephones so that SIM does not have to keep different variants of the same test program for different telephones. Further, the use of SATSA enables the creation of complex test cases while the ability to sign the latest program provides additional security for the mobile device.

It will be appreciated that the test programs may be ones that can be stored in the SIM but are too complex to be have been executed in the SIM. For example, the SIM may have insufficient processing power, whereas the mobile communications device has more processing power and is able to execute the program. This advantageously allows a synergy to be achieved between the security of the SIM and the processing power of the device being monitored, i.e. the relative complexity of the test programs that may be employed.

The test programs may be of any desired complexity. Typically, for higher complexity programs there will be a greater chance of finding problems, whereas for lower complexity programs there will typically be a lower processing and storage burden. One example is, say, to instruct the device being monitored to add three specified memory values and send the sum as an outcome. Another example, say, is to instruct the device being monitored to measure a current and send the measured current value as the

outcome, where the current value is one that indicates that the display, e.g. display 6 in above described mobile telephone 1, is correctly functioning. Another example is the test program can require the device being monitored, e.g. a mobile telephone, to communicate in a specific way with the cellular communications network operator.

The choice of which stored test program to send to the device being monitored can be determined according to any desired criterion according to the requirements of the arrangement under consideration. For example, the test program may be chosen randomly or pseudo-randomly (this option in particular enforces the earlier described advantage of the test programs being stored at the SIM and not at the mobile telephone in relation to any attacker of the mobile telephone therefore not being able to ascertain what programs any tampered version of the mobile telephone will need to be able to carry out to mask any changes made to the mobile telephone). Another possibility is the test program may be selected by sequentially from a sequentially ordered list. For example, yet another possibility is the program may be selected from the stored programs according to some algorithm that takes account of previous outcomes.

In any of the above embodiments, the test programs sent from the SIM or corresponding card or device to the device being monitored may be digitally signed programs, and the device being monitored correspondingly programmed or otherwise set up to grant the necessary rights to the digitally signed programs.

In the above described embodiments, a plurality of test programs are stored at the SIM or corresponding device. However, in other simpler embodiments, only one test program is stored at the SIM and used in the monitoring process.

For the avoidance of doubt, it is noted that the term "program" as used in the above description encompasses similar terms used in the art, such as "application".

The policies described above may be of many different forms. A simple policy is, as described above, for the SIM or corresponding device to cease co-operating with the device being monitored if the outcomes received are not the same as the expected, i.e. correct outcomes. This may include refusing to carry out network authentication, e.g. UMTS or GSM authentication with the network operator. Other policies may be based on more complicated algorithms, for example a weighting or similar operation carried out to determine a significance of one or more differences between received outcomes and correct outcomes. The policies may be such that resulting actions may further include contacting the network operator to report a discrepancy. This may be over a secure communication link provided via the device being monitored, for example when the device being monitored is a mobile telephone, the secure communication link may comprise

sending an SMS message or call to the network operator. The policies may be hard-coded, or may updatable in some manner. For example, they may be altered by user input. Another possibility is that the network operator may use a secure communication through the device being monitored to communicate with the SIM. For example, the network operator may change settings in the SIM memory, thereby changing the selection of test programs, policies, correct outcomes and so on.

In the above embodiments, a plurality of policies are stored at the SIM. However, in simpler embodiments, only one policy is stored and used, e.g. a policy of ceasing co-operation with the device being monitored in the event of any received outcome not matching the corresponding stored correct outcome.

In the above embodiments, there a plurality of outcomes are provided when the test program is run. However, in simpler embodiments, there may be just one outcome when the test program is run.

In the above embodiments, the test programs are provided using the SIM Application Toolkit. In particular, proactive commands in the SIM Application Toolkit are used to make the communication between the SIM and the mobile telephone two-way by virtue of the mobile telephone polling the SIM. In other embodiments, other functionality may be added to a conventional SIM (or corresponding device or card) and/or the mobile telephone or other device being monitored such as to provide that the SIM may push the test programs to the mobile telephone and/or the mobile telephone may pull the test programs from the SIM. One such possibility is that a conventional smartphone (e.g. in a form of PDA or a handheld device) equipped with an open operating system such as Symbian or Windows Mobile as typically used in mobile telephones under UMTS or GSM, may be adapted as required.

More generally, the above embodiments may be implemented by providing new designs of communications device, e.g. mobile telephone and/or SIM card, or by configuring or adapting previous designs of device. The described functionality may be provided by hardware, firmware, software, or any combination of these For example existing processors/storage medium may be programmed (for example with data stored at the described storage medium) to provide the above described processes. As such the described processes may be implemented by a processor implementing processor-implementable instructions stored at the storage medium. The storage medium may be any suitable storage medium, such as computer memory, ROM, PROM etc. Any described processor may comprise plural processors.

CLAIMS

1. A method for a first communications device to monitor a second communications device, the method comprising:

the first communications device sending a program stored at the first communications device to the second communications device;

the second communications device running the program to provide one or more outcomes;

the second communications device sending the one or more outcomes to the first communications device;

the first communications device comparing the one or more outcomes to one or more correct outcomes stored at the first communications device; and

the first communications device evaluating the result of the comparison according to one or more policies stored at the first communications device.

2. A method according to claim 1 wherein the first communications device is located in the second communications device.

3. A method according to claim 1 or 2 wherein the first communications device is a smart card and the second communications device comprises means for coupling with the smart card.

4. A method according to any of claims 1, 2 or 3, wherein the first communications device comprises cellular communications system Subscriber Identity Module, SIM, functionality and the second communications device is a mobile communications device that uses the SIM functionality of the first communications device.

5. A method according to any of claims 1 to 4, wherein the first communications device does not have a capability to run the program.

6. A method according to any of claims 1 to 5, wherein the first communications device selects the program to send to the second communications device from among a plurality of programs stored at the first communications device.

7. A method according to claim 6, wherein the first communications device selects randomly or pseudo-randomly the program to send to the second communications device from among the plurality of programs stored at the first communications device.

8. A method according to any of claims 1 to 7, wherein as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, the first communications device ceases co-operating with the second communications device.

9. A method according to claim 8 when dependent on claim 4, wherein ceasing co-operating comprises declining to provide cellular communications system authorisation.

10. A method according to claim 4, 8 or 9, wherein as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, the first communications device contacts a network operator of the cellular communications system through the second communications device.

11. A first communications device adapted to monitor a second communications device, the first communications device comprising:

storage means, the storage means storing a program, correct outcomes of the program, and policies;

means adapted to send the program to a second communications device;

means adapted to receive one or more outcomes of running the program from the second communications device;

means adapted to compare the received one or more outcomes to corresponding correct outcomes of the stored correct outcomes; and

means adapted to evaluate the result of the comparison according to one or more of the stored policies.

12. A first communications device according to claim 11, wherein the first communications device is adapted to be located in the second communications device.

13. A first communications device according to claim 11 or 12, wherein the first communications device is a smart card.

14. A first communications device according to any of claims 11 to 13, wherein the first communications device further comprises cellular communications system Subscriber Identity Module, SIM, functionality.

15. A first communications device according to any of claims 11 to 14, wherein the first communications device does not have a capability to run the program.

16. A first communications device according to any of claims 11 to 15, wherein the program is one of a plurality of programs stored by the storage means; and the first communications device further comprises means adapted to select the program from among the plurality of programs.

17. A first communications device according to claim 16, wherein the means adapted to select the program from among the plurality of programs are adapted to perform the selection randomly or pseudo-randomly.

18. A first communications device according to any of claims 11 to 17, further comprising means for, as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, ceasing co-operating with the second communications device.

19. A first communications device according to claim 18 when dependent on claim 14, wherein ceasing co-operating comprises declining to provide cellular communications system authorisation.

20. A first communications device according to claim 14, 18 or 19, further comprising means for, as a result of the evaluating step, when one or more received outcomes is not the same as the correct outcomes, contacting a network operator of the cellular communications system through the second communications device.

21. A second communications device adapted to be monitored by a first communications device, the second communications device comprising:

means adapted to receive a program from a first communications device;

means adapted to run the program to provide one or more outcomes; and

means adapted to send the one or more outcomes to the first communications device.

22. A second communications device according to claim 21, further comprising means for locating the first communications device in the second communications device.

23. A second communications device according to claim 21 or 22, wherein the first communications device is a smart card.

24. A second communications device according to any of claims 21 to 23, wherein the second communications device is a mobile communications device adapted to use cellular communications system Subscriber Identity Module, SIM, functionality of the first communications device.

25. A storage medium storing processor-implementable instructions for controlling one or more processors to carry out the method of any of claims 1 to 10.

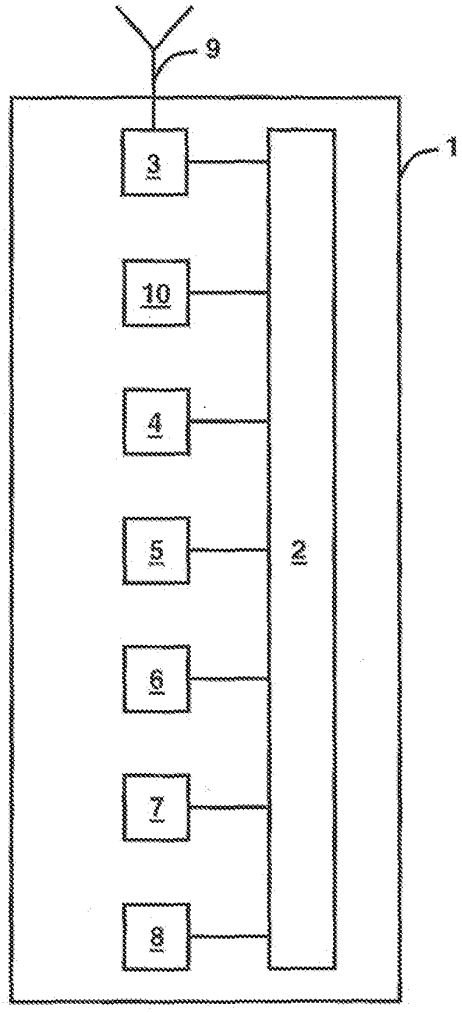


FIG. 1

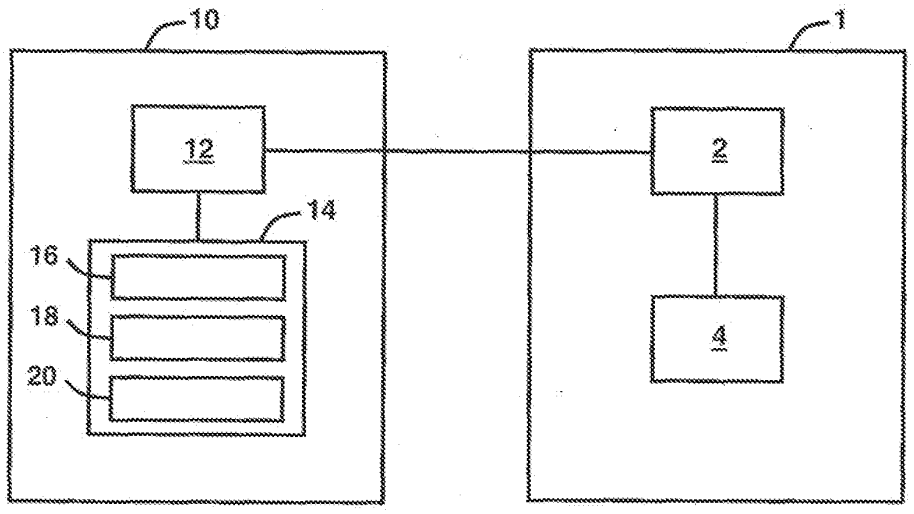


FIG. 2

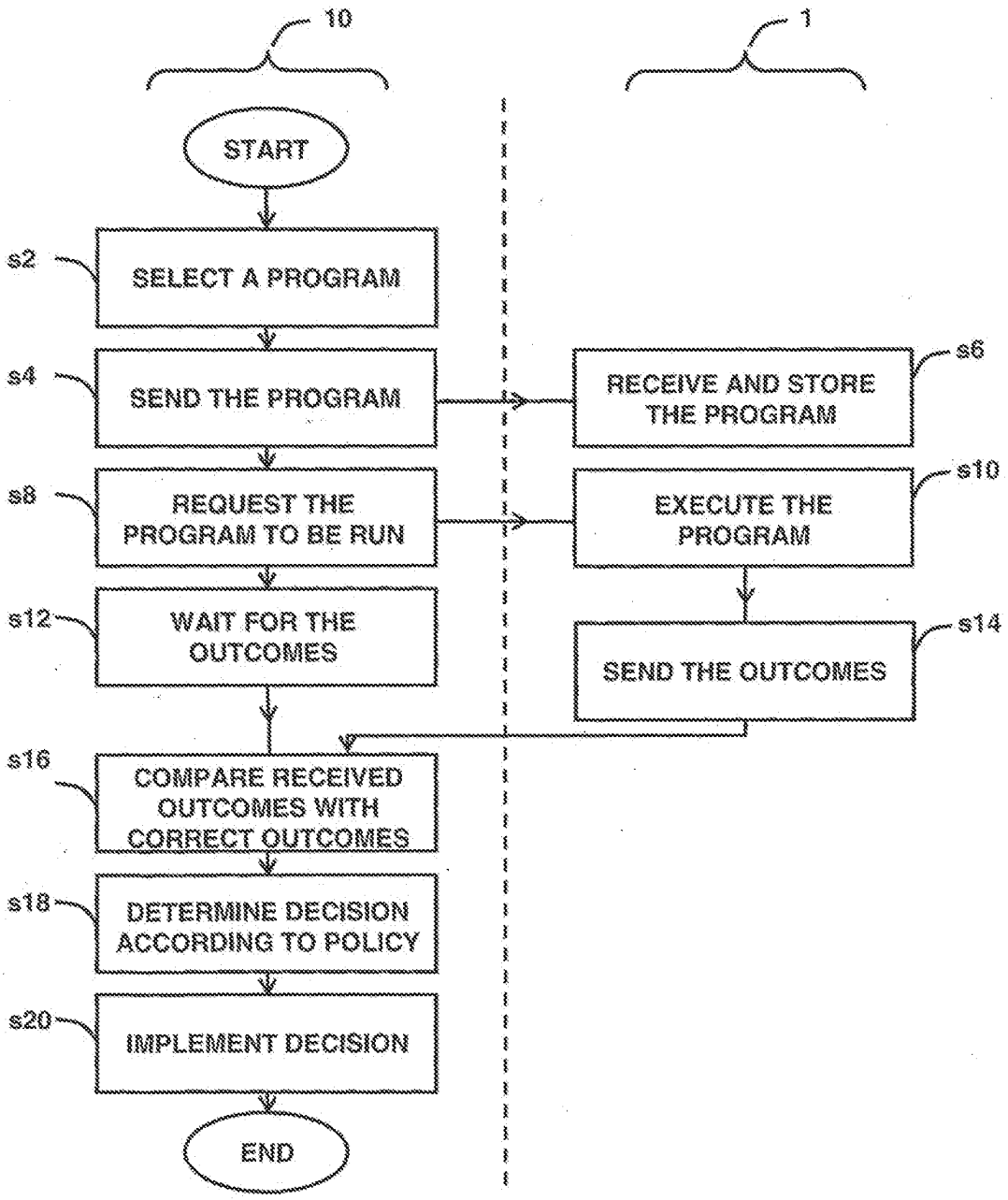

10
1
START
s2
SELECT A PROGRAM
s4
SEND THE PROGRAM
s6
RECEIVE AND STORE THE PROGRAM
s8
REQUEST THE PROGRAM TO BE RUN
s10
EXECUTE THE PROGRAM
s12
WAIT FOR THE OUTCOMES
s14
SEND THE OUTCOMES
s16
COMPARE RECEIVED OUTCOMES WITH CORRECT OUTCOMES
s18
DETERMINE DECISION ACCORDING TO POLICY
s20
IMPLEMENT DECISION
END

FIG. 3

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

(11) EP 1 463 238 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
29.09.2004 Bulletin 2004/40

(51) Int Cl.?: **H04L 12/24**, H04L 12/26

(21) Numéro de dépôt: **04290706.3**

(22) Date de dépôt: **15.03.2004**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Etats d'extension désignés:
AL HR LT LV MK

(30) Priorité: **28.03.2003 FR 0303835**

(71) Demandeur: **ALCATEL**
75008 Paris (FR)

(72) Inventeurs:
- **Marilly, Emmanuel**
  92160 Antony (FR)
- **Betge-Brezetz, Stéphane**
  75015 Paris (FR)
- **Martinot, Olivier**
  91210 Draveil (FR)
- **Chevanne, Michel**
  92140 Clamart (FR)
- **Delegue, Gérard**
  94230 Cachan (FR)

(74) Mandataire: **Chaffraix, Sylvain et al**
Compagnie Financière Alcatel
Département de Propriété Industrielle,
5, rue Noel Pons
92734 Nanterre Cedex (FR)

(54) Dispositif de gestion locale de procédés d'assurance pour un équipement de réseau de communications

(57) Un dispositif embarqué (D) est dédié à la gestion locale d'assurance pour un équipement de réseau (NE) d'un réseau de communications (N) équipé d'un système de gestion de réseau (NMS), ledit équipement (NE) présentant une configuration choisie et comportant des moyens (MM) de mesure de valeurs de paramètre (s) du réseau et une base d'informations de gestion (MIB) stockant des données de gestion représentatives des valeurs mesurées. Le dispositif (D) comprend des moyens de gestion (MAE) chargés d'adapter la configuration de l'équipement (NE) en fonction d'au moins les données de gestion stockées dans la base d'informations de gestion (MIB) et de règles, dites d'assurance, choisies.

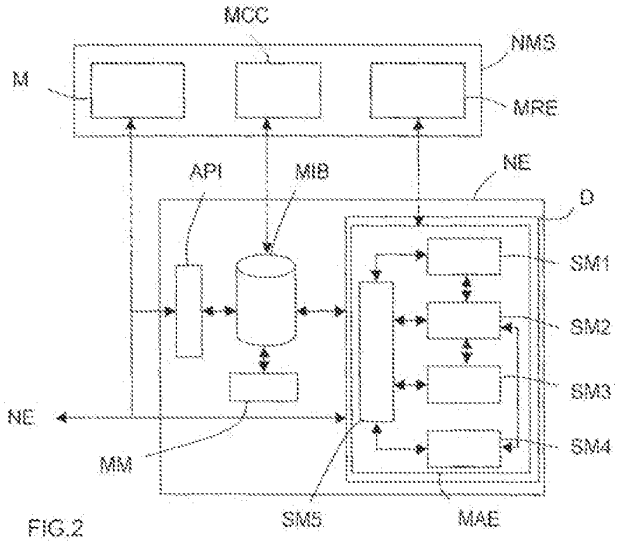


FIG.2

EP 1 463 238 A1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] L'invention concerne les réseaux de communications, et plus particulièrement ceux offrant une assurance de continuité de service(s).

[0002] De nombreux réseaux de communications mettent en oeuvre des procédés d'assurance qui contrôlent l'exécution d'activités de maintenance préventives et réactives destinées à assurer à leurs clients la continuité de la disponibilité de services, définis en termes de qualité de service (QoS). A cet effet, les réseaux disposent d'un système de gestion de réseau (ou NMS pour « Network Management System ») qui analyse continuellement l'état des ressources et les performances de manière à anticiper ou détecter des problèmes ou pannes et à déterminer les actions à entreprendre de sorte que les clients ne soient pas pénalisés.

[0003] Une telle analyse centralisée repose sur la collection d'un très grand nombre de données d'information et d'alarmes auprès des nombreux équipements de réseau, chargés d'effectuer des mesures de valeurs de paramètre(s) du réseau, et plus précisément auprès de leurs bases d'informations de gestion (ou MIB pour « Management Information Base ») chargées de stocker les données de gestion représentatives des valeurs mesurées. Une fois collectées, par exemple via un collecteur SNMP, les données sont stockées dans une base de données d'archivage, par exemple de type Oracle, et alimentent des modules de calcul qui mettent en oeuvre des formules ou équations prédéfinies.

[0004] Une telle solution est par exemple décrite dans l'article « *Real-Time Performance Monitoring and Anomaly Detection in the Internet: and Adaptative, Objective-Driven, Mix-and-Match Approach* » de L. Lawrence Ho, Christopher J. Macey and Ronald G. Hiller.

[0005] Un tel procédé d'assurance centralisé requiert l'emploi de bases de données de très grandes capacités, nécessite des temps de calcul importants et consomme de la bande passante (lors de la collecte), ce qui nuit aux performances du réseau.

[0006] Certaines tentatives ont été faites vers l'utilisation d'agents embarqués dans des éléments réseaux, mais les aspects décisionnels demeurent dans un organe centralisé et présentent les mêmes défauts que la solution précédente. De plus, ces tentatives ne concernent pas l'assurance.

[0007] Des exemples de telles tentatives peuvent être trouvées dans les brevets américains US 6 272 537 et US 6 085.

[0008] L'invention a donc pour but d'améliorer la situation.

[0009] Elle propose à cet effet un dispositif de gestion locale d'assurance pour un équipement de réseau de communications présentant une configuration choisie et comportant des moyens de mesure de valeurs de paramètre(s) du réseau et une base d'informations de gestion (MIB) stockant des données de gestion représentatives des valeurs mesurées.

[0010] Ce dispositif se caractérise par le fait qu'il comporte des moyens de gestion chargés d'adapter la configuration de l'équipement dans lequel il est implanté (ou embarqué) en fonction, notamment, des données de gestion stockées dans sa base d'informations de gestion et de règles, dites d'assurance, choisies, définissant une politique locale d'assurance.

[0011] En d'autres termes, l'invention consiste à intégrer dans des équipements (ou noeuds) du réseau un dispositif d'assurance embarqué de sorte qu'ils puissent assurer localement au moins une partie du procédé d'assurance géré par le NMS.

[0012] Le dispositif d'assurance embarqué, selon l'invention, pourra comporter des caractéristiques complémentaires qui pourront être prises séparément et/ou en combinaison, et en particulier :

- des moyens de gestion capables d'adapter la configuration de leur équipement en fonction de données d'informations provenant d'au moins un autre équipement de réseau,
- une adaptation consistant en une modification de la politique de mesure de paramètre(s) et/ou une modification de la politique d'envoi de rapport (ou « reporting ») au NMS,
- une adaptation consistant en une modification du mode de fonctionnement de l'équipement,
- des moyens de gestion comprenant des moyens d'analyse de paramètres du réseau capables de délivrer des données d'information représentatives de l'évolution temporelle, sur un intervalle choisi, de certaines valeurs de paramètre(s) du réseau (comme par exemple le trafic ou l'état d'un routeur) qui sont stockées dans la MIB. Dans ce cas, les moyens d'analyse peuvent être agencés de manière à délivrer des données d'information représentatives d'une analyse de tendance et/ou d'une analyse de profils ou de signatures (ou « baselines ») et/ou d'une analyse de discontinuité et/ou d'une agrégation de valeurs de paramètres du réseau. Par ailleurs, ces moyens d'analyse peuvent être configurables, notamment dans le but de mettre en oeuvre de nouveaux calculs, relatifs aux paramètres du réseau, transmis par le NMS,
- des moyens de gestion comprenant des moyens d'alarme chargés de déclencher l'envoi d'une alarme et/ou de données d'information au NMS et/ou à au moins un autre équipement de réseau, en fonction de règles d'assurance choisies. De telles données d'information et alarmes sont par exemple représentatives de résultat(s) d'analyse(s) ou d'agrégation(s) de données effectuée(s) par les moyens d'analyse et/ou de valeur(s) de paramètre(s) du réseau stockées dans la MIB. Par ailleurs, les moyens d'alarme peuvent être configurables,
- des moyens de gestion comprenant des moyens d'observation du réseau définissant un agent de mesure de flux de type « bout-en-bout » (ou « end-

to-end »), et délivrant des données d'informations. Dans ce cas, les moyens d'observation du réseau peuvent être configurables,

- des moyens de gestion comprenant des moyens de gestion d'accords de niveau de service (ou SLA pour « Service Level Agreement ») délivrant des données d'informations. Dans ce cas, les moyens de gestion d'accords de niveau de service peuvent être configurables,
- des moyens de gestion capables d'effectuer des tests, par exemple de mesure(s) active(s) ou d'aide au diagnostic. Ces tests peuvent notamment permettre de faire remonter une information agrégée ou le résultat du test (par exemple le temps pris pour une opération de type TCP) au niveau de la couche NMS,
- des moyens de gestion capables d'assurer leur gestion en fonction d'un calendrier, de sorte que certaines (ou toutes les) fonctions d'assurance ou tests ne soient effectuées que certains jours de la semaine ou du mois ou à certaines heures, par exemple,
- des moyens de gestion comprenant des moyens de contrôle chargés de gérer le fonctionnement (et notamment la configuration) des moyens d'analyse, des moyens d'alarme, des moyens d'observation du réseau et des moyens de gestion d'accords de niveau de service, en fonction des règles d'assurance choisies et des données d'informations qu'ils délivrent. De tels moyens de contrôle peuvent se présenter sous la forme d'un moteur de règles (ou « rule engine ») dans lequel sont stockées les règles d'assurance choisies. Par ailleurs, ces moyens de contrôle peuvent être configurables,
- des moyens de gestion configurables,
- des moyens de gestion et/ou des moyens d'analyse et/ou des moyens et/ou des moyens de contrôle et/ou des moyens d'observation du réseau et/ou des moyens de gestion d'accords de niveau de service agencés de manière à pouvoir être configurés par le NMS via une interface de langage de programmation (ou API pour « Application Programming Interface ») et éventuellement via la MIB. Dans ce cas, la MIB peut être configurée ou programmée par le NMS via l'API,
- des moyens de gestion et/ou des moyens d'analyse et/ou des moyens d'alarme et/ou des moyens d'observation du réseau et/ou des moyens de gestion d'accords de niveau de service et/ou des moyens de contrôle agencés de manière à pouvoir être configurés par le NMS via des commandes dédiées, telles que des « Command Line Interface » (ou CLI).

[0013] L'invention concerne également un équipement de réseau muni d'un dispositif du type de celui présenté ci-avant. L'invention convient plus particulièrement, bien que de façon non restrictive, aux équipements de réseau tels que les routeurs, les commutateurs (ou « switchs ») et les pare-feux (ou « firewalls »).

[0014] L'invention propose également un réseau de communications équipé d'un système de gestion de réseau (NMS) et d'une multiplicité d'équipements de réseau du type de celui présenté ci-avant. Dans un mode de réalisation de type distribué, chaque équipement de réseau peut être agencé de manière à délivrer au système de gestion de réseau des alarmes et/ou des données d'information de types différents.

[0015] L'invention peut notamment être mise en oeuvre dans toutes les technologies réseaux qui doivent être gérées, et notamment dans les réseaux de transmission (par exemple de type WDM, SONET, SDH), de données (par exemple de type Internet-IP ou ATM) ou de voix (par exemple de type classique, mobile ou NGN).

[0016] D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels :

- la figure 1 illustre de façon schématique un réseau de communications comprenant un système de gestion de réseau (NMS) et des équipements de réseau selon l'invention, et
- la figure 2 illustre de façon schématique un exemple de réalisation d'un équipement de réseau selon l'invention.

[0017] Les dessins annexés pourront non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

[0018] L'invention a pour objet de permettre la gestion locale, par des équipements de réseau, d'une partie du procédé d'assurance géré par le système de gestion de réseau (ou NMS pour « Network Management System ») d'un réseau de communications.

[0019] Comme cela est illustré sur la figure 1, un réseau de communications N comporte schématiquement une multiplicité d'équipements de réseau NEi (ici i = 1, 2, mais il peut prendre n'importe quelle valeur), comme par exemple des serveurs équipés d'un pare-feu ou (« firewall »), des commutateurs (ou « switchs »), des routeurs périphériques (ou « edge routers ») ou des routeurs de coeur (ou « core routers »), pouvant échanger des données, selon un protocole de gestion de réseau, avec un système de gestion de réseau, et notamment avec son serveur de gestion NMS.

[0020] Chaque équipement NEi comporte classiquement une base d'informations de gestion MIB (« Management Information Base »), également appelée base d'instances d'objets. Chaque MIB stocke des données de gestion représentatives de valeurs de champs d'information qui caractérisent l'équipement NEi associé. Certains de ces champs d'information désignent des paramètres du réseau dont les valeurs instantanées sont mesurées par des sondes MM implantées dans, ou gérées par, l'équipement NEi. Par ailleurs,

chaque MIB est associée à une définition de base d'informations de gestion (non représentée), également appelée définition de MIB, stockée dans le système de gestion de réseau et accessible au serveur de gestion NMS.

[0021] Dans ce qui suit, on considère à titre d'exemple non limitatif que le réseau de communications N est de type Internet (IP) et que le protocole de gestion du réseau est le protocole SNMP (pour « Simple Network Management Protocol » RFC 2571-2580). Bien entendu, l'invention s'applique à d'autres types de réseau, comme par exemple aux réseaux de transmission de type WDM, SONET ou SDH, de données de type ATM, ou de voix de type classique, mobile ou NGN, et à d'autres protocoles de gestion de réseau, comme par exemple TL1, CORBA ou CMISE/CMIP.

[0022] Par ailleurs, on considère dans ce qui suit que les équipements de réseau NEi sont des routeurs périphériques (ou de bordure) agissant en tant qu'agents d'observation de flux de type « bout-en-bout » (ou « end-to-end »). Ces routeurs sont généralement placés aux frontières du réseau et permettent l'établissement de liens avec d'autres réseaux. Ces agents sont généralement destinés à effectuer des mesures de bout en bout pour des problèmes d'échelle (ou « scalability »). Mais, bien entendu, l'invention n'est pas limitée à ce seul type d'équipement de réseau. Elle concerne tous les équipements de réseau capables d'échanger des données de gestion avec le NMS, et notamment les routeurs périphériques qui n'agissent pas en tant qu'observateurs, les routeurs de coeur, les commutateurs et les pare-feux.

[0023] Chaque équipement de réseau NEi est généralement configuré spécifiquement de manière à transmettre au NMS (ou couche NMS) des données d'information représentatives de mesures qu'il a effectuées avec sa ou ses sondes MM et qu'il a stockées dans sa MIB, ainsi que des alarmes signalant des problèmes ou des pannes. La configuration est généralement définie par une ou plusieurs politiques. Par exemple, une première politique est relative aux conditions d'envoi (ou « reporting ») de valeurs mesurées par l'équipement NEi à l'aide de ses sondes MM. Une deuxième politique peut concerner la ou les mesures de paramètre(s) que l'équipement NEi doit effectuer avec sa ou ses sondes MM. Une troisième politique peut concerner le mode de fonctionnement de l'équipement NEi. Ces politiques sont habituellement définies pour chaque équipement NEi par un module de configuration MC du NMS. Elles sont transmises aux équipements NEi, via le réseau N, à l'aide du protocole de gestion (ici SNMP).

[0024] Mais, le NMS, et notamment son module de collection MCC (ou « collector »), peut également, lorsqu'il l'estime nécessaire, adresser à un équipement de réseau NEi des requêtes pour qu'il lui transmette les valeurs de certains des champs d'information qui sont stockés dans sa MIB. C'est ce que l'homme de l'art appelle, en anglais, le « polling ».

[0025] Comme cela est mieux illustré sur la figure 2, l'invention propose un dispositif de gestion locale d'assurance D destiné à être soit implanté (ou embarqué) dans un équipement NEi, soit intégré dans un boîtier externe raccordé directement à un équipement NEi. Dans ce qui suit, on considère que le dispositif D est embarqué dans un équipement NEi.

[0026] Ce dispositif D selon l'invention comporte un module d'assurance MAE (ou module de gestion locale d'assurance) chargé d'adapter la configuration de l'équipement NEi, dans lequel il est embarqué, en fonction de règles, dites d'assurance, choisies, des données de gestion stockées dans sa MIB, et d'éventuelles données d'information qu'il reçoit des autres équipements de réseau.

[0027] On entend ici par « adapter », le fait de modifier une politique de mesure de paramètre(s) (voire mettre en place une nouvelle politique de mesure(s) ou reconfigurer la politique de mesure(s)) et/ou une politique d'envoi de rapport (ou « reporting ») au NMS et/ou le mode de fonctionnement de l'équipement NEi, initialement défini(s) par le module de configuration MC du NMS.

[0028] Par ailleurs, on entend par « règles d'assurance », des règles définissant la politique d'assurance locale de l'équipement compte tenu des valeurs prises par certains paramètres du réseau, stockées dans sa MIB, ou d'événements extérieurs, tels qu'une action de la couche NMS ou d'un autre routeur.

[0029] Le module d'assurance embarqué MAE permet ainsi d'embarquer dans un équipement NEi certaines fonctions d'assurance de manière à le rendre « plus intelligent », à limiter le nombre d'informations qui transitent dans le réseau, et éventuellement à permettre sa reconfiguration partielle, en fonction de règles d'assurance.

[0030] Afin de gérer localement la politique d'assurance, le module d'assurance MAE comporte préférentiellement un premier sous-module SM1 chargé d'appliquer un ou plusieurs traitements aux valeurs de certains champs d'information stockés dans la MIB. Plus précisément, ces traitements consistent à appliquer aux valeurs des champs d'information choisis, en fonction de règles d'assurance dédiées, des formules ou des équations, définies par le module de configuration MC du NMS, afin de délivrer des données d'information.

[0031] Par exemple, le premier sous-module SM1 est chargé d'effectuer des analyses de tendance sur un intervalle choisi (ou suivant un calendrier prédéfini), utiles aux anticipations de problèmes ou de pannes. Il peut notamment signaler que le pourcentage d'utilisation d'un CPU d'un routeur va atteindre un seuil critique dans une heure, ou que la bande passante d'un LSP va dépasser le seuil choisi dans deux heures.

[0032] Il peut être également chargé d'effectuer des analyses de profils ou de signatures (ou « baselines »). Cela est notamment utile lorsque l'on cherche, par exemple, à reconnaître ou identifier un profil caractéris-

tique d'utilisation, tel qu'une attaque spécifique d'un routeur, ou un mode de facturation (ou « billing »).

[0033] Il peut être également chargé d'effectuer des analyses de discontinuité de flux ou de trafic. Par exemple, en cas de surcharge d'un réseau, des paquets sont supprimés (ou « dropped »), si bien que la détection d'une discontinuité sur le paramètre de suppression (de 0 à x) permet d'informer que l'on a effectivement des paquets supprimés.

[0034] Il peut encore être chargé d'effectuer des agrégations de valeurs de paramètres du réseau, par exemple pour appliquer des formules du module de collection de données MCC dans le routeur ou pour calculer une moyenne sur une période donnée (par exemple la bande passante moyenne utilisée au cours de la dernière semaine). Dans ce cas, les valeurs agrégées peuvent être stockées dans la MIB et en être extraites sur requête de polling issue du module de collection MCC du NMS.

[0035] A titre d'exemple illustratif, le premier sous-module SM1 peut être chargé d'estimer l'évolution prévisionnelle (ou tendance) du nombre de paquets abandonnés (« dropped »), ainsi que l'évolution prévisionnelle de la bande passante utilisée et/ou de la charge de calcul (CPU) de l'équipement NEi. Il peut être également agencé pour effectuer des tests, par exemple de mesure(s) active(s) ou d'aide au diagnostic. Ces tests peuvent notamment permettre de faire remonter une information agrégée ou le résultat du test (par exemple le temps pris pour une opération de type TCP) au niveau de la couche NMS.

[0036] Préférentiellement, le premier sous-module SM1 délivre des données d'informations représentatives du résultat de ses analyses (ou estimations) à un (cinquième) sous-module de gestion (SM5), qui décide des actions à entreprendre en fonction de la politique d'assurance locale de son équipement NEi.

[0037] Le module d'assurance MAE comporte également de préférence un deuxième sous-module SM2 chargé de déclencher l'envoi d'alarme(s) et/ou de données d'information (ou rapports) sur ordre du cinquième sous-module SM5, en fonction de règles d'assurance qui lui sont dédiées.

[0038] Mais, on peut également envisager que le premier sous-module SM1 alimente le deuxième sous-module SM2 en données d'information, de sorte qu'il leur applique certaines des règles d'assurance et décide soit de leur envoi, soit de l'émission d'une alarme, à destination du NMS, et plus précisément d'un module de réception d'évènements MRE, et/ou d'au moins un autre équipement de réseau.

[0039] Dans l'exemple illustré d'un routeur périphérique de type « bout-en-bout », le module d'assurance MAE comporte également de préférence un troisième sous-module SM3 chargé d'observer le réseau, et notamment le trafic de type « bout-en-bout », en fonction de règles d'assurance qui lui sont dédiées. Par exemple, on dispose d'une sonde embarquée, pour effectuer les mesures de bout-en-bout. Cette sonde embarquée est alors configurée de manière à déterminer le flux à étudier et les résultats des mesures alimentent des règles d'assurance dédiées. Par exemple, l'une de ces règles peut être : « si entre deux routeurs périphériques on mesure deux flux différents, alors on agrége la mesure des deux flux pour limiter le calcul ».

[0040] Dans ce cas, le troisième sous-module SM3 définit ce que l'homme de l'art appelle un agent de mesure de flux « bout-en-bout » (ou « end-to-end »).

[0041] Préférentiellement, le troisième sous-module SM3 délivre des données d'informations représentatives du résultat de ses observations (ou mesures) au (cinquième) sous-module de gestion (SM5), qui décide des actions à entreprendre en fonction de la politique d'assurance locale de son équipement NEi. Mais, on pourrait également envisager que le troisième sous-module SM3 alimente le deuxième sous-module SM2 en données d'informations, de sorte qu'il leur applique certaines des règles d'assurance et décide soit de leur envoi, soit de l'émission d'une alarme, à destination du NMS, et plus précisément d'un module de réception d'évènements MRE, et/ou d'au moins un autre équipement de réseau.

[0042] Par ailleurs, et comme illustré sur la figure 2, le module d'assurance MAE peut comporter un quatrième sous-module SM4 chargé de gérer localement certains accords de niveau de service (ou SLA pour « Service Level Agreement »), en fonction de règles d'assurance qui lui sont dédiées. Par exemple, le sous-module SM4 connait l'accord de niveau de service (SLA) d'un client, de sorte qu'il peut être chargé de vérifier si ce SLA est bien respecté, et générer une alarme (ou données d'informations) si ce n'est pas le cas (ou si la situation se dégrade).

[0043] Préférentiellement, le quatrième sous-module SM4 délivre des données d'informations représentatives de comptes-rendus de gestion au cinquième sous-module SM5, qui décide des actions à entreprendre en fonction de la politique d'assurance locale de son équipement NEi. Mais, on pourrait également envisager que le quatrième sous-module SM4 alimente le deuxième sous-module SM2 en données d'information, de sorte qu'il leur applique certaines des règles d'assurance et décide soit de leur envoi, soit de l'émission d'une alarme, à destination du NMS, et plus précisément d'un module de réception d'évènements MRE, et/ou d'au moins un autre équipement de réseau.

[0044] Comme indiqué plusieurs fois ci-avant, le module d'assurance MAE comporte un cinquième sous-module SM5 (ou module de contrôle) chargé de contrôler le fonctionnement des autres sous-modules (ici SM1 à SM4). Plus préférentiellement, ce cinquième sous-module SM5 se présente sous la forme d'un moteur de règles (ou « rule engine ») dans lequel sont stockées toutes les règles d'assurance dédiées aux autres sous-modules. Il s'agit par exemple d'un « Java expert System Shell ».

[0045] Alors que chaque sous-module SM1 à SM4 effectue des calculs et/ou des analyses et/ou des rapports définis à partir de règles d'assurance dédiées, le cinquième sous-module SM5 gère préférentiellement l'ensemble desdites règles d'assurance dédiées. Par « gérer l'ensemble des règles », on entend ici gérer les conditions et les actions définies par les différentes règles.

[0046] Le cinquième sous-module SM5 a plus précisément deux fonctions principales

[0047] Une première fonction consiste à ordonner au deuxième sous-module SM2 de générer une alarme, ou d'adresser un rapport, à destination de la couche NMS (ou d'un autre équipement du réseau), parce qu'en appliquant une règle d'assurance à des données délivrées par l'un des autres sous-modules SM1 à SM4, il s'est aperçu que la condition correspondante n'était pas satisfaite.

[0048] Par exemple, il ordonne la génération d'une alarme parce que les données d'analyse délivrées par le premier sous-module SM1 ne satisfont pas la condition qui leur est associée par la politique locale d'assurance, ou parce que le quatrième sous-module SM4 l'a averti qu'un SLA qu'il gérait localement n'était pas respecté.

[0049] Une seconde fonction consiste à décider de l'adaptation de la configuration de l'équipement NEi, et notamment du module d'assurance embarqué MAE, en fonction des données d'informations qu'il reçoit des autres sous-modules SM1 à SM4 et des règles d'assurance qui définissent la politique locale d'assurance.

[0050] Par exemple, compte tenu des résultats d'analyse de certains paramètres du réseau, fournis par le premier sous-module SM1, le cinquième sous-module SM5 peut décider de modifier son mode d'analyse ou bien demander au deuxième sous-module SM2 d'adresser une alarme à la couche NMS de sorte qu'elle adresse de nouvelles formules d'analyse. Il peut également décider de modifier un calendrier d'analyses, par exemple effectuées par le premier sous-module SM1.

[0051] Lorsque le cinquième sous-module SM5 décide de modifier le fonctionnement (ou la configuration) de l'un des sous-modules SM1 à SM4, il lui adresse les instructions correspondantes, ce qui revient à lui demander de modifier ses calculs et/ou analyses et/ou rapports. De même, le cinquième sous-module SM5 peut, lorsque la politique locale l'y autorise, être chargé de rétroagir sur la configuration du routeur via un module de reconfiguration embarqué.

[0052] Il est important de noter que les actions de reconfiguration (ou de modification de fonctionnement) décidées par le cinquième sous-module SM5 sont définies par les règles d'assurance de la politique locale. En d'autres termes, le cinquième sous-module SM5 ne fait qu'ordonner l'exécution d'actions prédéfinies.

[0053] Le cinquième sous-module SM5 peut également appliquer des règles d'assurance choisies à des données d'information provenant d'autres équipements de réseau NEj. En effet, un équipement NEj peut être chargé de transmettre des valeurs qu'il a mesurées et/ou agrégées à un autre équipement NEi équipé d'un dispositif D chargé de traiter ces valeurs de manière à générer de nouvelles données d'information qui peuvent être ensuite remontées au NMS ou envoyées à un autre équipement NEj.

[0054] La politique d'assurance locale peut être par exemple définie comme suit :

- si la tendance, estimée par le premier sous-module SM1, du nombre de paquets abandonnés augmente de plus de 5%, alors une alarme de tendance doit être émise,
- si la bande passante utilisée, analysée par le premier sous-module SM1, demeure inférieure à un premier seuil, alors la valeur de la bande passante utilisée doit être transmise chaque jour au module de collection MCC du NMS,
- si la bande passante utilisée, analysée par le premier sous-module SM1, est comprise entre un premier et un second seuils, alors la valeur moyenne de la bande passante utilisée doit être transmise toutes les heures au module de collection MCC du NMS,
- si l'intervalle de temps, estimé par le premier sous-module SM1, pour que la bande passante utilisée atteigne le second seuil, est inférieur à deux heures, alors une alarme de tendance doit être émise,
- si la charge de calcul (CPU) de l'équipement NEi, estimée par le premier sous-module SM1, est supérieure à 80%, alors les analyses de tendances ne doivent plus être effectuées,
- si la perte de paquets, estimée par le premier sous-module SM1, augmente de 5%, alors la taille des mémoires tampons (« buffers ») doit être augmentée de 5%.

[0055] En d'autres termes la politique d'assurance locale consiste ici, d'une première part, à transmettre chaque jour la mesure de la bande passante si le comportement de l'équipement NEi est normal, mais à activer les analyses de tendance et à augmenter la fréquence d'envoi des rapports si le comportement change, d'une deuxième part, à interrompre toutes les tâches impliquant un paramètre si la valeur de ce paramètre devient critique, et d'une troisième part, à modifier le fonctionnement interne de l'équipement NEi, représenté par un paramètre, en fonction de la variation dudit paramètre.

[0056] De préférence, le module d'assurance MAE est configurable à distance, via le réseau N, par le module de configuration MC du NMS. Plus précisément, chaque sous-module SM1 à SM5 est préférentiellement configurable. Cela permet en effet d'adapter à distance, le fonctionnement de chaque sous-module SM en fonction des circonstances, par exemple du fait de l'évolution du réseau N, et/ou en fonction des besoins, par exemple lorsque le gestionnaire d'assurance centralisé

du NMS a besoin de disposer des valeurs de nouveaux paramètres, ou de paramètres agrégés complémentaires, ou encore de nouvelles analyses réelles ou prospectives (envoi de nouvelles formules ou équations).

[0057] Deux modes de configuration peuvent être envisagés. Un premier mode consiste à transmettre indirectement les données de configuration au module d'assurance MAE via une interface de langage de programmation (ou API pour « Application Programming Interface ») implantée dans l'équipement NEi, ainsi qu'éventuellement via la MIB. Cette interface API peut également, et avantageusement, permettre au module de configuration MC du NMS de configurer ou de programmer la MIB, de sorte qu'elle ne soit pas de type statique. Le module d'assurance MAE peut en effet coopérer avec la MIB pour se configurer et définir de nouvelles entrées dans la MIB, afin de pouvoir accéder à ces nouvelles entrées. Dans ce cas, on accède à la MIB via des requêtes SNMP (« GET » et « SET »), ce qui permet une configuration aisée (voire même une gestion des droits et de la sécurité des échanges avec SNMP 3) ; la MIB permet d'avoir une interface « normalisée » du fait que ses champs sont accessibles via des OIDs (pour « Object Identifiers ») bien définis. On entend ici par « Object Identifier », un identifiant objet d'une variable MIB que l'on souhaite récupérer. Un tel identifiant est généralement normalisé, par exemple par le standard RFC 1213 pour la MIB II.

[0058] Un second mode consiste à transmettre directement les données de configuration au module d'assurance MAE à l'aide de commandes dédiées, telles que des « Command Line Interface » (ou CLI).

[0059] Le module d'assurance MAE peut être réalisé sous la forme de circuits électroniques, de modules logiciels (ou informatiques), ou d'une combinaison de circuits et de logiciels.

[0060] L'invention ne se limite pas aux modes de réalisation de dispositif de gestion locale d'assurance et d'équipement de réseau décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre des revendications ci-après.

[0061] Ainsi, dans ce qui précède on a décrit des équipements de réseau capables de gérer localement le procédé d'assurance supervisé par le NMS. Mais, on peut envisager un fonctionnement distribué dans lequel certains au moins des équipements de réseau sont équipés de dispositifs de gestion locale d'assurance simplifiés, chargés de transmettre des alarmes et/ou des données d'informations spécifiques et complémentaires à un serveur d'assurance du NMS. Bien entendu, dans ce cas les équipements de réseau demeurent capables d'adapter leur configuration en fonction des valeurs des données de gestion stockées dans leur MIB.

[0062] Par ailleurs, on a décrit un mode de réalisation dans lequel le dispositif selon l'invention était implanté ou embarqué dans l'équipement de réseau. Mais, le dispositif selon l'invention peut être agencé sous la forme d'un élément externe implanté dans un boîtier directement raccordé à l'équipement de réseau.

Revendications

1. Dispositif (D) de gestion locale d'assurance pour un équipement de réseau (NE) d'un réseau de communications (N) équipé d'un système de gestion de réseau (NMS), ledit équipement (NE) présentant une configuration choisie et comportant des moyens (MM) de mesure de valeurs de paramètre (s) du réseau et une base d'informations de gestion (MIB) propre à stocker des données de gestion représentatives desdites valeurs mesurées, **caractérisé en ce qu'**il comprend des moyens de gestion (MAE) agencés pour adapter la configuration dudit équipement (NE) en fonction d'au moins lesdites données de gestion stockées dans ladite base d'informations de gestion (MIB) et de règles, dites d'assurance, choisies, définissant une politique locale d'assurance, ladite adaptation consiste en une modification d'une politique de mesure de paramètre (s) et/ou une modification d'une politique d'envoi de rapport audit système de gestion de réseau (NMS).

2. Dispositif selon la revendication 1, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont agencés pour adapter ladite configuration en fonction de données d'informations provenant d'au moins un autre équipement de réseau (NE).

3. Dispositif selon l'une des revendications 1 et 2, **caractérisé en ce que** ladite adaptation consiste en une modification de son mode de fonctionnement.

4. Dispositif selon l'une des revendications 1 à 3, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens d'analyse (SM1) agencés pour déterminer, en fonction de certaines desdites règles d'assurance choisies, des données d'information représentatives de l'évolution temporelle, sur un intervalle choisi, de valeurs de paramètre(s) du réseau stockées dans ladite base d'informations de gestion (MIB).

5. Dispositif selon la revendication 4, **caractérisé en ce que** lesdits moyens d'analyse (SM1) sont agencés pour délivrer des données d'information représentatives d'une analyse de tendance et/ou d'une analyse de profils ou de signatures et/ou d'une analyse de discontinuité et/ou d'une agrégation de valeurs de paramètres du réseau.

6. Dispositif selon l'une des revendications 4 et 5, **caractérisé en ce que** lesdits moyens d'analyse (SM1) sont configurables.

7. Dispositif selon la revendication 6, **caractérisé en ce que** lesdits moyens d'analyse (SM1) sont agencés pour mettre en oeuvre de nouveaux calculs, relatifs aux paramètres du réseau, reçus dudit système de gestion de réseau (NMS).

8. Dispositif selon l'une des revendications 1 à 7, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens d'alarme (SM2) propres à déclencher l'envoi d'une alarme et/ou de données d'information audit système de gestion de réseau (NMS) et/ou à au moins un autre équipement de réseau (NE), en fonction de certaines desdites règles d'assurance choisies.

9. Dispositif selon la revendication 8, **caractérisé en ce que** lesdits moyens d'alarme (SM2) sont configurables.

10. Dispositif selon l'une des revendications 8 et 9, **caractérisé en ce que** lesdites données d'information et lesdites alarmes sont représentatives d'un résultat d'analyse, effectuée par lesdits moyens d'analyse (SM1), et/ou d'une agrégation de données, effectuée par lesdits moyens d'analyse (SM1), et/ou d'une valeur de paramètre du réseau stockée dans ladite base d'informations de gestion (MIB).

11. Dispositif selon l'une des revendications 1 à 10, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens d'observation du réseau (SM3) définissant un agent de mesure de flux de type « bout-en-bout », et agencés pour déterminer des données d'information représentatives dudit flux de type bout-en-bout en fonction de certaines desdites règles d'assurance choisies.

12. Dispositif selon la revendication 11, **caractérisé en ce que** lesdits moyens d'observation du réseau (SM3) sont configurables.

13. Dispositif selon l'une des revendications 1 à 12, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens de gestion d'accords de niveau de service (SM4) agencés pour déterminer des données d'information représentatives de ladite gestion des accords en fonction de certaines desdites règles d'assurance choisies.

14. Dispositif selon la revendication 13, **caractérisé en ce que** lesdits moyens de gestion d'accords de niveau de service (SM4) sont configurables.

15. Dispositif selon l'une des revendications 2 à 14, **caractérisé en ce que** lesdits moyens de gestion (MAE) comprennent des moyens de contrôle (SM5) propres à gérer le fonctionnement desdits moyens d'analyse (SM1), desdits moyens d'alarme (SM2), desdits moyens d'observation du réseau (SM3) et desdits moyens de gestion d'accords de niveau de service (SM4), en fonction de certaines au moins desdites règles d'assurance choisies.

16. Dispositif selon la revendication 15, **caractérisé en ce que** lesdits moyens de contrôle (SM5) sont alimentés en données d'information par lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'observation du réseau (SM3) et/ou lesdits moyens de gestion d'accords de niveau de service (SM4), et sont agencés pour ordonner auxdits moyens d'alarme (SM2) de générer des alarmes et/ou des rapports en cas de détection du non respect d'une règle d'assurance par des données d'information reçues.

17. Dispositif selon l'une des revendications 15 et 16, **caractérisé en ce que** lesdits moyens de contrôle (SM5) sont agencés sous la forme d'un moteur de règles (« rule engine ») stockant lesdites règles d'assurance choisies.

18. Dispositif selon l'une des revendications 15 à 17, **caractérisé en ce que** lesdits moyens de contrôle (SM5) sont configurables.

19. Dispositif selon l'une des revendications 1 à 18, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont propres à être configurés par ledit système de gestion de réseau (NMS) via une interface de langage de programmation (API) dudit équipement (NE).

20. Dispositif selon l'une des revendications 1 à 19, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont propres à être configurés par ledit système de gestion de réseau (NMS) via une interface de langage de programmation (API) dudit équipement (NE) et via ladite base d'informations de gestion (MIB).

21. Dispositif selon l'une des revendications 19 et 20, **caractérisé en ce que** lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'alarme (SM2) et/ou lesdits moyens d'observation du réseau (SM3) et/ou lesdits moyens de contrôle (SM5) et/ou lesdits moyens de gestion d'accords de niveau de service (SM4) sont propres à être configurés par ledit système de gestion de réseau (NMS), via ladite interface de langage de programmation (API).

22. Dispositif selon l'une des revendications 19 et 20, **caractérisé en ce que** lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'alarme (SM2) et/ou lesdits moyens d'observation du réseau (SM3) et/ou lesdits moyens de contrôle (SM5) et/ou lesdits moyens de gestion d'accords de niveau de service (SM4) sont propres à être configurés par ledit sys-

tème de gestion de réseau (NMS), via ladite interface de langage de programmation (API) et via ladite base d'informations de gestion (MIB).

23. Dispositif selon l'une des revendications 1 à 22, **caractérisé en ce que** lesdits moyens de gestion (MAE) sont propres à être configurés par ledit système de gestion de réseau (NMS) via des commandes dédiées.

24. Dispositif selon la revendication 23, **caractérisé en ce que** lesdits moyens d'analyse (SM1) et/ou lesdits moyens d'alarme (SM2) et/ou lesdits moyens d'observation du réseau (SM3) et/ou desdits moyens de gestion d'accords de niveau de service (SM4) et/ou lesdits moyens de contrôle (SM5) sont agencés pour être configurés par ledit système de gestion de réseau (NMS) via des commandes dédiées.

25. Dispositif selon l'une des revendications 23 et 24, **caractérisé en ce que** lesdites commandes sont de type « Command Line Interface ».

26. Equipement de réseau (NE) pour un réseau de communications (N) équipé d'un système de gestion de réseau (NMS), ledit équipement (NE) présentant une configuration choisie et comportant des moyens (MM) de mesure de valeurs de paramètre (s) du réseau et une base d'informations de gestion (MIB) propre à stocker des données de gestion représentatives desdites valeurs mesurées, **caractérisé en ce qu'**il comprend un dispositif (D) selon l'une des revendications précédentes.

27. Equipement selon la revendication 26, **caractérisé en ce qu'**il comprend une interface de langage de programmation (API), et **en ce que** ladite base d'informations de gestion (MIB) est propre à être configurée par ledit système de gestion de réseau (NMS) via ladite interface de langage de programmation (API).

28. Equipement selon l'une des revendications 26 et 27, **caractérisé en ce qu'**il comprend une interface de langage de programmation (API), et **en ce que** ladite base d'informations de gestion (MIB) est propre à être programmée par ledit système de gestion de réseau (NMS) via ladite interface de langage de programmation (API).

29. Equipement selon l'une des revendications 26 à 28, **caractérisé en ce qu'**il est choisi dans un groupe comprenant au moins les routeurs, les commutateurs et les pare-feu.

30. Réseau de communications (N) comportant un système de gestion de réseau (NMS), **caractérisé en ce qu'**il comprend une multiplicité d'équipements de réseau (NE) selon l'une des revendications 26 à 29.

31. Réseau selon la revendication 30, **caractérisé en ce que** chaque équipement (NE) est agencé pour délivrer audit système de gestion de réseau (NMS) des alarmes et/ou des données d'information de types différents.

32. Utilisation des dispositif, équipement et réseau de communications selon l'une des revendications précédentes dans les technologies réseaux devant être gérées.

33. Utilisation selon la revendication 32, **caractérisé en ce que** lesdites technologies réseaux sont choisies dans un groupe comprenant les réseaux de transmission, en particulier de type WDM, SONET et SDH, de données, en particulier de type Internet-IP et ATM, et de voix, en particulier de type classique, mobile et NGN.

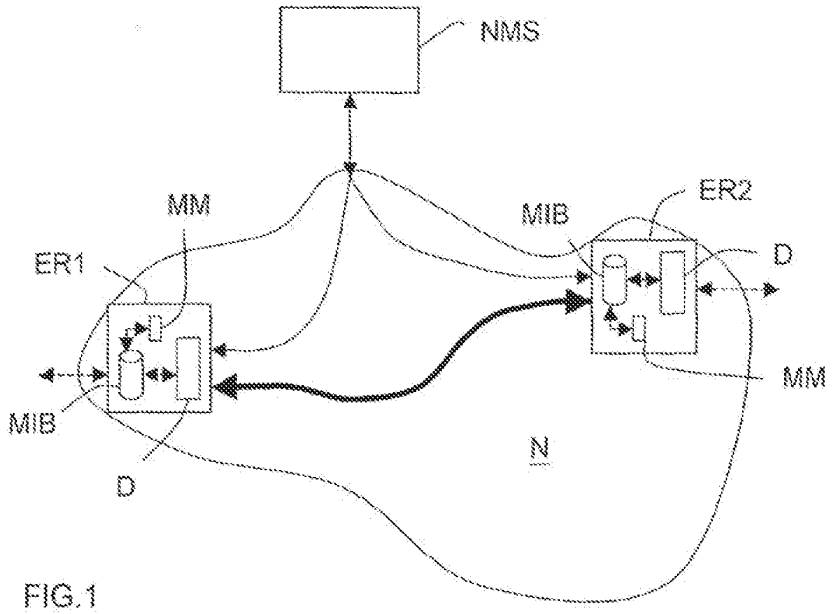

NMS
MM
MIB
ER2
ER1
D
MM
MIB
N
D

FIG.1

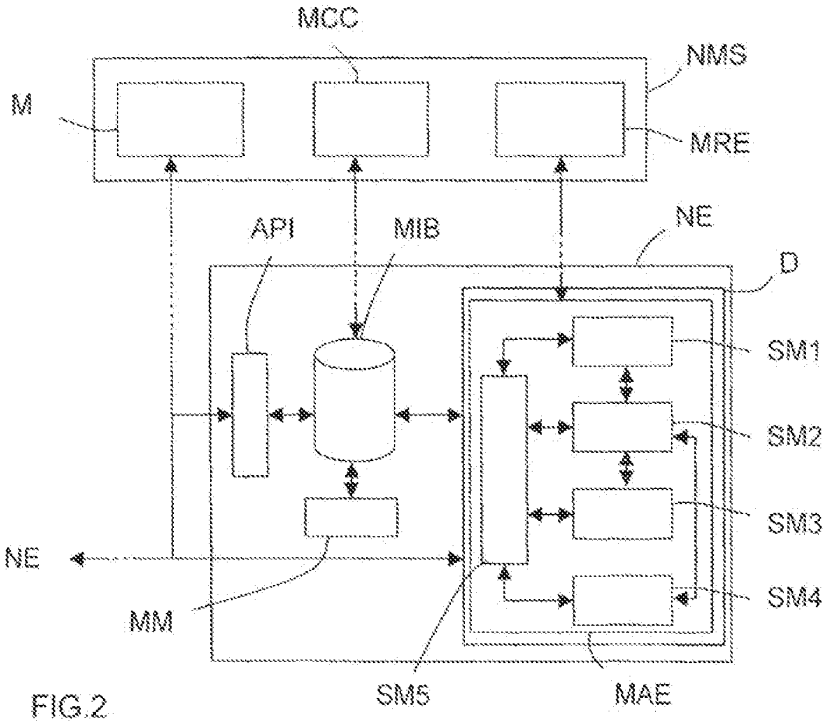

MCC
NMS
M
MRE
API
MIB
NE
D
SM1
SM2
SM3
SM4
NE
MM
SM5
MAE

FIG.2

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 04 29 0706

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	HO L L ET AL: "REAL-TIME PERFORMANCE MONITORING AND ANOMALY DETECTION IN THE INTERNET: AN ADAPTIVE, OBJECTIVE-DRIVEN, MIX-AND-MATCH APPROACH" BELL LABS TECHNICAL JOURNAL, WILEY, CA, US, vol. 4, no. 4, octobre 1999 (1999-10), pages 23-40, XP000902469 ISSN: 1089-7089 * abrégé * * page 24, colonne de droite - page 35, colonne de droite * * page 38, colonne de droite, alinéa 2 - page 39, colonne de gauche, alinéa 1 * -----	1-33	H04L12/24 H04L12/26
X	US 6 272 537 B1 (KEKIC MIODRAG M ET AL) 7 août 2001 (2001-08-07) * colonne 7, ligne 20 - ligne 65 * * colonne 8, ligne 42 - colonne 9, ligne 8 * * colonne 13, ligne 50 - colonne 85, ligne 11 * -----	1-33	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7) H04L
X	FR 2 774 191 A (INST EURECOM) 30 juillet 1999 (1999-07-30) * abrégé * * page 1, ligne 2 - ligne 8 * * page 3, ligne 5 - ligne 7 * * page 3, ligne 12 - ligne 17 * * page 4, ligne 12 - ligne 17 * * page 5, ligne 1 - page 6, ligne 3 * * page 7, ligne 1 - ligne 12 * * page 11, ligne 12 - page 16, ligne 6 * * figures 2,6,7 * ----- -/--	1-33	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	27 juillet 2004	Le Bras, P

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 04 29 0706

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	US 6 085 243 A (BANTHIA PRAKASH C ET AL) 4 juillet 2000 (2000-07-04) * abrégé * * colonne 1, ligne 17 - ligne 20 * * colonne 3, ligne 52 - colonne 5, ligne 10 * * colonne 5, ligne 52 - ligne 54 * * colonne 5, ligne 65 - colonne 6, ligne 26 * * colonne 6, ligne 44 - ligne 46 * * colonne 7, ligne 12 - ligne 23 * * colonne 8, ligne 14 - colonne 10, ligne 58 * * colonne 12, ligne 2 - ligne 4 * * colonne 14, ligne 11 - ligne 21 *	1-33	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	27 juillet 2004	Le Bras, P

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C09)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 04 29 0706

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

27-07-2004

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6272537 B1	07-08-2001	AUCUN	
FR 2774191 A	30-07-1999	FR 2774191 A1	30-07-1999
US 6085243 A	04-07-2000	AU 6601198 A	03-07-1998
		CA 2275235 A1	18-06-1998
		EP 0956680 A1	17-11-1999
		GB 2335124 A	08-09-1999
		WO 9826541 A1	18-06-1998
		US 5922044 A	13-07-1999
		US 6009274 A	28-12-1999
		US 6108782 A	22-08-2000
		WO 9843170 A1	01-10-1998

EPO FORM P0459

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No 12/82

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
10 July 2008 (10.07.2008)

(10) International Publication Number
WO 2008/080430 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2006/012006

(22) International Filing Date:
29 December 2006 (29.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELECOM ITALIA S.P.A.** [IT/IT]; Piazza degli Affari, 2, I-20123 Milano (IT).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **COSTA, Luciana** [IT/IT]; Telecom Italia S.p.A, Via G. Reiss Romoli, 274, I-10148 Torino (IT). **FREGUGLIA, Giorgio** [IT/IT]; Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT). **FROSALI, Federico** [IT/IT]; Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT).

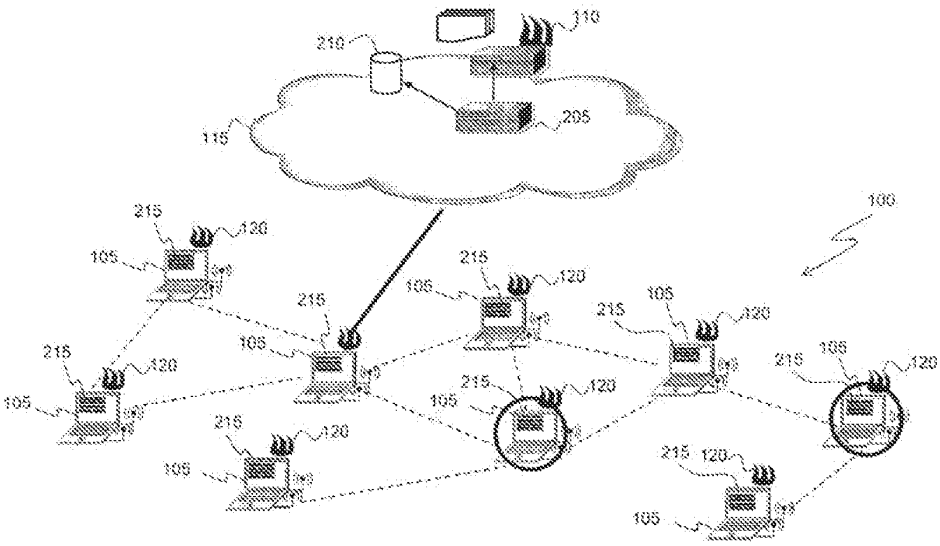
(74) Agent: **BATTIPEDE, Francesco**; Telecom Italia S.p.A., Piazza L. Einaudi, 8, I-20124 Milano (IT).

(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).

Published:
— *with international search report*

(54) Title: METHOD AND SYSTEM FOR ENFORCING SECURITY POLICIES IN MANETs



(57) Abstract: A method of enforcing security policies in a mobile ad-hoc network, comprising: - entrusting at least one first network node, along a data traffic route from a data traffic origin node to a data traffic destination node, with the enforcing of predefined security policies on said data traffic; - entrusting at least one second network node, distinct from said first network node, with the control of the enforcement of the security policies by said first network node.

WO 2008/080430 A1

METHOD AND SYSTEM FOR ENFORCING SECURITY POLICIES IN MANETs

DESCRIPTION

Background of the invention

Field of the invention

The present invention generally relates to the field of telecommunications, and particularly to Mobile Ad-hoc NETworks (MANETs). Even more particularly, the invention relates to the implementation and enforcing of security policies in MANETs. Specifically, the invention concerns a method and a system adapted to detect and react to situations wherein the enforcement of security policies set forth for a MANET is missing or improper.

Description of the related art

The heterogeneous nature and the mobility characteristics of a MANET makes it particularly difficult to control the behavior of the nodes that make up the network.

Nowadays, the acceptance of one or more network security rules by a generic MANET node as a condition for allowing the node accessing and becoming part of the network does not prevent that node from violating said rules later, and thus escaping from the control upon it. A node that, after an authentication procedure, has been granted access to an *ad-hoc* network is potentially able to perform any action, such as stop properly routing traffic received from and directed to other MANET nodes, allowing access to services to which some node is not authorized, allowing access to other nodes by revealing the necessary security information, like the ciphering keys.

For these reasons, distributed security mechanisms need to be defined for MANETs, aiming at making it more difficult to corrupt the network nodes.

The problem of the enforcement of security policies in *ad-hoc* networks has already been addressed.

For example, in the thesis work "Adaptive distributed firewall using intrusion detection" of L. Strand of the Oslo University, reference is made to a distributed firewalling architecture in which a master (a management station) distributes the security policies to clients, which are the nodes making up the network; the clients apply the security policies and notify the master of the results of the security policies application.

The described architecture is not expressly conceived for MANETs, but the latter is one of the environments considered as a possible application. The interaction with a distributed intrusion detection system is also considered, which, in case of necessity, allows to command a reconfiguration of the firewall of a certain node.

In J. Grant *et al.* "Distributed firewall technology", Signal 9 Solutions Inc., 2000, a distributed firewalling architecture is considered wherein a Distributed Firewall Server (DFS) distributes the security policies, valid for a certain network, to all the clients belonging thereto (possibly in a personalized way).

Each client, in normal operation, creates locally log files of its operation (also related to possible malfunctioning of the firewall) and of the traffic passing through that node; the logged data are then sent to the DFS, that correlates them for detecting possible inconsistencies with respect to the security policies deployed. The DFS, if possible, may also attempt to sniff the traffic, to check the proper implementation of the security policies deployed.

A different approach is described in S. Rajavaram *et al.*, "Neighboring watch: an intrusion detection and response protocol for mobile ad-hoc networks", University of Maryland, October 2002, where an architecture for detecting intrusions and anomalous behavior of the nodes belonging to a MANET is discussed. The possibility is exploited that a client (controller) being in the neighbourhood of other nodes "listens", over the wireless link, to the communications of said neighbouring nodes, so as to determine the presence of undesired or non-compliant traffic. The detection is made individually by every client, and the (possible) countermeasures may be applied locally, in a passive way, by exclusion of the malicious node from the announcements performed by the controller with the routing protocol, or in active way, notifying the violation to a master-cluster station that sets-up an election system involving all the MANET nodes for deciding together whether or not to exclude a certain client.

Summary of the invention

The Applicant has observed that the adoption of a distributed security mechanism is not, *per-se*, sufficient to ensure that each network node behaves properly. Moreover, from the viewpoint of a network operator/administrator, the adoption of a totally distributed security mechanism may be unacceptable, because incompatible with the network control capability that an administrator may want to have.

In the work of L. Strand, there is no real and reliable way of controlling the application of the security policies. From one hand, it is stated that it is the network node applying the policies that has to notify to the management station whether the policy application was successful: regretfully, if that node is corrupted, or pursues different plans, it may send to the management station false information. From the other hand, even if a distributed intrusion detection mechanism is envisaged, which might affect the firewall reconfiguration on the nodes, nothing is said about how this could be done; moreover, it seems that the proposed way is to employ the intrusion detection system to reveal classic intrusions, instead of controlling the proper application of the firewalling rules.

In the work of J. Grant *et al.*, which is not expressly conceived for MANETs, no efficient method of control of the security policies applied by the different clients is provided. The proposed solution relies in part on the communications between the clients and the DFS, but the reported data might be totally false. Also in respect of the envisaged possibility that the DFS directly sniffs the traffic for controlling the proper application of the policies, it is not explained how this could be done; moreover, within a MANET it is practically impossible that a single station, even if located within the MANET, can intercept all the network traffic, because in a wireless network any station may at most listen to the traffic passing within its radio

range.

In the work of S. Rajavaram *et al.*, the detection of anomalous behaviors is not focused on the control of the implementation of firewalling policies, rather on the generic control of a node. No mechanism is described for the selection of the nodes to be controlled by a controller node: this means that a node controls all the clients within its radio range, without limitations, but this might cause a great waste of the controller node's resources. Additionally, the proposed architecture does not envisage the presence of a real management node that tracks the overall behavior of the network.

The Applicant believes that there is the need of providing, for MANETs managed by a network operator/administrator, security mechanisms capable of exercising a control on the behavior of the network nodes, and also capable of allowing to check the proper application of the security policies intended to be implemented.

The Applicant has found that this need can be satisfied by means of a security mechanism which is based, from one side, on the centralization of the control mechanisms, through which the network is coordinated and managed, and, from another side, on the distribution of the security functions across the different network nodes.

In particular, the security mechanism according to an embodiment of the present invention allows to control the proper application, by every network node, of the security policies set forth by a network administrator, and to identify possible violations. This is achieved by entrusting the nodes of the network with the task of controlling the enforcement of the security policies, in order to detect cases of violations/improper enforcement of the security policies by other network nodes, and to identify the network nodes that are responsible of the security policies misapplication.

By distributing the control function to several, potentially all the network nodes, the data processing burden on the generic node is reduced, and the performance is thus improved, avoiding at the same time the formation of malicious "agreements" between network nodes, which could make the control vain; the overall network security is thus increased.

Essentially, the present invention proposes a mechanism for identifying the network nodes that are eligible for being controlled: advantageously, these nodes are a subset of the nodes of the network, and particularly they are the nodes that, due to the network topology, have the task of routing traffic from/to other network nodes.

In turn, the nodes that will have to perform the task of controllers are identified by an interaction with the routing protocol, designed to reduce, as far as possible, the number of nodes to be controlled by each controller node. Indeed, to verify the proper application of the security policies defined for the MANET, particularly to detect unauthorized traffic, each node should monitor all the traffic involving the nodes that are within its radio range, but this would imply a substantial waste of resources (particularly energy, which in mobile, wireless nodes is always precious). According to an embodiment of the present

invention, the number of controls to be carried out is significantly limited, by properly choosing the nodes to be controlled, to the extent that, at best, a node may continuously control just a single other node. Advantageously, a generic node may in general be controlled by more than one controller nodes (depending on the network topology).

The controller nodes are able to identify which node(s) has not properly enforced the security policies, as well as which node(s) violated the security policies, exploiting the missing enforcement of the security policies by network nodes that are entrusted with the enforcement thereof on the violator node.

The invention also provides for countermeasures to be taken once one or more nodes have been identified that violated or did not enforce the security policies.

Further, according to an embodiment of the present invention, selfish network nodes may be identified (and contrasting actions can accordingly be taken), *i.e.* nodes that tend to participate to the MANET in a utilitarian way, propagating only their own data packets, and not forwarding (discarding) data packets originated by, and addressed to other nodes.

According to an aspect of the present invention, a method of enforcing security policies in a mobile *ad-hoc* network is provided, comprising:

- entrusting at least one first network node, along a data traffic route from a data traffic origin node to a data traffic destination node, with the enforcing of predefined security policies on said data traffic;

- entrusting at least one second network node, distinct from said first network node, with the control of the enforcement of the security policies by said first network node.

According to another aspect of the present invention, a system for enforcing security policies in a mobile *ad-hoc* network, comprising:

- at least one first network node, along a data traffic route from a data traffic origin node to a data traffic destination node, entrusted with the enforcing of predefined security policies on said data traffic;

- at least one second network node, distinct from said first network node, entrusted with the control of the enforcement of the security policies by said first network node.

Brief description of the drawings

The features and advantages of the present invention will result apparent by reading the following detailed description of an embodiment thereof, provided merely by way of non-limitative example, and referring to the annexed drawings, wherein:

Figure 1 pictorially shows a scenario of a MANET where the present invention can be applied;

Figure 2 schematically shows network elements implementing a Distributed Firewall Control (DFC) architecture, according to an embodiment of the present invention;

Figure 3 describes a format of HELLO messages exploited by a routing protocol adopted in the MANET;

Figure 4 schematically shows an example of application of a DFC mechanism implemented by the DFC architecture of Figure 2;

Figure 5A shows a format of Topology Control (TC) messages used by the routing protocol;

Figure 5B schematically shows the information that a DFC client of the DFC architecture maintains in order to detect the nodes whose behavior is not compliant to MANET security policies;

Figure 5C schematically shows the information included in a routing table kept by a DFC client;

Figure 6 schematically shows a DFC selection mechanism in case of a loop;

Figure 7 is a schematic flowchart of a node identification mechanism for identifying the network node that has not enforced the prescribed security policies, according to an embodiment of the present invention;

Figures 8A to 8F schematically show examples of the identification of nodes that have not enforced the security policies;

Figure 9 is a schematic flowchart of a node quarantine mechanism according to an embodiment of the present invention;

Figures 10A and 10B are schematic flowcharts of a process of management of alarm messages used in the DFC architecture, according to an embodiment of the present invention;

Figure 11 schematically shows a content of a notification alarm message used in an embodiment of the present invention;

Figure 12 schematically shows a content of a quarantine alarm message used in an embodiment of the present invention;

Figure 13 schematically shows a content of an alert alarm message used in an embodiment of the present invention;

Figures 14A and 14B show a content of global repair request and accept alarm messages used in an embodiment of the present invention;

Figure 15 describes an architecture of a selfish node detection mechanism according to an embodiment of the present invention; and

Figure 16 shows a content of a selfish node quarantine message used in an embodiment of the present invention;

Detailed description of the preferred embodiment of the invention

In Figure 1, a scenario in which the present invention is advantageously applied is schematically shown. In the drawing, reference numeral 100 denotes a MANET comprising a plurality of mobile network nodes 105, in wireless communications relationship, where the generic network node 105 communicates with other network nodes through neighbouring network nodes 105 that, at a certain moment, fall within its radio range. In the drawing, two nodes that are in direct connection with one another are depicted as connected by a dashed line. Since in general two network nodes cannot in direct connection, because

they cannot fall within their respective radio ranges, each node **105** of the MANET acts not only as a traffic originator and/or a traffic destination, but also as a traffic router, routing traffic from/to other nodes of the network. Thus, even if the radio range of the network nodes is relatively limited, the network can cover a wide area, because nodes that are not directly interconnected can nevertheless communicate with each other *via* a multi-hop transmission.

Reference numeral **110** denotes a functional entity, like a server, connected to the MANET **100** through an infrastructured network **115**, and configured to centrally manage the deployment to, and implementation of security policies in the MANET nodes **105**. The infrastructured network may include one or more Public Switched Telephone Network (PSTN) and/or one or more mobile telephony networks like GPRS or UMTS networks; the nature and type of the infrastructured network **115** is *per-se* not limitative to the present invention. The MANET **100** may in particular constitute an "extension" of the infrastructured network **115**, by means of which services offered by the network operator to users of the infrastructured network **115** can also be offered to users of the mobile network nodes **105**. The MANET **100** may also operate as a replacement of the infrastructured network **115** in case of failure of the latter.

In particular, the server **110** may be managed by an administrator of the MANET **100**, for example an administrator operating on behalf of the operator of the infrastructured network **115** MANET **100**. By means of the server **110**, the network administrator keeps a control on the traffic exchanged through the MANET **100**, defining security policies to be applied by the MANET nodes **105**; the security policies may for example be deployed dynamically *via* the infrastructured network **115** and the MANET **100**.

According to the present invention, it is ensured that the desired security policies are effectively applied and respected, *i.e.* that the security policies are enforced.

According to an embodiment of the present invention, a Distributed Firewalling Architecture (DFA) is implemented in the MANET **100**, adapted to set-up a distributed firewalling mechanism, according to which the firewalling operations are entrusted to the MANET nodes **105**. The generic MANET node **105** behaves as a client (hereinafter referred to as a Distributed Firewalling Architecture client or, shortly, "DFA client") in respect of the server **110** (hereinafter referred to as the "DFA server"). The client resident in the generic MANET node **105**, schematically depicted in the drawing and denoted **120**, is adapted to dynamically receive from the DFA server **110** security policies to be applied in the MANET, to interpret the received security policies and to translate them into lower-level traffic filtering rules (e.g., Internet Protocol – IP - filtering rules), used for filtering the traffic that is routed by the MANET nodes, as will be described in detail later.

According to an embodiment of the present invention, the generic MANET node **105** does not filter its own traffic, *i.e.* the traffic it originates or that is destined thereto, rather it filters the traffic of the other MANET nodes, particularly of the neighbouring MANET nodes; in other words, considering the

generic MANET node **105**, its traffic is filtered by one or more of the neighbouring MANET nodes.

In particular, according to an embodiment of the present invention, an efficient traffic filtering policy is implemented, which provides for entrusting the network traffic filtering operation to a subset of MANET nodes, particularly to the neighbouring nodes of a node that is either the source of the data traffic or the destination of the data traffic. In this way, it is avoided that every MANET node has to apply the security policies, *i.e.* the data traffic filtering rules valid for all the MANET nodes, and has to compare to such rules every data packet received before routing it. In other words, according to an embodiment of the present invention, the filtering of a data packet sent by a certain source or origin node, like the network node denoted **105s** in **Figure 1**, towards a certain destination, like the network node **105d** in the drawing, is carried out only by the (DFA client resident on the) node **105a** that, along the route **125** followed by the data packet, immediately follows the source node, and by the node **105b** that, along said route, immediately precedes the destination node.

In particular, in an embodiment of the present invention, indications about the network topology are exploited to identify which MANET nodes have to filter the data traffic; in particular, said network topology indications are included in and propagated by routing messages from which the generic DFA client **120** can derive, in real time, which are the MANET nodes with which it can communicate. In particular, the knowledge of the distance from each node, in terms of number of hops, enables the DFA client **120** resident on the generic MANET node **105** to classify the nodes of the MANET as neighbouring nodes and distant nodes; for the purposes of the present description and claims, by "neighbouring node" it is meant a MANET node that is one hop distant from the generic node, whereas by "distant node" it is meant a MANET node more than one hop distant from the generic node. In this way, the DFA client **120** resident on the generic MANET node **105** is adapted to dynamically configure itself, adding and/or removing security policy rules based on the changes in the network topology, and actuating only the rules that are associated with the nodes it knows, *i.e.* its neighbouring nodes.

Entrusting the enforcement of the security policies defined in respect of a certain MANET node **105**, like for example the node **105s** in **Figure 1**, to the (DFA client **120** resident on the) neighbouring nodes, *i.e.* the node **105a** in the example of **Figure 1**, avoids that the remaining, successive nodes on the route **125** followed by a data packet sent by the node **105s** (like the node **105c** in the shown example) have to perform filtering operations on the same data traffic, because this filtering operation is useless, since assumed that the filtering has been made by the node **105a** the traffic inherently complies with the prescribed security policies.

The further filtering entrusted to the node that, like the node **105b** in the example of **Figure 1**, immediately precedes the data packet destination node **105d** is not essential, but it increases the overall network security.

In addition to the distributed firewalling architecture and mechanism described above, according

to an embodiment of the present invention, a distributed firewall control architecture is implemented in the MANET **100**, adapted to set-up a distributed control mechanism for detecting the presence, in the MANET **100**, of traffic not compliant with a certain security policy, and, in case such non-compliant traffic is detected, to identify the node(s) which has not properly enforced the security policy, as well as to identify the node(s) that violated the security policy, and to consequently take proper countermeasures. The distributed control mechanism allows avoiding that unauthorized traffic, generated by a node that violated the security policies, and not properly filtered by the client DFA on the node entrusted with the security policies enforcement (the node that immediately follows the source node), is routed through several network nodes before being filtered out, for example by the node that immediately precedes the destination node, with a consequent saving of network nodes' power and bandwidth resources.

According to an embodiment of the present invention, as schematically shown in **Figure 2**, the distributed firewall control architecture comprises a distributed firewall control server (hereinafter shortly referred to as "DFC server") **205**, possibly, albeit not limitatively, co-located with the DFA server **110**. The DFC server **205** is configured to centrally manage and coordinate a distributed firewall control mechanism, taking proper countermeasures in respect of MANET nodes that do not properly enforce the security policies and nodes that violate the security policies defined for the MANET; the DFC server **205** interacts with the DFA server **110** and, possibly, with further entities forming a security platform of the MANET, like for example one or more authentication servers **210**.

Like in the scenario of **Figure 1**, each MANET node **105** acts as a client (DFA client) of the DFA server **110**, *i.e.* as an enforcer of the firewalling policies defined for the nodes that, at a certain time, are its neighbours. In addition to the DFA client, a DFC client **215** is resident on each MANET node **105**, adapted to detect the proper application of the security policies by the DFA clients, *i.e.* by the security policies enforcers.

Additionally, on the generic MANET node **105** one or more applications designed to implement the desired routing protocol are assumed to be resident (not shown in the drawing), adapted to set up the data packets routes for reaching nodes that are distant more than one hop. In particular, said routing protocol is assumed to be a proactive routing protocol. As known to those skilled in the art, routing protocols defined for MANETs are generally classified as proactive protocols and reactive protocols, depending on how the routes towards the destination nodes are determined; in proactive protocols, every node periodically propagates to the network its topological information so that each node in the MANET is able to build the network map and to calculate a path to reach every node. With reactive protocols, the generic node calculates a path towards another node only at the time the former node has to send data to the latter node.

In particular, according to an embodiment of the present invention, the routing protocol adopted is the Optimized Link State Routing (OLSR) protocol, described for example in T. Clausen, P. Jacquet,

"Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003. The OLSR protocol uses a broadcast algorithm exploiting a subset of the MANET nodes **105**, referred to as the MultiPoint Relay (MPR), specifically for the propagation of the routing messages. Each node that implements the OLSR routing protocol builds its own set of MPR nodes (the "MPR set"), by means of a procedure called "neighbour detection", and gets indications about the lists of nodes that are distant one or two hops therefrom; then, the considered node elects as MPR node one of the neighbouring nodes with which there is a bidirectional link (a "symmetric neighbour"), which allows the considered node to reach another node distant two hops. In this way, the union of the areas covered by the radio ranges of all the MPR nodes elected by one generic node covers all the nodes that are distant two hops therefrom. Each node sends to its neighbouring nodes the respective set of elected MPR nodes through particular OLSR protocol messages, referred to as "*HELLO*" messages; the structure of a *HELLO* message is pictorially shown in **Figure 3**. The *HELLO* message, globally denoted **300**, includes one or more fields **305** called "*Neighbour Interface Address*", wherein each node inserts the network addresses (IP addresses) of its neighbouring nodes, distant one hop, and a field **310** called "*Neighbour Type*", wherein each node defines if the node with neighbour interface address is an MPR for it . For example, referring to scenario shown in **Figure 4**, wherein an exemplary network topology **400** is depicted, node **405a** inserts into the fields **305** of the *HELLO* messages it sends the addresses of nodes **405b**, **405c**, **405d** and **405e**; among these nodes, node **405a** elects as MPR node only the node **405e**, thus, in the *HELLO* messages, it sets for this node the field **310** to a value "*MPR_NEIGH*", to indicate that the node **405e** is an MPR.

The nodes that are elected MPR nodes, in addition to sending their own *HELLO* messages, periodically send "*TOPOLOGY CONTROL*" ("*TC*") messages; the structure of a *TC* message is pictorially shown in **Figure 5A**: the message, globally denoted **500**, includes a plurality of fields **505** called "*Advertised Neighbour Main Address*", each one adapted to contain the address of one network node that has elected the considered node as its MPR. In this way, each network node can build its own routing table: the routes towards all the possible destinations are calculated passing through the MPR nodes elected by each node.

According to an embodiment of the present invention, the firewall control mechanism implemented by the DFC architecture advantageously exploits the principles of operation of the OLSR routing protocol and the correspondingly obtained network topological indications, in order to limit the number of controls to be performed to a subset of the MANET nodes. In particular, also the MANET data traffic is caused to pass through the nodes that are elected MPR nodes in respect of the OLSR protocol. This is achieved by causing every node, when building the respective routing table, to configure as next-hop for reaching a desired destination one of the MPR nodes which have been elected by that node. In this way, a first optimization of the DFC mechanism is achieved, that allows performing the firewall control function only on the MPR nodes, *i.e.* only on those nodes that actually handle the routing of data traffic

from/to the other nodes. The MPR nodes form altogether a relatively small subset of all the MANET nodes (in **Figure 4**, the MPR nodes are shown as encircled, and the subset of MPR nodes is denoted **450**). Thus, the subset of MPR nodes becomes the set of the DFA clients **120** that are subjected to controls in order to guarantee that the security policies defined for the MANET are actually applied and enforced.

Additionally, the DFC client **215** resident on the generic network node is adapted to choose, within the above-mentioned subset **450** of DFA clients **120** to be controlled, that or those DFA clients on which to perform the control, by means of a nodes selection mechanism.

According to an embodiment of the present invention, the nodes selection mechanism enables the generic DFC client **215** to:

- limit the number of controls it has to perform to a small, possibly the smallest number of DFA clients **120** (ideally, a DFC client may have to control just one DFA client); and

- guarantee that the choice of the node to control does not jeopardize the possibility of controlling a different DFA client **120**; in other words, all the DFA clients belonging to the above-mentioned subset **450** of the MPR nodes should be controlled by at least one DFC client.

Hereinafter, the DFC mechanism according to an embodiment of the present invention is described in detail, applied to the exemplary MANET shown in **Figure 4**. It is assumed that the nodes denoted **405a**, **405e**, **405f**, **405g** and **405h** (shown as encircled) are the elected MPR nodes elected by the routing process of the OLSR; the nodes **405a**, **405e**, **405f**, **405g** and **405h** thus represent the subset **450** of the DFA clients **120** that are to be controlled. Each DFC client **215** knows this subset of nodes **405a**, **405e**, **405f**, **405g** and **405h** based on the topological indications acquired by the routing protocol.

Essentially, the DFC mechanism includes three phases.

In a first phase, based on the subset of nodes thus built, each DFC client **215** chooses one DFA client **120** (*i.e.*, one node) within the subset of nodes to be controlled, using the above mentioned selection mechanism.

A second phase and a third phase, described in detail later on, concern actions to be taken in case it is ascertained that the security policies are not properly implemented; the actions that, according to an embodiment of the present invention, can be taken are a local repair action and a global repair action.

In an embodiment of the present invention, the selection mechanism adopted for selecting the DFA clients **120** to be controlled is the following.

Each DFC client **215**, residing on a certain network node **105**, firstly assesses the number of MPR nodes that have been elected by the network node where such DFC client **215** resides.

If the number of elected MPR nodes is equal to 1, then the DFA client to be controlled is the sole MPR node that has been elected. Referring to the example of **Figure 4**, the node **405c** is assumed to have elected as MPR only the node **405a**, thus the DFC client **215** resident on node **405c** controls the DFA client **120** resident on node **405a**.

If instead the number of elected MPR nodes is greater than 1, the DFC client **215** assesses whether the node where it resides is involved in a loop, *i.e.* it is part of a closed path, originating at and terminating in a same node; in the example depicted in **Figure 6**, a loop **600** exists, originating at node **605a**, passing through nodes **605b**, **605c**, **605d** and **605e**, and terminating in node **605a**. The assessment of the existence of loops by the generic DFC client is for example carried out using the MPR selector set transmitted by every MPR node in the *TC* messages it sends (the MPR selector set is the group of node addresses contained in the fields *Advertised Neighbour Main Address* **505** of the *TC* message **500** depicted in **Figure 5A**); as mentioned in the foregoing, this information allows building up a path from a certain source node to a certain destination node.

If the DFC client ascertains that there is a loop originating at and terminating in the node where it resides, like in the case of the DFC client **215** residing on node **605a** of **Figure 6**, then the DFC client **215** decrees that the node where it resides is involved in a loop.

In case no loops are identified, the DFC client **215** chooses to control, among the MPR nodes elected by the node where it resides, the MPR node through which the lowest number of nodes distant two hops can be reached. Referring to the example of **Figure 4**, let it be assumed that the node **405e** has elected as MPR the nodes **405a** and **405f**; through the node **405a**, the node **405e** can reach the nodes **405b**, **405c** and **405d**, distant from it two hops, whereas through the node **405f** it can only reach the node **405g**: thus, the DFC client resident on the node **405e** chooses to control the DFA client **120** resident on the node **405f**. If two or more MPR nodes allow reaching the same number of nodes distant two hops, then the DFC client **215** chooses as DFA client to control the one resident on a node which, in turn, has elected the lowest number of MPR nodes. If even in this way two or more nodes are identified, then the choice is made randomly. This is for example the case of node **405f** of **Figure 4**, which has elected as MPR nodes the nodes **405e** and **405g**; through the node **405e**, the node **405f** can reach the nodes **405a**, **405i** and **405m**, whereas through the node **405g** it can reach the nodes **405h**, **405n** and **405p**, all distant two hops. Not being able to make a discrimination, between the nodes **405e** and **405g**, then the node **405f** looks which, among the nodes **405e** and **405g**, has elected the lowest number of MPR nodes: the node **405e** has elected as MPR nodes the nodes **405a** and **405f**, whereas the elected MPR nodes of the node **405g** are the nodes **405f** and **405h**; again, it is not possible to discriminate between the nodes **405e** and **405g**,, so the DFC client resident on the node **405f** performs a random choice, and for example the choice is made of node **405g**.

Let now the case be considered that loops exist. In the worst case, for each DFA client **120** there is only one DFC client **215** that can control it. It is therefore necessary to avoid that two DFC clients **215** choose to control a same DFA client **120**, otherwise it may happen that the control of (the DFA client **120** resident on) all the nodes in the subset **450** of elected MPR nodes is not guaranteed. In this case, the DFC client **215** should select the DFA client **120** to control following a certain control direction, denoted

610 in the example of Figure 6. In particular, according to an embodiment of the present invention, the control direction is defined by the node, in the loop, having the numerically lowest IP address; for example, making reference to Figure 6, and assuming that the IP addresses of the nodes 605a, 605b, 605c, 605d and 605e are *210*, *212*, *214*, *216* and *218*, the numerically lowest address is *210*. In the *TC* message 500 transmitted by the node 605a, each DFC client 215 identifies the first node 505a announced in the MPR selector set among those making part of the loop. Thus, each DFC client 215 chooses, as DFA client 120 to control, the one residing on the MPR node that, starting from the node where the considered DFC client 215 resides and passing through the node in the loop having lowest IP address, allows reaching the first node 505 announced in the MPR selector set in the *TC* message. Referring to the example of Figure 6, a loop 600 exists formed by the nodes 605a, 605b, 605c, 610d and 610e; in this case, the node of the loop 600 having the lowest IP address is the node 605a (IP address = *210*), so this node 605a is the one defining the control direction to be followed. All the DFC clients 215 resident on the nodes of the loop 600 look at the MPR selector set announced by the node 605a in the *TC* messages it sends; in this example, the MPR selector set is assumed to be formed by the nodes 605e and 605b, and it is also assumed that the node 605e is the first to be announced in the MPR selector set (this node is also part of the loop). Thus, the control direction 610 to be followed is the direction that, passing through the node 605a (*i.e.* the node with lowest IP address in the loop), allows reaching the node 605e (the first announced node in the MPR selector set). The DFC client 215 resident on the node 605c thus chooses to control the DFA client 120 resident on the node 605b, which allows it to reach the node 605e passing through the node 605a; similarly, the DFC client 215 resident on the node 605d chooses to control the DFA client 120 resident on the node 605c, which allows it reaching the node 605e passing through the node 605a. In this way, each node of the loop is controlled by another node.

Hereinafter, examples of countermeasures that can be taken when it is detected a violation of the security policies will be described.

Local repair mechanism

The local repair mechanism calls for placing in quarantine the network node where a DFA client 120 resides which has not properly enforced the security policies defined for the MANET. The quarantine has effect locally to the MANET (*i.e.* the DFC server 205 is not involved) and it is directed to temporarily isolate the detected node on which the DFA client 120 which has not properly enforced the security policies resides.

In particular, in an embodiment of the present invention, the quarantine mechanism is applied to a generic node a maximum, predetermined number of times, defined for example by a threshold value; once a node has been put in quarantine the maximum number of times, a global repair mechanism (described later on) can be applied to that node.

The choice of allowing a DFA client 120 to be put in quarantine more than once is motivated by

the fact that an incorrect enforcement of the security policies might be caused by a temporary misalignement of a DFA client **120** with the DFA server **110**, due for example to an ongoing update of the security policies, or to a delay of convergence of the routing protocol, thereby the topological indications used for applying the security policies may not be sufficiently up to date.

Every DFC client **215** performs an active control of the DFA client **120** that has been selected for being controlled, by means of a continuous monitoring of the (entering and exiting) traffic flowing through the node hosting the controlled DFA client **120**, so as to detect cases of missed enforcement of the security policies.

Each time a DFC client **215** detects an improper application of the security policies defined for the MANET, it stores data, schematized in **Figure 5B** and denoted therein as **507**, comprising:

- the IP address (IP_S) **510** of the node originating the data packets that violate a certain security policy;
- the IP address (IP_D) **515** of the destination node of those data packets;
- the MAC (Media Access Control) address (MAC_in) **520** of the node originating the incoming traffic entering into the node hosting the controlled DFA client **120**; this MAC address MAC_in corresponds to the node that has routed the traffic to the node hosting the DFA client **120** being controlled;
- the identifier (ID) **525** of the traffic session.

Additionally, every DFC client **215** keeps, for all the MANET nodes, an association between the IP address IP_S of the source node and the related MAC address MAC_S (field **530**).

Based on this data, the DFC client **215** starts the local repair procedure, which calls for:

- identifying the DFA client **120** that has not properly enforced the security policies; and
- put in quarantine the network node on which the identified DFA client **120** resides.

To identify the DFA client **120** that has not properly enforced the security policies, the DFC client **215** exploits the data **507**, particularly the MAC address MAC_in **520** of the traffic entering the controlled DFA client **120**, as well as the routing table; as known to those skilled in the art, the routing table, schematically depicted in **Figure 5C** and denoted therein as **550** is a table that the generic node uses to know how to reach any other network node, and wherein the number of hop counts necessary to reach the other nodes is specified. Using the data contained in the routing table **550**, the DFC client **215** is capable of determining how far is, in terms of hops number ("hop count"), the source node, whose address is the IP_S.

The procedure for identifying the DFA client **120** that has not enforced the security policies is schematized by the flowchart of **Figure 7**.

Firstly, the DFC client searches, in its routing table, the entry corresponding to the node having address equal to IP_S, *i.e.* the source node originating the traffic that violated the security policy, so as to

derive the corresponding hop count value (block **705**).

If the hop count value is equal to 1 (block **710**, exit branch Y), then the node with address IP_S is directly reachable by the node where the DFC client **215** resides. The DFC client **215** checks whether the MAC address MAC_in of the traffic entering the controlled DFA client **120** coincides with the MAC address MAC_S of the source node (block **715**). In the affirmative case (exit branch Y of block **715**), the (node hosting the) controlled DFA client **120** is thus responsible of the security policies violation (*i.e.*, it is the security policy violator node): the DFC client **215**, being the next hop in respect of the security policies violator node, puts the latter node in quarantine (block **720**).

Considering the exemplary situation depicted in **Figure 8A**, let the traffic originated by node **805a** and destined to node **805b** be considered, and let it be assumed that the node **805a** is not authorized, by the security policies defined for the MANET, to generate such traffic. In such a case, the node **805c**, is a direct neighbour of the source node **805a**, and the node **805d** is a direct neighbour of the destination node **805b**. The two nodes **805c** and **805d** are responsible of enforcing the security policies, blocking the traffic generated by the node **805a**. Let it be assumed that the DFA client **120** resident on the node **805c** does not enforce the security policies, and lets the traffic originated by the node **805a** pass through. The DFA client **120** resident on the node **805c** is thus the security policies violator, which should be identified by the DFC mechanism. Let it be assumed that the DFC client **215** resident on a node **805e** is the controller of the DFA client **120** hosted by the node **805c**: inspecting the traffic exiting the node **805c**, the DFC client **215** hosted by the node **805e** is able to detect that the traffic having IP_S equal to that of the node **805a** is not authorized in the MANET. Looking at its routing table, the DFC client **215** hosted by node **805e** determines that the hop count value for the node **805a** is equal to 1, and that the MAC address MAC_in of the traffic entering the controlled DFA client **120** hosted by node **805c** coincides with the MAC address MAC_S of the source node **805a**. Thus, the DFC client **215** hosted by node **805e** determines that the controlled DFA client **120** has not enforced the security policies, and it is a security policies violator: being the controller node **805e** a direct neighbour of the violator node **805c**, the controller node **805e** directly puts the violator node **805c** in quarantine.

Referring back to **Figure 7**, if the two MAC addresses MAC_in and MAC_S do not coincide (exit branch **N** of block **715**), the DFA client **120** that has not enforced the security policies resides on the node that, along the route from the source node (IP address IP_S) to the destination node (IP address IP_D) precedes the controlled DFA client **120**, *i.e.* on the node whose MAC address is MAC_in (in fact, the node responsible of enforcing the security policies is the next hop of the source node, with IP address IP_S, so it cannot be the controlled DFA client **120**, because the latter is distant two hops). The DFC client **215**, not being the next-hop of the security policies violator node, does not directly put the violator node in quarantine: it instead broadcasts an alarm signal, particularly a *NOTIFICATION* message (block **725**), described in detail later on, for notifying to the other MANET nodes that the identified DFA client **120** has

not properly enforced the security policies, for asking the neighbouring nodes to put the violator node in quarantine, and for asking the nodes that are along the route from the source node to the destination node to temporarily apply the violated security policies.

Considering the exemplary situation depicted in **Figure 8B**, let the traffic originated by the source node **805a** and destined to the destination node **805b** be considered, assuming that the node **805a** is not authorized, by the security policies defined for the MANET, to generate such traffic. Node **805c** is a direct neighbour of the source node **805a**, and node **805d** is a direct neighbour of the destination node **805b**; the two nodes **805c** and **805d** are thus responsible of enforcing the security policies, blocking the traffic generated by the node **805a**. Let it be assumed that the DFA client **120** resident on node **805c** does not enforce the security policies, and lets the traffic originated by node **805a** pass through; the node **805c** is thus the security policies violator, that should be identified by the DFC mechanism. The DFC client **215** resident on node **805f** is the controller of the DFA client **120** resident on node **805g**. Inspecting the traffic leaving node **805g**, the DFC client **215** resident on node **805f** detects that the traffic source IP address IP_S corresponding to the IP address of the source node **805a** is not authorized in the MANET. Based on its routing table, the DFC client **215** resident on node **805f** derives that the hop count value for the source node **805a** is equal to 1, but the MAC address MAC_in of the traffic entering the controlled DFA **120** client resident on node **805g** differs from the MAC address MAC_S of the source node **805a**. Thus, the DFA client **120** that has not enforced the security policies resides on the node having MAC address equal to MAC_in, *i.e.* on the node **805c**. The DFC client **215** resident on the node **805f** cannot directly put in quarantine the violator node **805c**, thus it broadcasts a *NOTIFICATION* alarm message.

Referring back again to **Figure 7**, if the hop count is not equal to 1 (exit branch **N** of block **710**), the DFC client **215** ascertains whether the hop count value is equal to 2 (block **730**).

If the hop count value is equal to 2 (exit branch **Y** of block **730**), then the source node originating the traffic in violation of the security policies is not directly reachable by the DFC client **215**. The DFC client **215** then checks if the MAC address MAC_in of the traffic entering the controlled DFA client **120** coincides with the MAC address MAC_S of the source node (block **735**). In the affirmative case (exit branch **Y** of block **735**), the DFA client **120** controlled by the considered DFC client **215** is responsible of the security policies violation, *i.e.* it is the violator node. The DFC client **215**, being in this case a next hop of the violator node, directly puts the violator node in quarantine (block **720**).

Referring to the exemplary scenario depicted in **Figure 8C**, let the traffic originated by source node **805a** and destined to the destination node **805b** be considered, and let it be assumed that the source node **805a** is not authorized, based on the security policies valid for the MANET, to generate such traffic. In this situation, node **805c** is a direct neighbour of the source node **805a**, and node **805d** is a direct neighbour of the destination node **805b**. The two nodes **805c** and **805d** are thus responsible of the enforcement of the security policies, blocking the traffic generated by the source node **805a**. Let it be

assumed that the DFA client **120** resident on the node **805c** does not enforce the security policies, letting the traffic originated by the source node **805a** pass through: the (DFA client **120** on) node **805c** is thus the security policies violator, that should be identified by the DFC mechanism. The DFC client **215** resident on node **805h** is one of the controllers of the DFA client **120** on node **805c**. Inspecting the traffic exiting the node **805c**, the DFC client **215** resident on node **805h** detects that the traffic with source IP address IP_S equal to the IP address of the source node **805a** is not authorized in the MANET. Looking at its routing table, the DFC client **215** resident on node **805h** derives that the hop count value for the source node **805a** is equal to 2, and that the MAC address MAC_in of the traffic entering the controlled node **805c** coincides with the MAC address MAC_S of the source node **805a**. Thus, the DFA client **120** resident on node **805c** controlled by the DFC client **215** resident on node **805h** has not enforced the security policies, and node **805c** is the violator; since the controller node **805h** is a next-hop of the violator node **805c**, the DFC client **215** resident on node **805h** directly puts the violator node **805c** in quarantine.

Back to **Figure 7**, if the two MAC addresses MAC_in and MAC_S do not coincide (exit branch **N** of block **735**), the DFC client **215** checks if the IP address IP_S of the source node is included in the MPR selector set announced in the *TC* messages issued by the node having the MAC address MAC_in of the traffic entering the controlled node (block **740**).

In the affirmative case (exit branch **Y** of block **740**), the security policy violator node is the node which, along the route from the source node (with IP address IP_S) to the destination node (with IP address IP_D), precedes the controlled node, *i.e.* the node having MAC address equal to MAC_in. In such a case, the considered DFC client **215**, not being the next hop of the violator node, cannot directly put the latter in quarantine, so the DFC client **215** broadcasts a *NOTIFICATION* alarm message (block **725**), concerning the violator node.

Referring to the exemplary scenario shown in **Figure 8D**, let it be assumed that there is a traffic flow originating from the source node **805a** and directed to the destination node **805b**, assuming that the node **805a** is not authorized, by the security policies defined for the MANET, to originate such traffic. Node **805c** is a direct neighbour of the source node **805a**, and node **805d** is a direct neighbour of the destination node **805b**; the nodes **805c** and **805d** are thus responsible of enforcing the security policies, blocking the traffic generated by the source node **805a**. It is assumed that the DFA client **120** resident on node **805c** does not enforce the security policies, letting the traffic coming from the source node **805a** pass through; the node **805c** is thus a security policies violator that has to be identified by the DFC mechanism. The DFC client **215** resident on node **805i** is the controller of DFA client **120** resident on the node **805m**. Inspecting the traffic exiting the node **805m**, the DFC client **215** resident on node **805i** detects that the traffic with IP address corresponding to the address IP_S of the source node **805a** is not authorized. Based on its routing table, the DFC client **215** determines that the hop count value for the source node **805a** is equal to 2, and that the MAC address MAC_in of the traffic entering the node **805m** does not

coincide with the MAC address MAC_S of the source node **805a**, being instead the MAC address of the node **805c**. The controller node **805i** checks whether, in the *TC* messages sent by the node **805c**, the IP address IP_S of the source node **805a** is included in the MPR selector set: thus, the DFA client **120** that has not enforced the security policies (the security policies violator) resides on node **805c**. In such a case, the node **805i**, not being a direct neighbour of the security policies violator node, broadcasts a *NOTIFICATION* alarm message.

Back to **Figure 7**, if the IP address IP_S of the source node originating the traffic is not included in the MPR selector set (exit branch **N** of block **740**) announced by the node with MAC address equal to MAC_in, then the DFC client **215** ascertains whether its MAC address coincides with the MAC address MAC_in of the traffic entering the controlled DFA client **120** (block **745**). If the two addresses coincides (exit branch **Y** of block **745**), the DFA client **120** that has not enforced the security policies resides on the node that precedes the node hosting the DFC client **215** along the route from the source node (IP address IP_S) to the destination node (IP address IP_D), and thus said DFA client **120** resides on a neighbouring node (a next hop) of the node where the DFC client **215** resides. In order to identify which of its neighbours has not enforced the security policies, the DFC client **215** searches, in the MPR selector set included in the *TC* messages sent by its neighbours, the IP address IP_S of the source node (block **750**). Then, if the IP address IP_S is found, the DFC client **215** checks how many of its neighbours announce the IP address IP_S in their MPR selector set: if only one of the neighbours announces the IP address IP_S in its MPR selector set (exit branch **Y** of block **755**), then such neighbour is the node where the DFA client **120** that violated the security policies resides: the DFC client **215**, residing on a node that is a next-hop of the violator node, directly puts the latter node in quarantine (block **720**); if instead more than one of the neighbour nodes announces the IP address IP_S, then the DFC client **215**, not being able to identify which is the node where the DFA client **120** that violated the security policies resides, broadcasts an alarm message, particularly an *ALERT* message (block **760**).

Considering the exemplary scenario depicted in **Figure 8E**, let the traffic originated by the source node **805a** and destined to node **805b** be considered, assuming that the node **805a** is not authorized, by the security policies defined for the MANET, to generate such traffic. Node **805c** is a direct neighbour of the source node **805a**, and node **805d** is a direct neighbour of the destination node **805b**. The two nodes **805c** and **805d** are thus responsible of enforcing the security policies, blocking the traffic generated by the node **805a**. Let it be assumed that the DFA client **120** resident on node **805c** does not enforce the security policies, letting the traffic originated by node **805a** pass through: the DFA client **120** resident on node **805c** is thus the security policies violator, that should be identified by the DFC mechanism. The DFC client **215** resident on node **805n** is the controller of the DFA client **120** resident on node **805p**; monitoring the traffic on node **805p**, the DFC client **215** resident on node **805n** detects that the traffic having IP address equal to the IP address IP_S of the source node **805a** is not authorized. Based

on its routing table, the DFC client **215** derives that the hop count for node **805a** is equal to 2, and that the MAC address MAC_in of the traffic entering the controlled DFA client **120** resident on node **805p** coincides with its own MAC address. In this case, the controller node **805n** can decree that the DFA client **120** violating the security policies resides on one of its neighbours, particularly on the preceding node along the route from the source node to the destination node. In order to identify which is the violator node, among its neighbours **805q**, **805c**, **805r**, the DFC client **215** resident on the controller node **805n** checks whether, in the *TC* messages sent by the neighbour nodes, there is the IP address IP_S of the source node **805a**. The nodes **805q** and **805r**, not being MPR nodes, do not send *TC* messages (in the drawing, the nodes that have been elected as MPR nodes are encircled). In the considered example, only the node **805c** sends *TC* messages containing the IP address IP_S of the source node **805a**, thus the DFA client **120** that has not enforced the security policies resides on node **805c**; the node **805n**, being a direct neighbour thereof, directly puts the violator node **805c** in quarantine.

Back to **Figure 7**, if the hop count is different from 2 (exit branch **N** of block **730**), the DFC client **215** checks whether the hop count is equal to 3 (block **765**).

In the affirmative case (exit branch Y of block **765**), the DFA client **120** that violated the security policies is not the one controlled by the considered DFC client **215**. The DFC client **215** checks if the IP address IP_S of the source node is included in the MPR selector set announced in the *TC* messages sent by the node having MAC address equal to MAC_in, *i.e.* the MAC address of the traffic entering the DFA client **120** controlled by the DFC client **215** considered (block **770**). In the affirmative case (exit branch Y of block **770**), the DFA client **120** that violated the security policies resides on the node that, along the route from the source node (IP address equal to IP_S) to the destination node (IP address equal to IP_D), precedes the node hosting the controlled DFA client **120**, *i.e.* the violator node is the node having MAC address equal to MAC_in. In this case, the DFC client **215** is not a next-hop of the violator node, and cannot directly put the violator node in quarantine; the DFC client **215** thus broadcasts an alarm message, particularly a *NOTIFICATION* message (block **725**) related to the violator node.

Looking at the exemplary scenario depicted in **Figure 8F**, let the traffic originating from source node **805a** and destined to destination node **805b** be considered, and let it be assumed that the source node **805a** is not authorized, by the security policies defined for the MANET, to generate such traffic. Node **805c** is a direct neighbour of the source node **805a**, and node **805d** is a direct neighbour of the destination node **805b**; the two nodes **805c** and **805d** are responsible of enforcing the security policies, blocking the traffic generated by the node **805a**. It is assumed that the DFA client **120** resident on node **805c** does not enforce the security policies, letting the traffic generated by the source node **805a** pass through: the node **805c** is thus the security policies violator, that should be identified by the DFC mechanism. The DFC client **215** resident on node **805r** is the controller of the DFA client **120** resident on node **805s**. Monitoring the traffic on node **805s**, the DFC client **215** resident on node **805r** detects that the traffic with IP address

equal to that (IP_S) of the source node **805a** is not authorized; based on its routing table, the DFC client **215** resident on node **805r** determines that the hop count for the source node **805a** is equal to 3; the DFC client **215** also checks if the IP address of the source node **805a** is included in the MPR selector set announced in the *TC* messages sent by the node having MAC address MAC_in, from which the traffic entering the controlled node **805s** comes. The violator node **805c**, having MAC address MAC_in, is thus the node that precedes the controlled node **805s**. The DFC client **215** resident on node **805r** is not a next-hop of the violator node **805c**, thus it cannot directly put the violator node in quarantine: the node **805r** then broadcasts an alarm message, particularly a *NOTIFICATION* message related to the violator node **805c**.

Back to **Figure 7**, if the IP address IP_S of the source node is not included in the MPR selector set announced in the *TC* messages of the node having MAC address equal to the MAC address MAC_in of the traffic entering the DFA client **120** controlled by the DFC client **215** considered (exit branch **N** of block **770**), the DFC client **120** is not able to identify the violator node, and thus simply issues an *ALERT* message (block **760**).

If the hop count is higher than 3 (exit branch **N** of block **765**), the DFA client **120** that did not enforce the security policies is not that resident on the node controlled by the DFC client **215**, neither does it reside on the node that precedes the node where the DFA client **120** controlled by the considered DFC client **215** resides, along the route from the source node to the destination node. In this case, the DFC client **215**, not being able to determine which is the DFA client **120** that violated the security policies, performs no control on the MAC address MAC_in, and directly broadcasts an alarm message, particularly an *ALERT* message (block **760**). However, the DFA client **120** that did not enforce the security policies has in this case already been identified by the monitoring action performed by the nodes distant 1 or 2 hops from the source node; in fact, the filtering is performed only by the neighbour nodes of the node originating the unauthorized traffic. The control of the nodes more distant than 2 hops, which are not responsible of enforcing the security policies in respect of the source node, is scarcely useful for identifying the DFA client **120** that did not enforce the security policies. Such a control is nevertheless useful to detect unauthorized traffic in the MANET, and thus to alert the nodes along the route from the source node to the destination node, avoiding that such unauthorized traffic is routed further until these nodes receive a *NOTIFICATION* message (or a *QUARANTINE* message, as described later) generated as a consequence of the control performed by the DFC clients **215** controlling the DFA clients **120** resident on nodes that are closer to the node originating the unauthorized traffic.

Quarantine

As explained in the foregoing, each time a DFC client **215** detects or is informed by other DFC clients **215** that the DFA client **120** resident on a direct neighbouring node violates the security policies, the DFC client **215** puts the policy violator node in quarantine.

The schematic flowchart of **Figure 9** depicts the quarantine procedure, in an embodiment of the present invention.

Firstly, the DFC client **215** increments a first counter (hereinafter referred to as "FW counter") that is used to keep track of the number of consecutive times that the considered DFA client **120**, to be put in quarantine, has not properly enforced the security policies defined for the MANET (block **905**).

The DFC client **215** then checks if the value of the FW counter for the considered DFA client **120** has reached a predetermined threshold FwThr (block **910**); in the affirmative case (exit branch Y of block **910**), the DFC client **215** starts the global repair procedure in respect of that DFA client **120** (block **915**), as described in detail later on; in such a case, the DFC client **215** preferably broadcasts a *QUARANTINE* message with a flag set to indicate that the global repair procedure has been started for that DFA client **120**, so as to avoid that different DFC clients **215** start the global repair procedure for the same DFA client **120**.

Then, the DFC client **215** increments a second counter (hereinafter referred to as the "source counter"), that is used to keep track of the number of consecutive times that the source node (having IP address IP_S) originating the traffic that violates the security policies has attempted to generate unauthorized traffic (block **920**). The DFC client **215** checks (block **925**) if the value of the source counter has reached a predetermined threshold value SThr: in the affirmative case (exit branch Y of block **925**), the DFC client **215** starts the global repair procedure (block **930**) for the source node having IP address IP_S, and sets the respective flag to be included in a *QUARANTINE* message that is successively broadcast, so as to avoid that other DFC clients **215** start the global repair procedure in respect of that node.

The quarantine involves temporarily isolating the node hosting the DFA client **120** that did not enforce the security policies. The node hosting the DFC client **215** ceases announcing the violator node as its neighbour in *HELLO* messages it sends (block **935**), and activates a third counter, hereinafter referred to as "Qtimer" (block **940**). Then, the DFC client **215** broadcasts a *QUARANTINE* message (block **945**), so that the other network nodes are made aware of the security policies violation, and remove from their routing tables the routes involving the violator node. Until the value of the timer Qtimer reaches the prescribed threshold value (exit branch N of block **950**), the DFC client **215** continues to broadcast *HELLO* messages without announcing the violator node (**955**). When instead the value of the timer Qtimer reaches the preset threshold value (exit branch Y of block **950**), the DFC client **215** re-inserts the node hosting the violator DFA client **120** into the *HELLO* messages it broadcasts (block **960**), and resets the time Qtimer (block **965**): the quarantine is thus stopped, and the DFA client **120** that violated the security policies is re-inserted in the routing tables of the MANET nodes.

In the schematic flowchart of **Figures 10A** and **10B** the management of the alarm messages that have been mentioned in the foregoing and that are used in an embodiment of the present invention is

depicted.

As mentioned in the foregoing, the *NOTIFICATION* message is broadcasted to all the MANET nodes whenever a DFC client **215**, during the monitoring of the traffic on the controlled DFA client **120**, detects a violation of the security policies defined for the MANET, and identifies the violator DFA client **120** that has not enforced the security policies, but the DFC client **215** cannot directly put the violator node in quarantine, because the violator node is not a next-hop thereof.

The purpose of the *NOTIFICATION* message is:

- notifying to the other MANET nodes that a certain DFA client **120** has not properly enforced the security policies;
- ask the neighbouring nodes to put the violator node in quarantine; and
- ask the nodes that are along the route from the source node to the destination node to temporarily apply the violated security policies.

The structure of the *NOTIFICATION* message is depicted in **Figure 11**; the message includes:

- a field **1105** for carrying the IP address IP_S of the source node originating the data packets violating the security policies;
- a field **1110** for carrying the IP address IP_D of the destination node of the data traffic;
- a field **1115** for carrying the IP address IP_DFA of the node where the DFA client **120** that has not enforced the security policies resides;
- a field **1120** for carrying an identifier ID of the traffic session;
- a field **1125** for carrying an identifier RuleID of the security policy (firewalling rule) that has been violated; and
- a field **1130** for carrying the IP address IPNotification of the node where the DFA client **120** resides that is controlled by the DFC client **215** and that has detected traffic not compliant with the security policy identified by the identifier RuleID.

Referring to **Figure 10A**, each DFC client **215**, upon receiving an alarm message, checks (block **1005**) if the received message is a message of the type *NOTIFICATION*. In the affirmative case (exit branch **Y** of block **1005**), the DFC client **215** checks if the node where it resides is a direct neighbour of the node where the violator DFA client **120** resides (the node whose IP address IP_DFA is contained in the field **1115**) (block **1010**). In the affirmative case (exit branch **Y** of block **1010**), the DFC client **215** checks whether it has already put the violator node in quarantine (block **1015**). If the violator node has already been put in quarantine (exit branch **Y** of block **1015**), the DFC client **215** stops propagating the *NOTIFICATION* message (block **1020**). If on the contrary the violator node has not been put in quarantine yet (exit branch **N** of block **1015**), the DFC client **215** starts the quarantine procedure in respect of the violator node (block **1025**) and then it stops propagating the *NOTIFICATION* message (block **1020**).

If the node where the DFC client **215** that received the *NOTIFICATION* message is not a direct

neighbour of the violator node (exit branch **N** of block **1010**), then the DFC client **215** checks whether the node where it resides is on the route from the source node (IP address IP_S) to the destination node (IP address IP_D), by assessing if the IP address of the node where it resides coincides with the address IPNotification contained in the field **1130** of the received message (block **1030**). In the affirmative case (exit branch **Y** of block **1030**), the DFC client **215** assesses whether it has already applied the security policy (firewalling rule) that has been violated (identified by the identifier RuleID contained in the field **1125** of the received message) (block **1035**). If it has (exit branch **Y** of block **1035**), then it means that the DFC client **215** has already received previous *NOTIFICATION* alarm messages, possibly by other DFC clients **215** that control it, and thus it stops further propagating the *NOTIFICATION* message (block **1020**). Differently (exit branch **N** of block **1035**), it applies the violated security policy (identified by the identifier Rule ID) (block **1040**), and stops routing further data packets of the type identified by the identifier ID contained in the field **1120** of the received message. The DFC client **215** then checks (block **1045**) if it already received previous *NOTIFICATION* messages in respect of the same traffic session identifier by the identifier ID: in the negative case (exit branch **N** of block **1045**), it propagates further the message (block **1050**), otherwise (exit branch **Y** of block **1045**) it stops propagating the message (block **1020**).

If the DFC client **215** assesses that the node where it resides is not on the route from the source node to the destination node (exit branch **N** of block **1030**), then it checks whether it already received previous *NOTIFICATION* messages for the same traffic session (block **1045**); in the affirmative case (exit branch **Y** of block **1045**), it stops propagating the message (block **1020**), otherwise (exit branch **N** of block **1045**), it further propagates the message (block **1050**).

The *QUARANTINE* message is broadcasted to all the MANET each time a DFC client **215** detects that a controlled DFA client **120** has not enforced the security policies, and, being the node where it resides a next-hop of the node where the violator DFA client **120** resides, it directly puts the latter in quarantine. The *QUARANTINE* message is also broadcasted by a DFC client **215** that, having received a *NOTIFICATION* message, recognizes to be a direct neighbour of the violator DFA client **120**, and thus puts the latter in quarantine.

The purpose of the *QUARANTINE* message is that of informing the other nodes that a certain node has been put in quarantine, and thus it allows keeping the counters FW counter and source counter aligned.

The structure of the *QUARANTINE* message is depicted in **Figure 12**; the message includes:

- a field **1205** for carrying the IP address IP_S of the source node originating the data packets violating the security policies;
- a field **1210** for carrying the IP address IP_D of the destination node of the data traffic;
- a field **1215** for carrying the IP address IP_DFA of the node where the DFA client **120** that has not enforced the security policies resides;

- a field **1220** for carrying an identifier ID of the traffic session;

- a field **1225** for carrying an identifier RuleID of the security policy (firewalling rule) that has been violated;

- a field **1230** for carrying a flag CGR ("Client Global Repair") used to notify to the other nodes that a global repair procedure has been started for the violator DFA client **120** residing on the node of address IP_DFA; and

- a field **1235** for carrying a flag SGR ("Source Global Repair") used to notify to the other nodes that the global repair procedure has been started for the source node of address IP_S that generated the unauthorized traffic.

Referring to **Figure 10B**, the DFC client **215**, upon verifying that received alarm message is not a *NOTIFICATION* message (exit branch **N** of block **1005**), checks whether the message is a *QUARANTINE* message (block **1055**). In the affirmative case (exit branch **Y** of block **1055**) it checks whether the node where it resides is a direct neighbour of the node where the violator DFA client **120** resides, identified by the address IP_DFA contained in the field **1215** of the received message (block **1060**): if this is not the case (exit branch **N** of block **1060**), the DFC client **215** checks whether it already received previous *QUARANTINE* messages for the same session identified by the session identifier ID contained in the field **1220** of the received message (block **1065**), in which case (exit branch **Y** of block **1065**) it stops propagating the *QUARANTINE* message (block **1070**); if no *QUARANTINE* messages were previously received (exit branch **N** of block **1065**), the DFC client **215** increases the counters FW counter and source counter (block **1075**), stops forwarding the *NOTIFICATION* messages (block **1080**) received/generated in respect of the same session identified by the identifier ID, and propagates the *QUARANTINE* message to the other nodes (block **1081**).

If the DFC client **215** instead realizes to be a direct neighbour of the node where the violator DFA client **120** resides (exit branch **Y** of block **1060**), it checks whether the violator node has already been put in quarantine (block **1083**): if it has not (exit branch **N** of block **1083**), the DFC client **215** puts the violator node in quarantine (connector **B** and block **1025**), otherwise (exit branch **Y** of block **1083**) it stops propagating the *QUARANTINE* message (block **1070**).

ALERT alarm messages, differently from the *NOTIFICATION* and *QUARANTINE* messages, are sent only to the next hops of the node hosting a DFC client **215** each time the latter is more than 3 hops far from the source node of the unauthorized traffic, and only in case the DFC client **215** is not able to identify which is the DFA client **120** that has not enforced the security policies. The *ALERT* message is sent to inform a DFA client **120** controlled by the DFC client **215** about the presence of unauthorized traffic along the route from the source node to the destination node, so that the DFA client **120**can block the unauthorized traffic.

The structure of the *ALERT* message is depicted in **Figure 13**; the message includes:

- a field **1305** for carrying the IP address IP_S of the source node originating the data packets violating the security policies;

- a field **1310** for carrying the IP address IP_D of the destination node of the data traffic;

- a field **1315** for carrying the IP address IP_DFA of the node where the DFA client **120** that has not enforced the security policies resides;

- a field **1320** for carrying an identifier ID of the traffic session;

- a field **1325** for carrying an identifier RuleID of the security policy (firewalling rule) that has been violated;

- a field **1330** for carrying the IP address IP_Alert of the node hosting the DFA client **120** controlled by the DFC client **215** and that detected the presence of unauthorized traffic.

Upon receiving an *ALERT* message (exit branch **N** of block **1055**), the DFC client **215** checks whether it is on the route from the source node to the destination node, by comparing its own IP address with the address IP_Alert contained in the field **1330** of the received message (block **1085**). If the two addresses coincide (exit branch **Y** of block **1085**), then the DFC client **215** ascertains whether it has already applied the violated security policies (identified by the identifier RuleID) (block **1087**). If not (exit branch **N** of block **1087**), the security policy is applied (block **1089**), otherwise it means that previous *ALERT* messages were already received for the same session, and the message is thus ignored (block **1091**). In both cases, the DFC client **215** waits for the next *NOTIFICATION* and *QUARANTINE* messages (block **1093**). A DFC client **215** that, upon receiving the *ALERT* message, assesses not to be along the route from source node to the destination node (exit branch **N** of block **1085**) ignores the *ALERT* message (block **1091**) and keeps on listening next *NOTIFICATION* and *QUARANTINE* messages (block **1093**).

Global repair mechanism

The global repair mechanism involves the intervention of the DFC server **205**, which is responsible of centrally managing the DFC mechanism, each time a stronger countermeasure against the security policies violator nodes is requested, in respect of nodes that have repeatedly violated the security policies, not enforcing them properly. The global repair mechanism is used whenever the quarantine did not succeed.

The global repair mechanism may involve the exclusion from the MANET of a node where the violator DFA client **120** resides, identified during the local repair procedure; the node excluded from the MANET may be requested to re-authenticate itself in order to be re-admitted to the MANET.

The global repair procedure in respect of a generic network node is started by the first DFC client **215** whose counter FW counter for that node reaches the predetermined threshold: in such a case, the DFC client **215**, during the local repair procedure, sets the CGR flag in the *QUARANTINE* message it broadcasts. The DFC clients **215** that receive the *QUARANTINE* message with the CGR flag set are informed of the fact that some node already started the global repair procedure, and thus they reset the

respective counters FW counter in respect of the same DFA client **120**.

The global repair procedure involves the transmission to the DFC server **205** of a *GLOBAL REPAIR REQUEST* message, whose structure is pictorially shown in **Figure 14A**. The message, globally denoted **1400**, includes:

- a field **1405** for carrying the IP address IP_S of the source node of the data packets that violate a certain security policy;

- a field **1410** for carrying the IP address IP_DFA of the node where the violator DFA client **120** resides, that has not enforced the security policy; and

- a field **1415** for carrying the identifier RuleID of the violated security policy (firewalling rule).

Upon receiving a *GLOBAL REPAIR REQUEST* message, the DFC server **205** verifies whether a violation actually occurred. This is done by an interaction with the DFA server **110**. The latter:

- checks the correspondence between the security policy identified by the identifier RuleID contained in the received *GLOBAL REPAIR REQUEST* message, and one of the security policies in a list of security policies configured for the MANET;

- ensures that the security policy identified by the identifier RuleID has actually been sent to the source node of the unauthorized traffic and the node where the violator DFA client **120** resides, specified in the received *GLOBAL REPAIR REQUEST* message (the DFA server **110** keeps a list of the active MANET nodes, and, for each of them, an indication of the current security policies (general and specific) applied by the node).

If the DFA server **110** finds that the DFA client **120** identified by the IP address IP_DFA in the received *GLOBAL REPAIR REQUEST* message actually violated the security policies, the DFA server **110** removes the IP address IP_DFA of that node (and thus the firewalling rule defined for it) from its database. Then, the DFA server **110** sends to the authentication server of the MANET the identifier IP_DFA of the node to be de-authenticated. The DFA server **110** also sends to the DFC server **205** a *GLOBAL REPAIR ACCEPT* message, by means of which it requests the exclusion of the node identified by the IP address IP_DFA from the MANET. The structure of the *GLOBAL REPAIR ACCEPT* message is schematically depicted in **Figure 14B**: the message, globally denoted **1450**, contains a field **1455** for carrying the IP address IP_DFA of the node to be excluded from the list of DFC clients **215**, and a field **1460** for carrying a signature of the DFC server **205**. The signature is included in the *GLOBAL REPAIR ACCEPT* message by the DFC server **205**, which then sends it to the node that sent the *GLOBAL REPAIR* REQUEST message; the *GLOBAL REPAIR ACCEPT* message is then broadcasted in the MANET, so that the nodes can exclude the node identified by the IP address IP_DFA, blocking any kind of traffic it generated, exception made for authentication traffic for the re-authentication of the node in the MANET. At the same time, the DFA server **205** informs every node of the exclusion of the DFA client **120** resident on the excluded node; this is done through the periodic polling mechanism by which the DFA clients **120** get from

the DFA server **110** the security policies to be enforced.

The same global repair procedure is also applied when the counter source counter reaches the predetermined threshold.

§ § § § §

In addition to the detection of the improper enforcement of the security policies, the present invention can also be used for detecting and contrasting selfish nodes, which tend to participate to the MANET in such a way that they only route their own data packets, discarding the data packets originating from/directed to other nodes. Exploiting the same mechanisms described in the foregoing (selection of the controlled DFA clients **120** and of the controller DFC clients **215**, local and global repair mechanisms), it is possible to isolate the selfish nodes, thereby promoting cooperation between the nodes.

Referring to **Figure 2**, each node acts as a controller (DFC client **215**) of a certain DFA client **120**, through the constant monitoring of the traffic entering and exiting the controlled DFA client **120**. In order to detect and manage a selfish behaviour of a controlled DFA client **120**, the controller DFC client **215** checks that the packets related to the routing protocol and the application-layer packets are properly routed (complying the security policies defined for the MANET).

In particular, referring to **Figure 15**, for each data packet **1500** entering and/or exiting a controlled DFA client **120**, it is first assessed whether the packet complies with the security policies defined for the MANET (block **1505**); in case of violation of the security policies (exit branch **Y** of block **1505**), this is managed as described in the foregoing, first through the local repair mechanism (block **1510**), and then through the global repair mechanism (block **1520**), if the counters FW counter and/or source counter have reached the predetermined threshold (block **1515**). If the packet complies with the security policies defined for the MANET (exit branch **N** of block **1505**), the selfish node detection logic is applied (block **1525**): for each packet entering the controlled DFA client **120**, having destination IP address IP_D different from the IP address IP_DFA of the node where the controlled DFA client **120** resides, the presence of a corresponding packet exiting the node is checked by the controller DFC client **215**. In case the entering packets are discarded (not let pass through), the controller DFC client **215** decrees a selfish behaviour (exit branch **Y** of block **1525**), and applies a simplified local repair mechanism (**1530**): the controller DFC client **215** increases a dropped packets counter associated with the controlled DFA client **120**; if the dropped packets counter reaches a selfish node detection threshold (set by the controller DFC client **215** according to the security policies of the MANET), then the controller DFC client **215** broadcasts a *SELFISH NODE QUARANTINE* message, schematized in **Figure 16** and including:

- a field **1605** carrying an IP address IP_SELF of the selfish node;
- a field **1610** carrying the MAC address of the selfish node;
- a field **1615** carrying the identifier RuleID of the violated firewalling rule; and
- a field **1620** carrying a flag indicating whether the global repair procedure has already been

started.

Each DFC client **215** which, upon receiving the *SELFISH NODE QUARANTINE* message, realizes to be a direct neighbour of the selfish node, puts the latter in quarantine, stopping to announce the selfish node as its neighbour in the *HELLO* messages, and ignores routing messages coming from the selfish node. In this way, the distant DFC clients, not receiving information about the selfish node, remove it from their routing tables. Similarly to the case of violation of a security policies described above, the quarantine is temporary, and lasts a predetermined time (for example, a timer is used for this purpose), after which the nodes that are direct neighbours of the selfish node restart announcing the selfish node as their neighbour; the selfish node is thus re-inserted in the routing tables of all the nodes of the MANET.

The *SELFISH NODE QUARANTINE* message is also exploited to keep the counters FW counter of the controller DFC clients aligned; these counters are used, as described above, for handling the global repair procedure (a same counter is used for starting the global repair procedure, irrespective of whether a violation of a security policy or a selfish behaviour are detected).

The invention has been here described making reference to an exemplary embodiment thereof, those skilled in the art will recognize that several modifications to the described embodiment, as well as other embodiments are conceivable, without departing from the scope of the invention, defined in the appended claims.

CLAIMS

1. A method of enforcing security policies in a mobile *ad-hoc* network, comprising:

- entrusting at least one first network node, along a data traffic route from a data traffic origin node to a data traffic destination node, with the enforcing of predefined security policies on said data traffic;

- entrusting at least one second network node, distinct from said first network node, with the control of the enforcement of the security policies by said first network node.

2. The method of claim 1, wherein said at least one first network node comprises a network node being a direct neighbour of the origin node.

3. The method of claim 2, wherein said at least one first network node further comprises a network node being a direct neighbour of the destination node.

4. The method of any one of the preceding claims, further comprising:

- providing at least one central security policies distribution server configured to distribute the predefined security policies to the network nodes.

5. The method of any of claims 1 to 4, comprising:

- having the at least one second network node control a compliance with the predefined security policies of the data traffic passing through at least one third network node along said data traffic route.

6. The method of claim 5, further comprising:

having the at least one second network node selecting the said at least one third network node among a set of multipoint relay nodes thereof.

7. The method of claim 6, wherein said having the at least one second network node selecting the at least one third network node comprises selecting the at least one third network node among two or more respective multipoint relay nodes as either:

- the multipoint relay node through which the lowest number of nodes distant two hops can be reached; or

- in case two or more of the multipoint relay nodes of the second network nodes allow reaching a same, lowest number of nodes distant two hops, the multipoint relay node that has in turn elected the lowest number of multipoint relay nodes.

8. The method of claim 7, wherein said having the at least one second network node selecting the at least one third network node further comprises

- in case two or more of the multipoint relay nodes of the second network nodes have elected a same, lowest number of multipoint relay nodes, choosing the at least one third network node at random among said two or more of the multipoint relay nodes of the second network node that have elected the lowest number of multipoint relay nodes.

9. The method of claim 6, 7 or 8, wherein in case the at least one second network node is included in a loop, said selecting the at least one third network node comprises selecting, among the multipoint relay nodes of the second network node, the network node that, starting from the second network node and passing through a node in the loop having lowest network address, allows reaching a first node announced in a multipoint relay selector set in a transmission control protocol message.

10. The method of any one of claims 5 to 9, further comprising:

- in case the second network node detects a security policies violation:

- having the second network node ascertain whether the third network node is the first network node;

- if the third network node is the first network node, having the second network node undertake an action directed to at least temporarily exclude the first network node from the network;

- if the third network node is not the first network node, having the second network node:

- identifying the first network node, and

- in case said first network node is a direct neighbour of the second network node, undertaking an action directed to at least temporarily exclude the first network node from the network;

- in case said first network node is not a direct neighbour of the second network node, or the first network node cannot be identified, broadcasting an alarm message adapted to inform the other network nodes of the security policies violation.

11. The method of claim 10, wherein said at least temporarily exclude from the network comprises causing the first network node to be removed from routing tables of the network nodes in the data traffic routes involving the first network node.

12. The method according to claim 10, further comprising:

- causing the first network node to be de-authenticated from the network after a predetermined number of said temporarily exclude.

13. The method according to any of claims 5 to 12, further comprising:

- having the second network node controlling whether the third network node properly routes data traffic entering thereinto, and

- in the negative case, having the second network node undertake an action to temporarily exclude the third network node from the network.

14. The method of claim 13, wherein said controlling whether the third network node properly routes data traffic entering thereinto comprises:

- having the second network node ascertain that, for each data packet entering the third network node and destined to a destination network node different from the third node, there is a corresponding data packet exiting the third node.

15. A system for enforcing security policies in a mobile *ad-hoc* network, comprising:

- at least one first network node, along a data traffic route from a data traffic origin node to a data traffic destination node, entrusted with the enforcing of predefined security policies on said data traffic;

- at least one second network node, distinct from said first network node, entrusted with the control of the enforcement of the security policies by said first network node.

16. The system of claim 15, wherein said at least one first network node comprises a network node being a direct neighbour of the origin node.

17. The system of claim 16, wherein said at least one first network node further comprises a network node being a direct neighbour of the destination node.

18. The system of any one of claims 15 to 17, further comprising at least one central security policies distribution server configured to distribute the predefined security policies to the network nodes.

19. The system of any of claims 15 to 18, wherein the at least one second network node is configured to control a compliance with the predefined security policies of the data traffic passing through at least one third network node along said data traffic route.

20. The system of claim 19, wherein:

the at least one second network node is adapted to select the at least one third network node among a set of a multipoint relay nodes thereof.

21. The system of claim 20, wherein said at least one second network node is adapted to select the at least one third network node among two or more respective multipoint relay nodes as either:

- the multipoint relay node through which the lowest number of nodes distant two hops can be reached; or

- in case two or more of the multipoint relay nodes of the second network nodes allow reaching a same, lowest number of nodes distant two hops, the multipoint relay node that has in turn elected the lowest number of multipoint relay nodes.

22. The system of claim 21, wherein said at least one second network node is adapted to select the at least one third network node randomly among two or more of the multipoint relay nodes of the second network node that have elected the lowest number of multipoint relay nodes.

23. The system of claim 20, 21 or 22, wherein in case the at least one second network node is included in a loop, the second network node is adapted to select, among the multipoint relay nodes of the second network node, the network node that, starting from the second network node and passing through a node in the loop having lowest network address, allows reaching a first announced node announced in a multipoint relay selector set in a transmission control protocol message.

24. The system of any one of claims 19 to 23, wherein:

- in case the second network node detects a security policies violation, the second network node is adapted to assess whether the third network node is the first network node, and:

- in the affirmative case, to undertake an action directed to at least temporarily exclude the first network node from the network;

- in the negative case:

- to identify the first network node;

- in case said first network node is a direct neighbour of the second network node, undertake an action directed to at least temporarily exclude the first network node from the network;

- in case said first network node is not a direct neighbour of the second network node, or the first network node cannot be identified, to broadcast an alarm message adapted to inform the other network nodes of the security policies violation.

25. The system of claim 24, wherein said at least temporarily exclude from the network comprises causing the first network node to be removed from routing tables of the network nodes in the data traffic routes involving the first network node.

26. The system of claim 25, wherein said at least temporarily excluding from the network further comprises causing the network node responsible of the security policies violation to be de-authenticated from the network after the first network node has been removed a predetermined number times from routing tables of the network nodes in the data traffic routes involving the first network node.

27. The system according to any of claims 19 to 26, wherein the second network node is further adapted to control whether the third network node properly routes data traffic entering thereinto, and, in the negative case to undertake an action to temporarily exclude the third network node from the network.

28. The system of claim 27, wherein the second network node is adapted to ascertain that, for each data packet entering the third network node and destined to a destination network node different from the third node, there is a corresponding data packet exiting the third node.

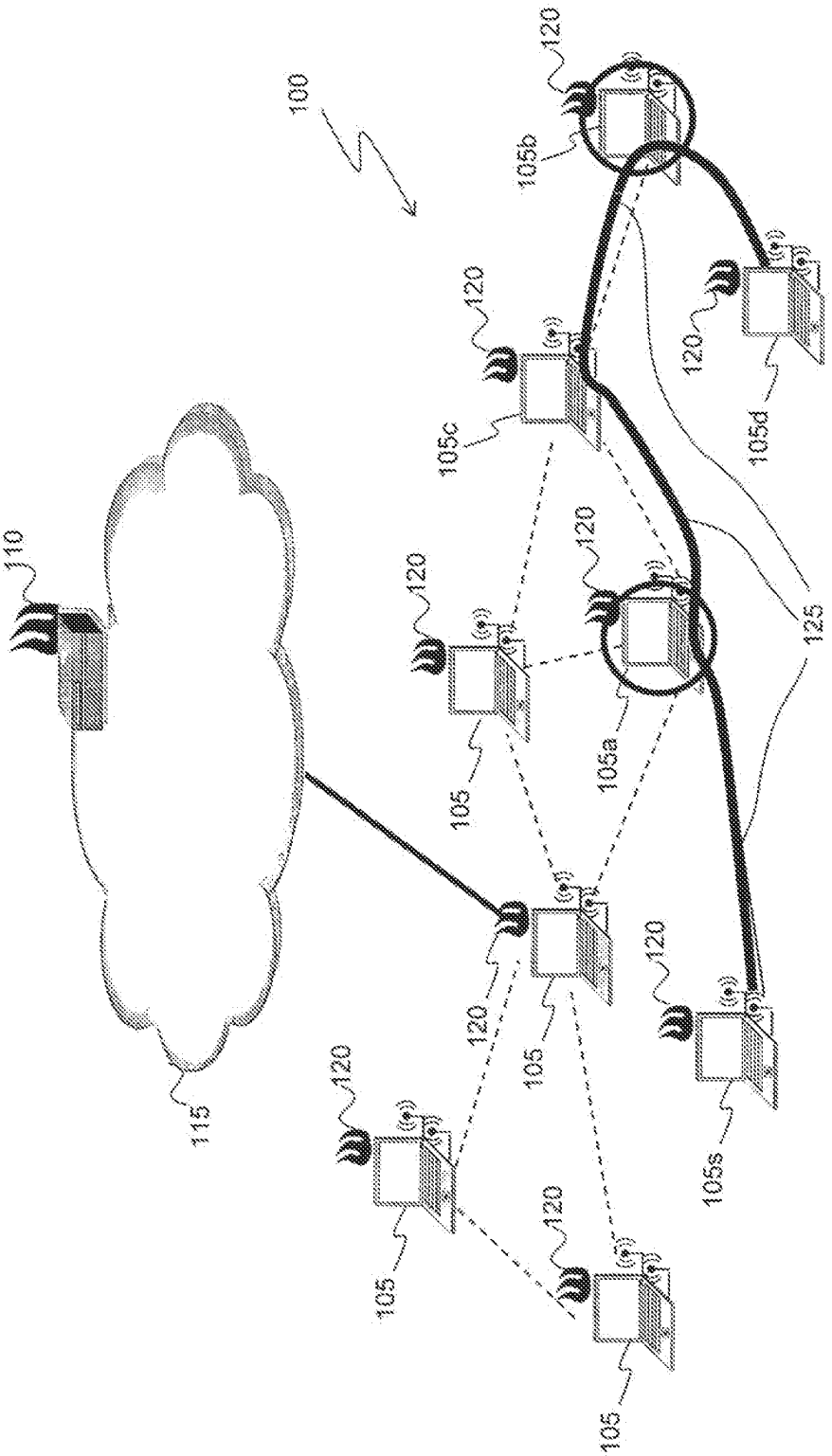


FIG. 1

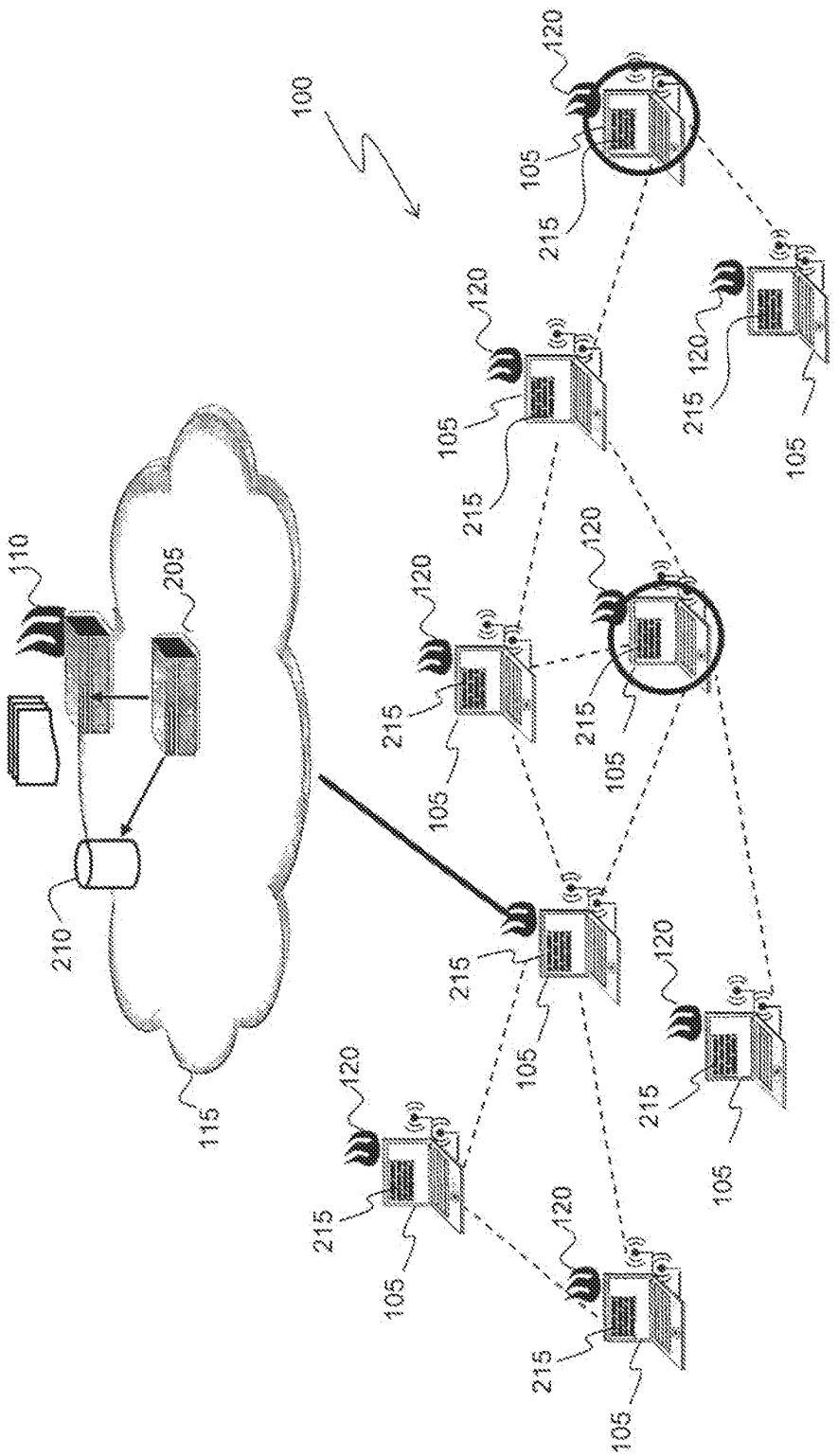


FIG. 2

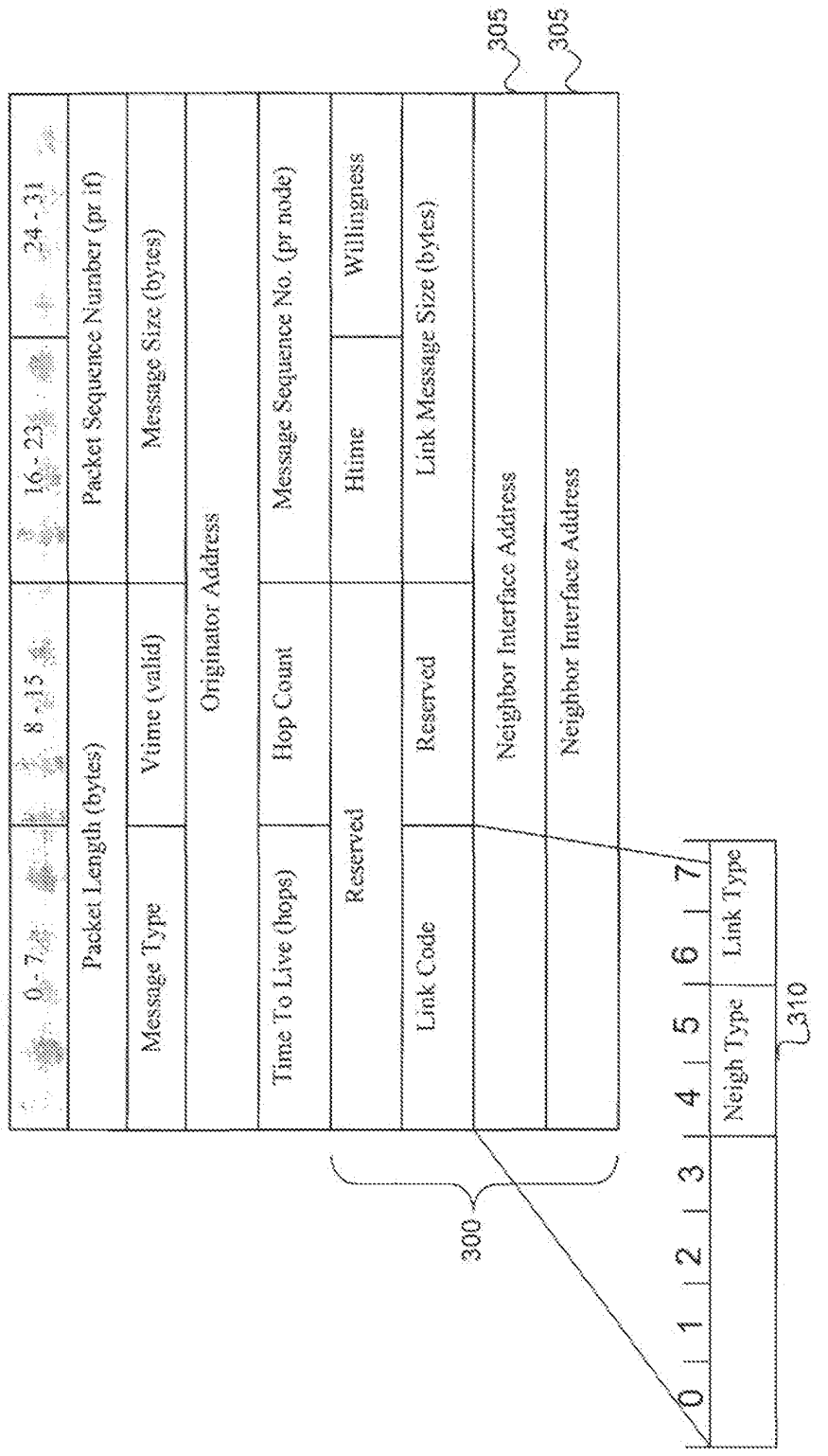

0 - 7
8 - 15
16 - 23
24 - 31
Packet Length (bytes)
Packet Sequence Number (pr if)
Message Type
Vtime (valid)
Message Size (bytes)
Originator Address
Time To Live (hops)
Hop Count
Message Sequence No. (pr node)
Reserved
Htime
Willingness
Link Code
Reserved
Link Message Size (bytes)
Neighbor Interface Address
Neighbor Interface Address
300
305
305
0 1 2 3 4 5 6 7
Neigh Type
Link Type
310

FIG. 3

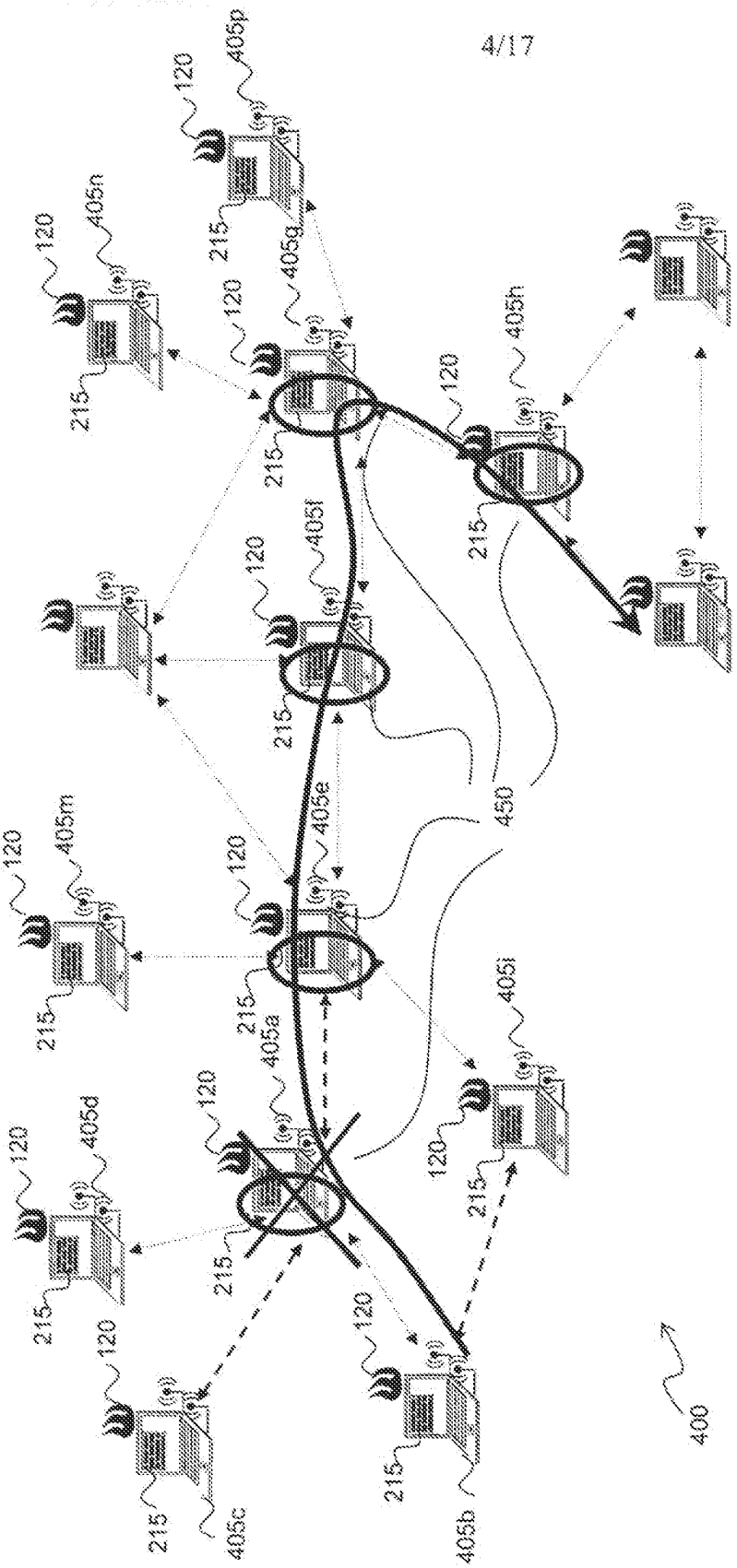

405a
405b
405c
405d
405e
405f
405g
405h
405i
405m
405n
405p
120
215
450
400

FIG. 4

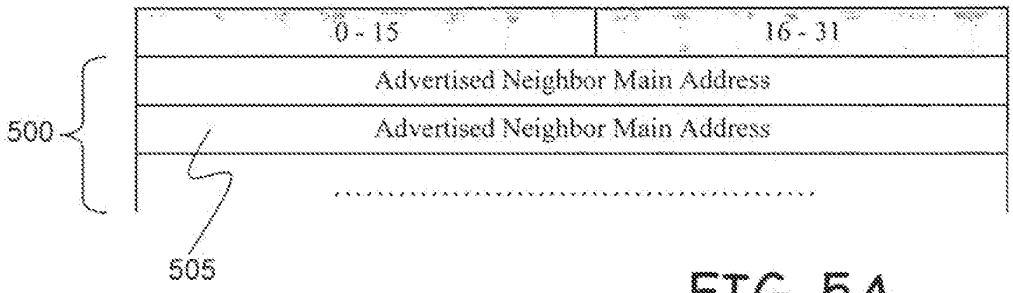


FIG. 5A

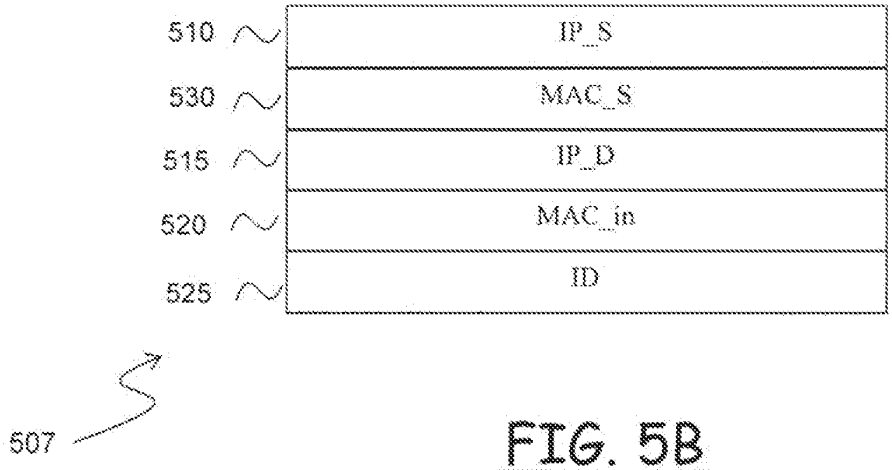


FIG. 5B

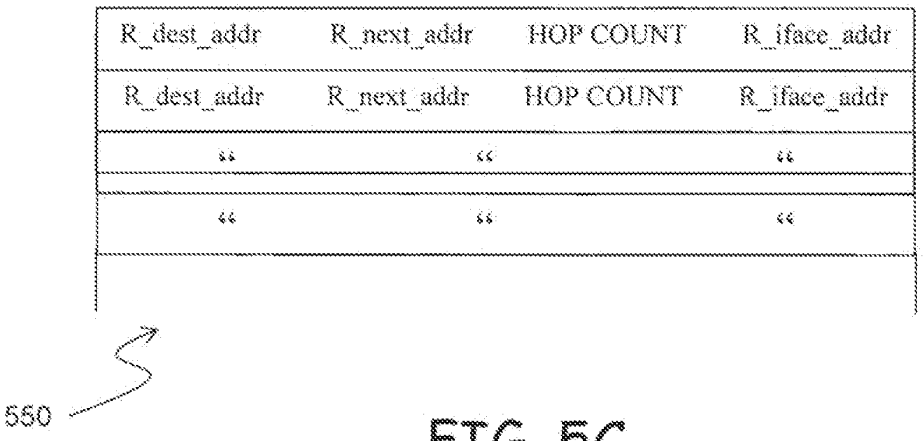


FIG. 5C

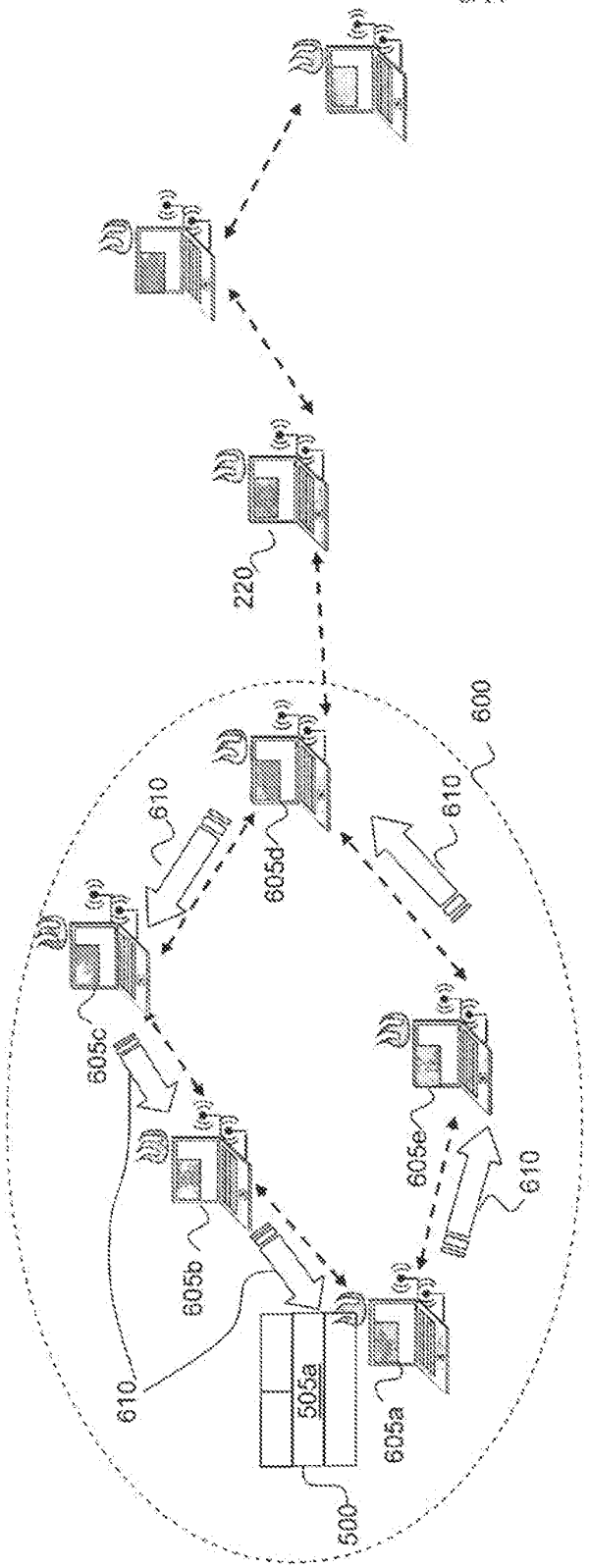


FIG. 6

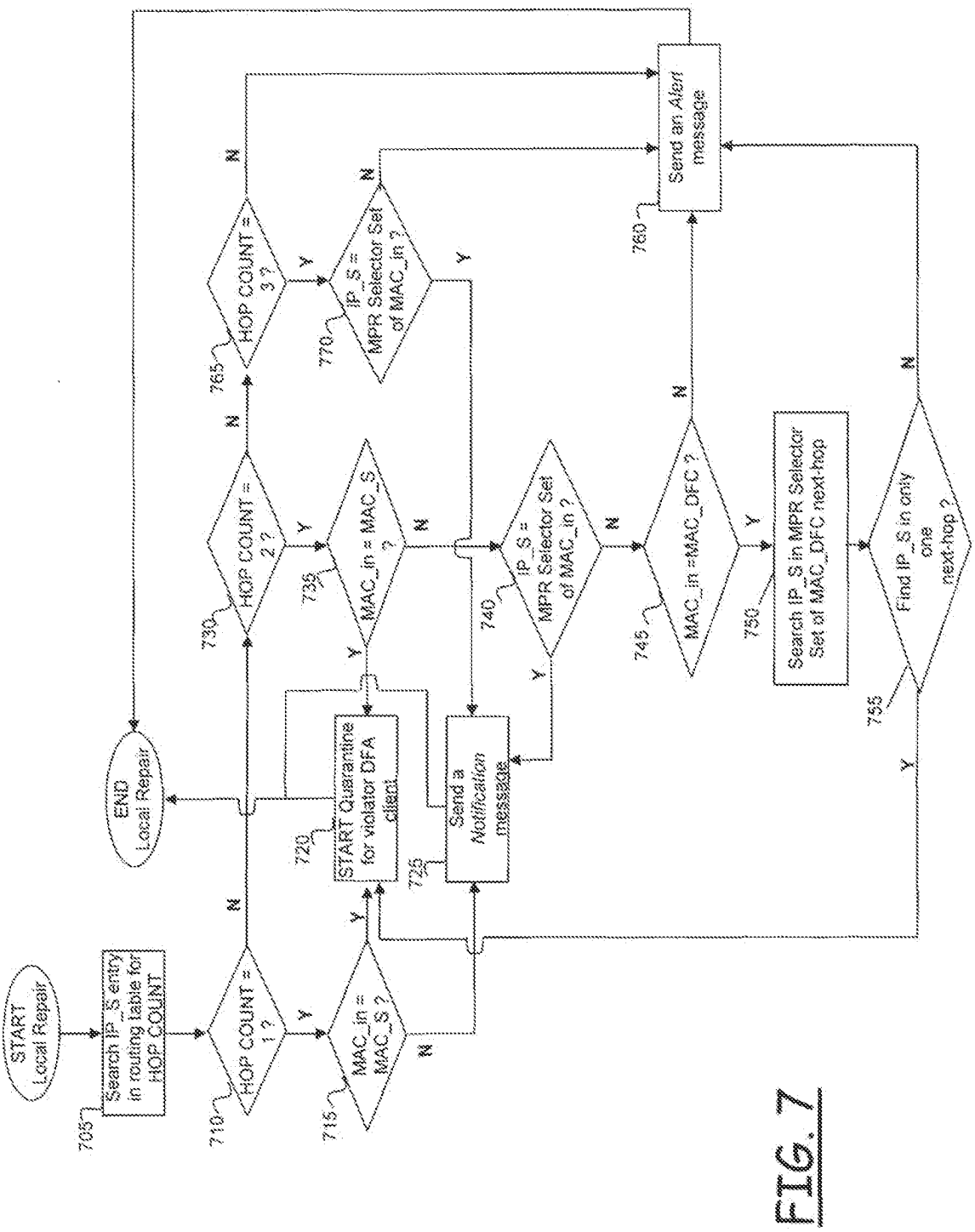

START Local Repair
Search IP_S entry in routing table for HOP COUNT
HOP COUNT = 1 ?
MAC_in = MAC_S ?
HOP COUNT = 2 ?
MAC_in = MAC_S ?
HOP COUNT = 3 ?
IP_S = MPR Selector Set of MAC_in ?
IP_S = MPR Selector Set of MAC_in ?
MAC_in =MAC_DFC ?
Find IP_S in only one next-hop ?
Search IP_S in MPR Selector Set of MAC_DFC next-hop
START Quarantine for violator DFA client
Send a Notification message
Send an Alert message
END Local Repair
705
710
715
720
725
730
735
740
745
750
755
760
765
770
Y
N

FIG. 7

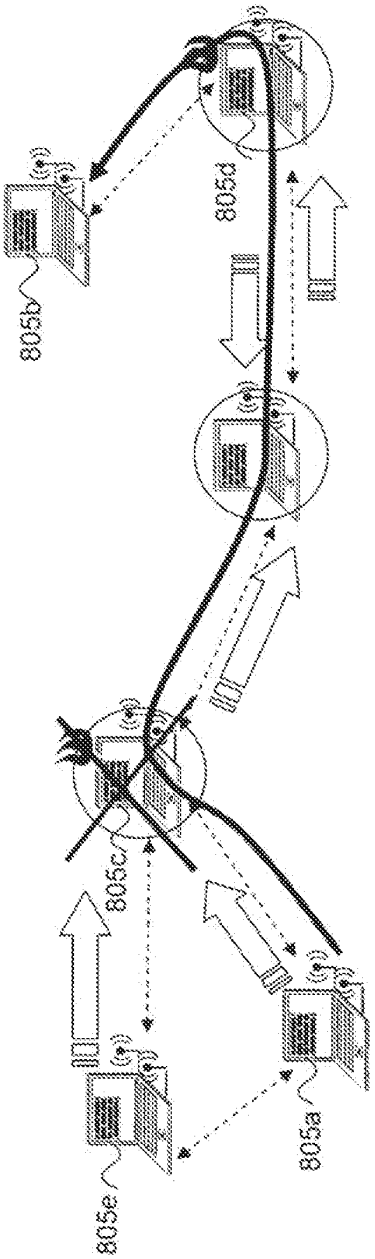


FIG. 8A

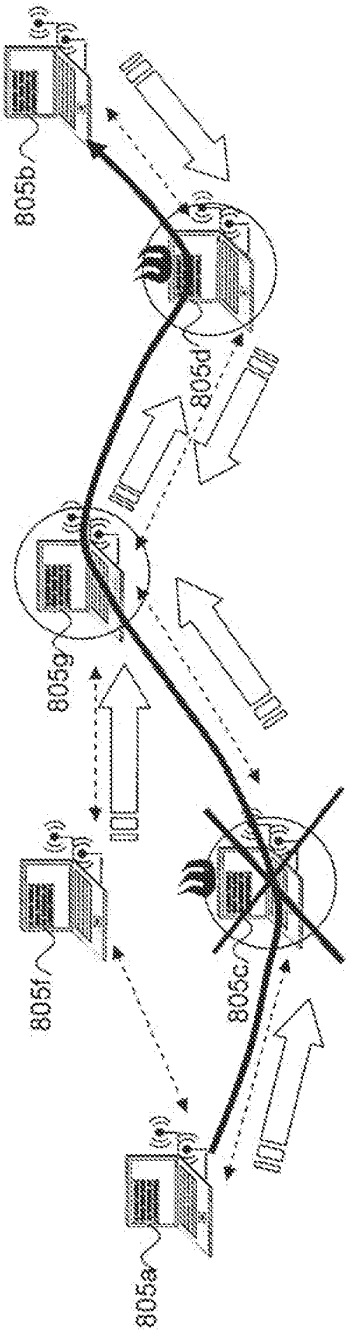


FIG. 8B

FIG. 8C

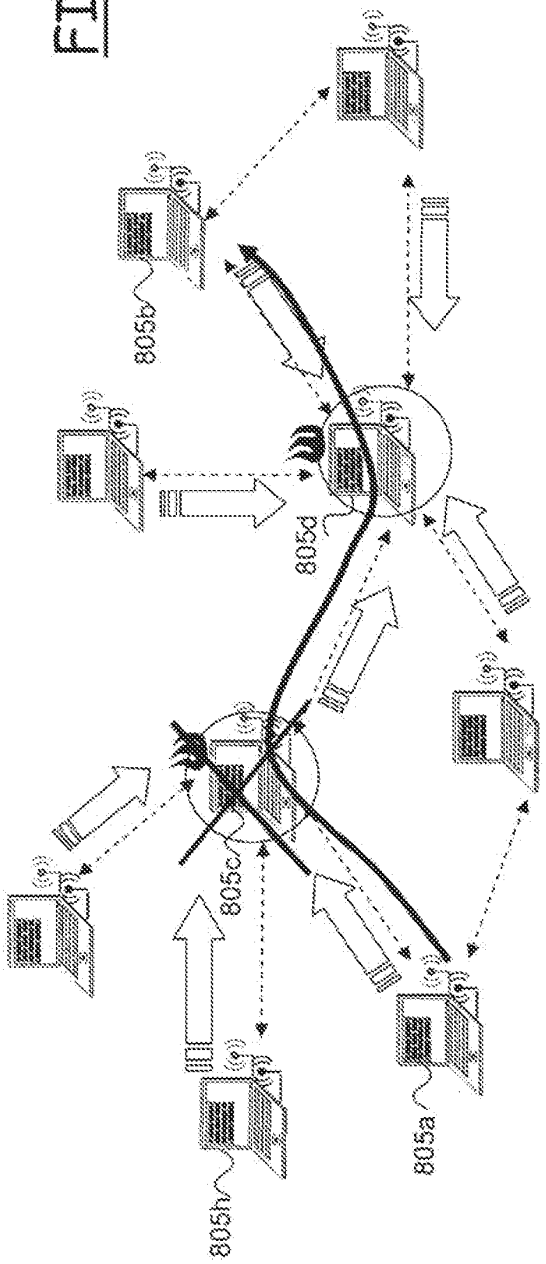
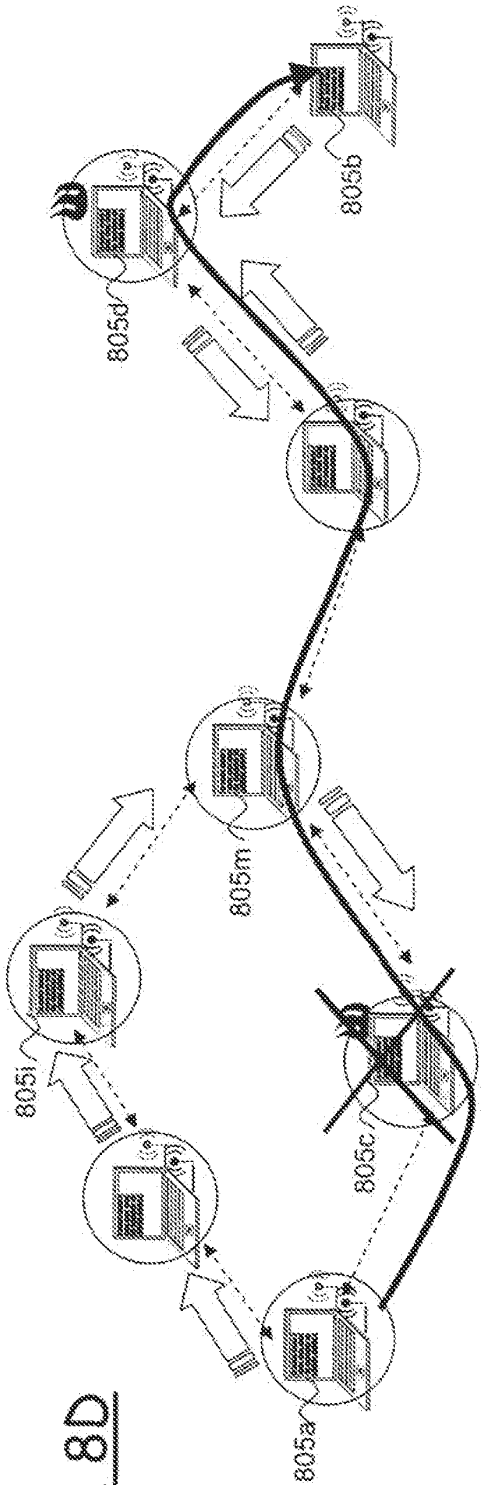


FIG. 8D



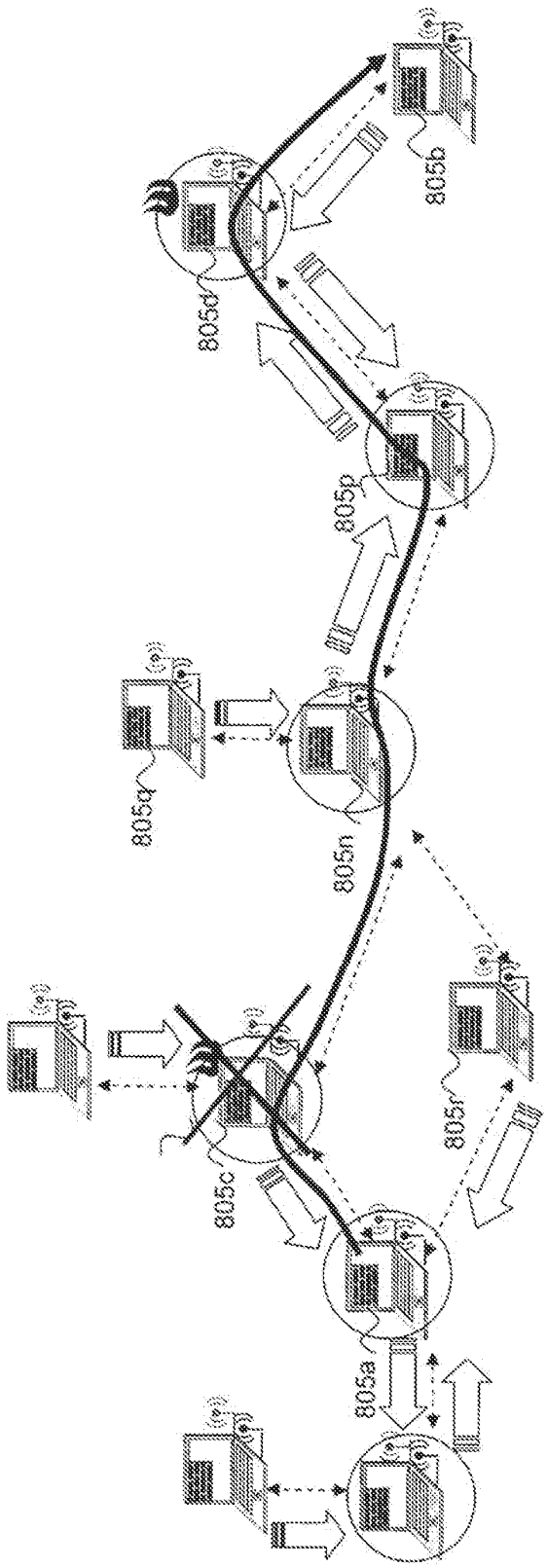


FIG. 8E

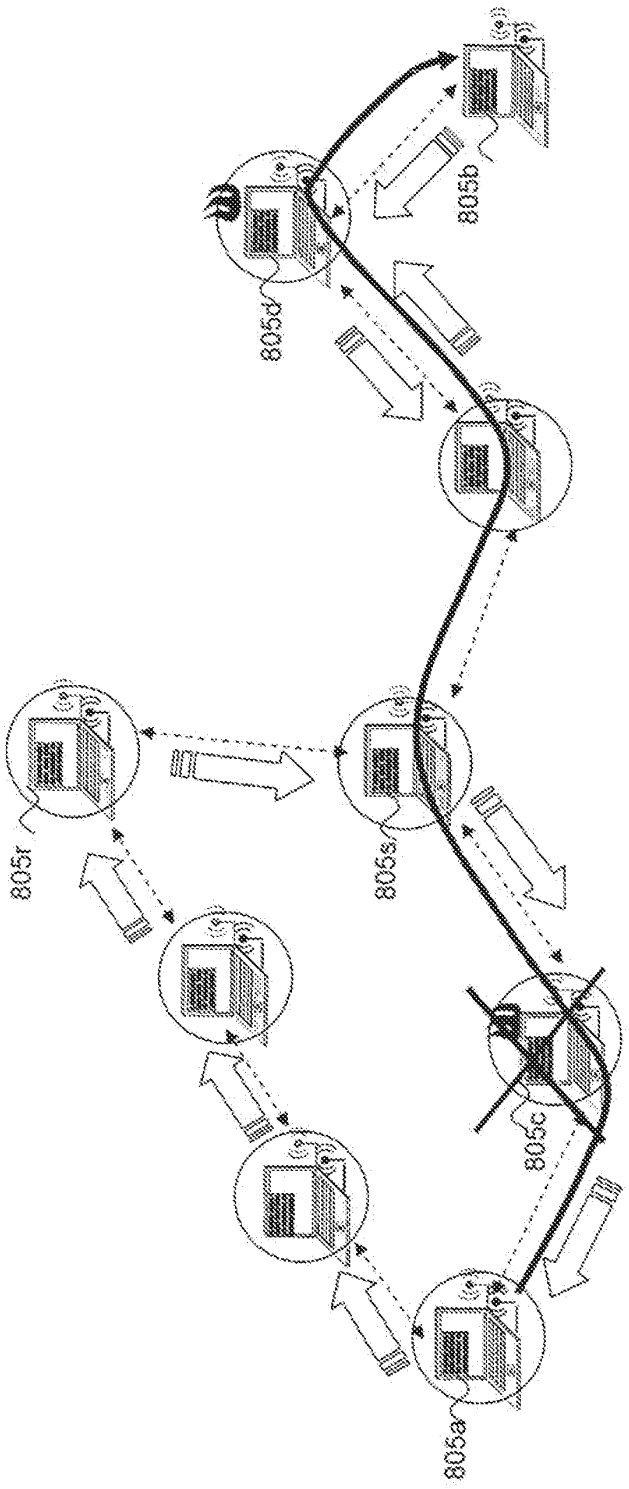


FIG. 8F

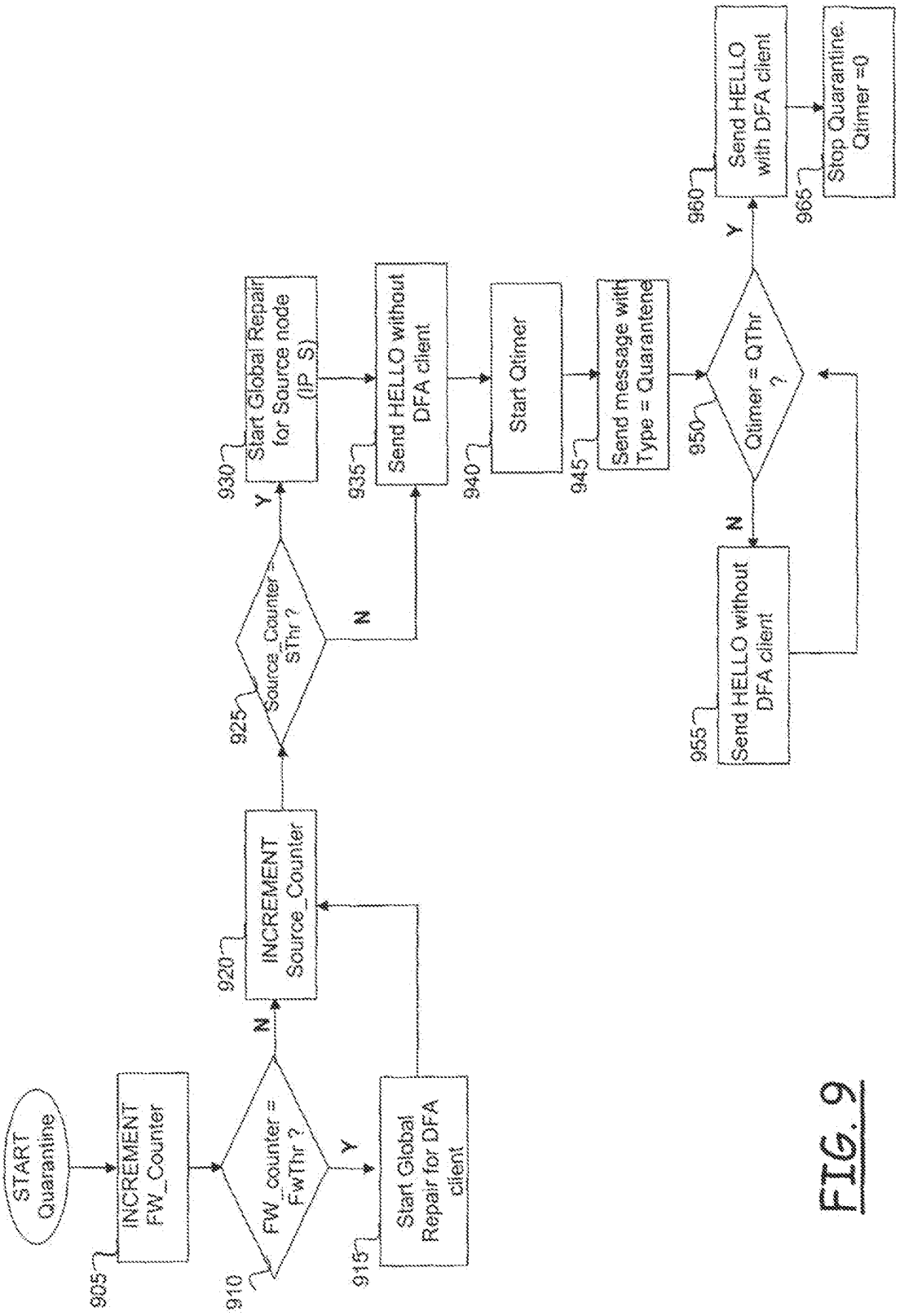

START Quarantine
INCREMENT FW_Counter
905
FW_counter = FwThr ?
910
Y
N
Start Global Repair for DFA client
915
INCREMENT Source_Counter
920
Source_Counter = SThr ?
925
Y
N
Start Global Repair for Source node (IP_S)
930
Send HELLO without DFA client
935
Start Qtimer
940
Send message with Type = Quarantene
945
Qtimer = QThr ?
950
Y
N
Send HELLO with DFA client
960
Stop Quarantine. Qtimer =0
965
Send HELLO without DFA client
955

FIG. 9

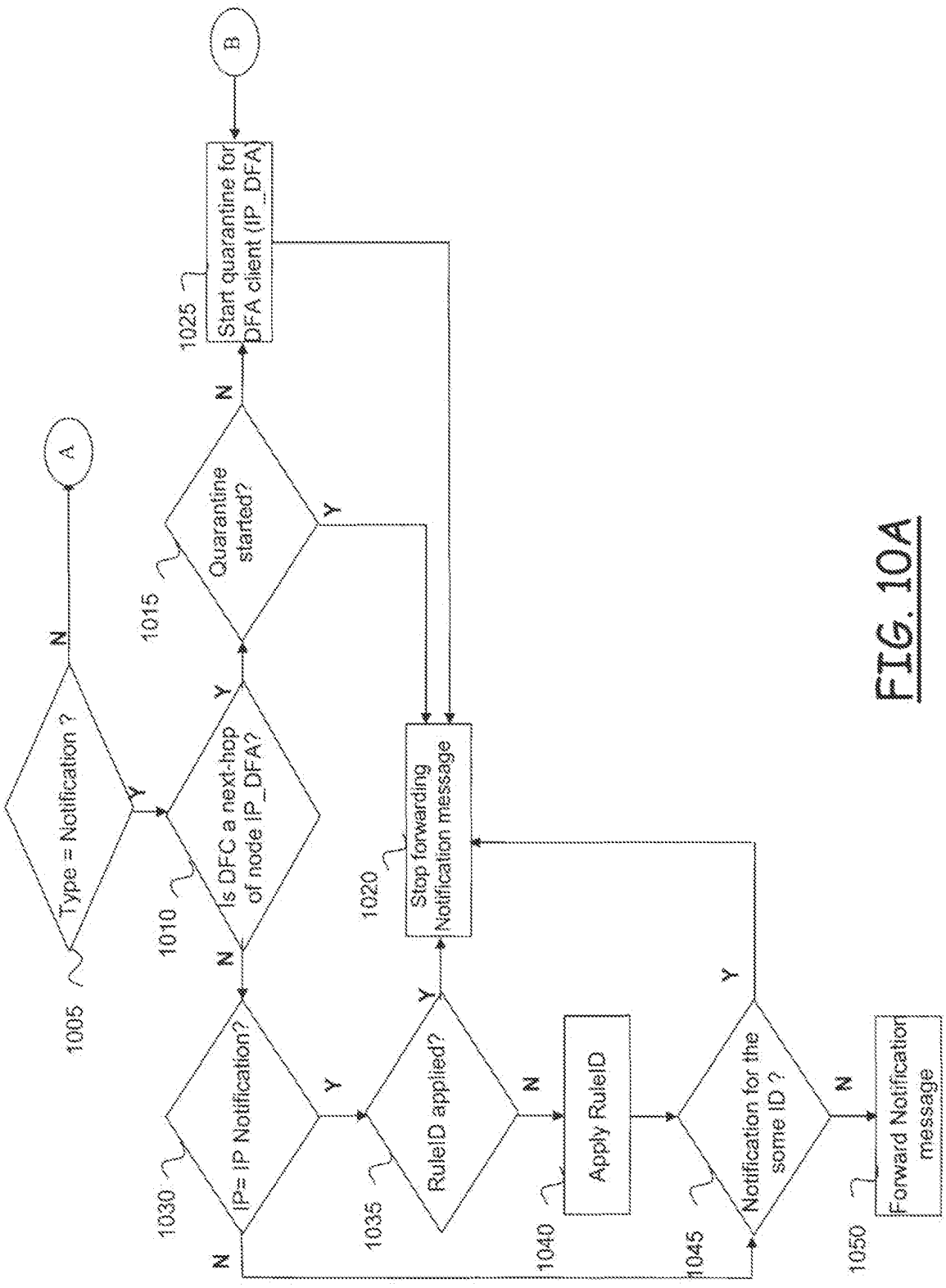

A
B
Type = Notification ?
1005
Y
N
Is DFC a next-hop of node IP_DFA?
1010
Y
N
Quarantine started?
1015
Y
N
Start quarantine for DFA client (IP_DFA)
1025
Stop forwarding Notification message
1020
IP= IP Notification?
1030
Y
N
RuleID applied?
1035
Y
N
Apply RuleID
1040
Notification for the some ID ?
1045
Y
N
Forward Notification message
1050

FIG. 10A

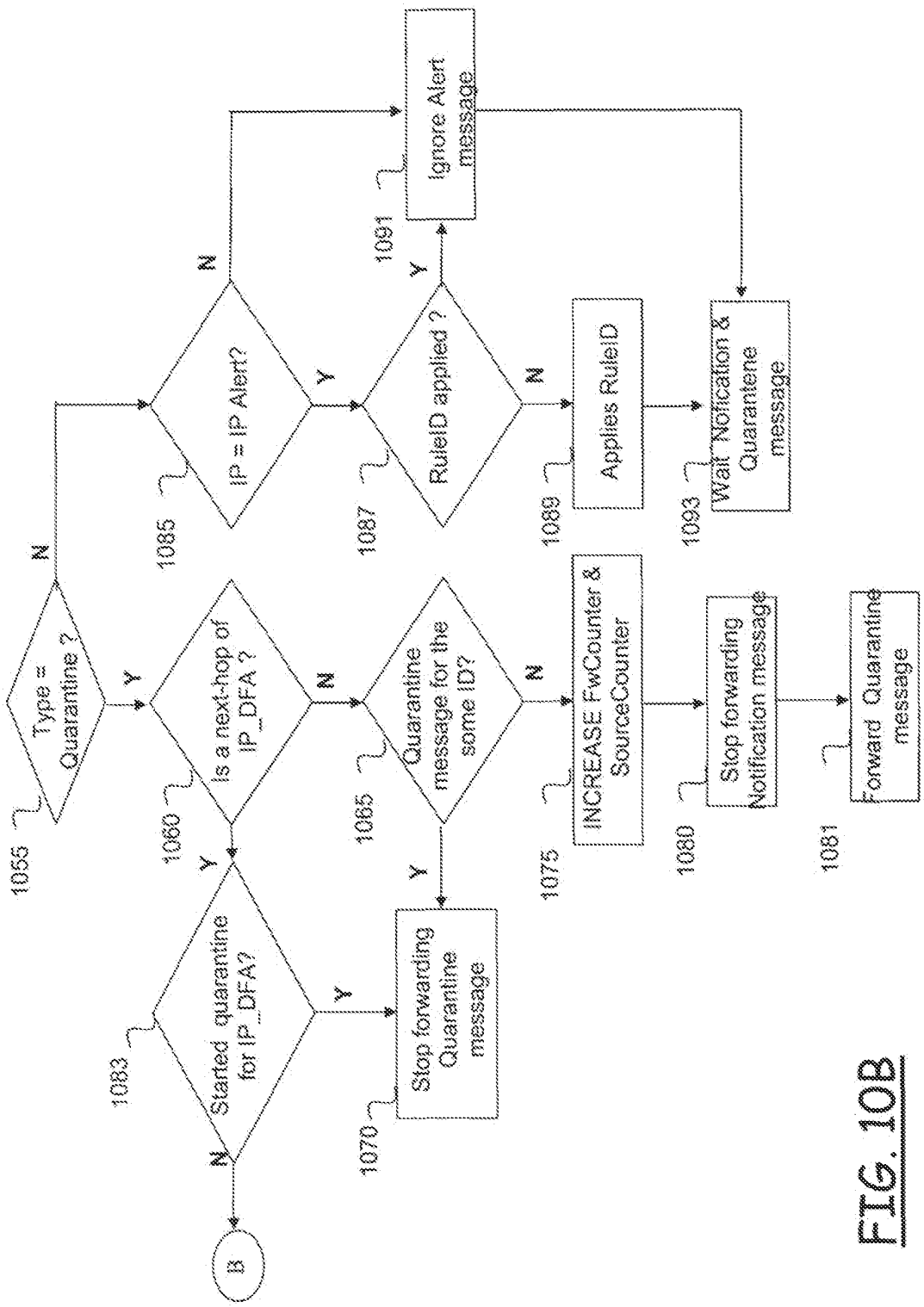

Type = Quarantine ?
1055
Y
N
Is a next-hop of IP_DFA ?
1060
Y
N
Started quarantine for IP_DFA?
1083
Y
N
B
Stop forwarding Quarantine message
1070
Quarantine message for the some ID?
1065
Y
N
INCREASE FwCounter & SourceCounter
1075
Stop forwarding Notification message
1080
Forward Quarantine message
1081
IP = IP Alert?
1085
Y
N
RuleID applied ?
1087
Y
N
Applies RuleID
1089
Wait Notication & Quarantene message
1093
Ignore Alert message
1091

FIG. 10B

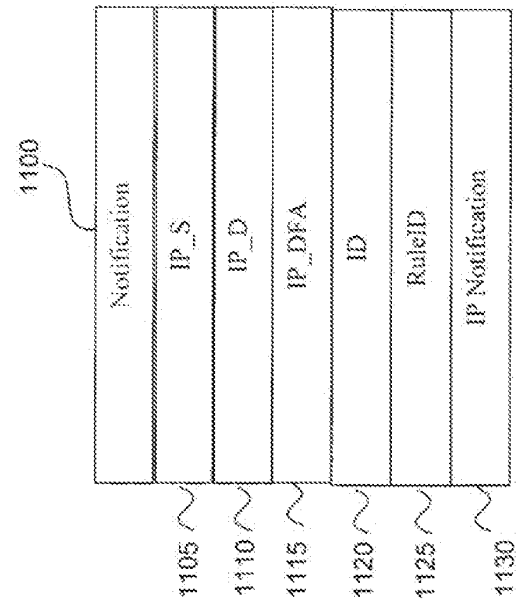


FIG. 11

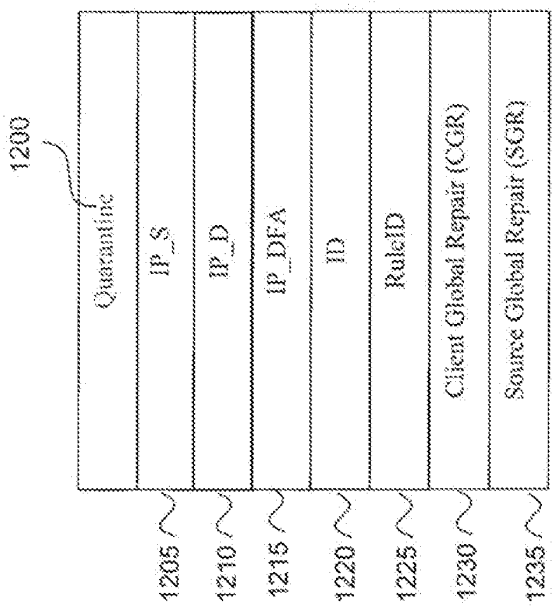


FIG. 12

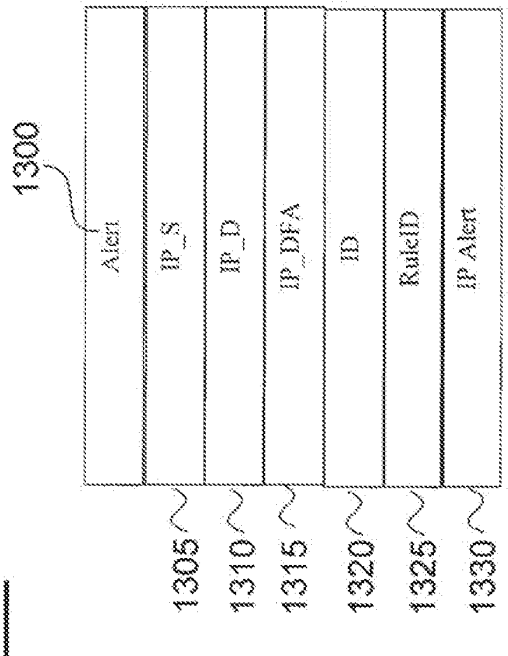


FIG. 13

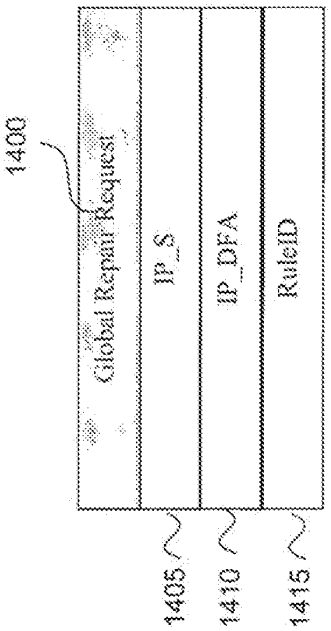


FIG. 14A

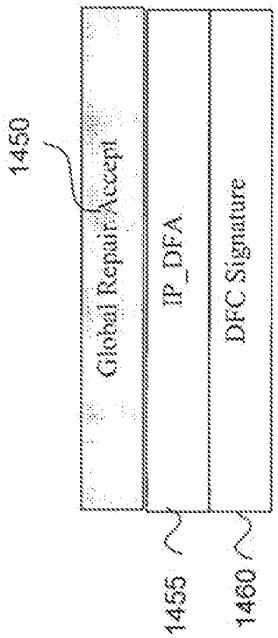


FIG. 14B

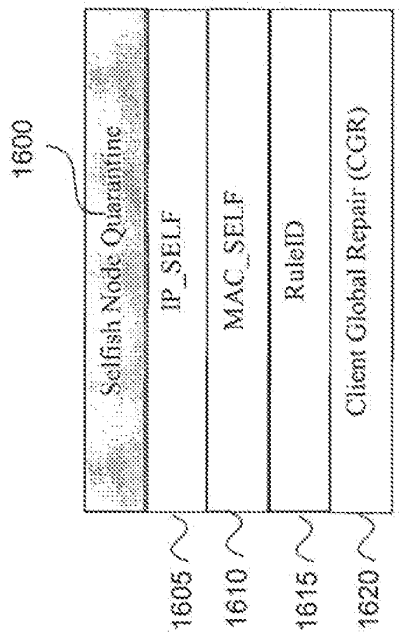
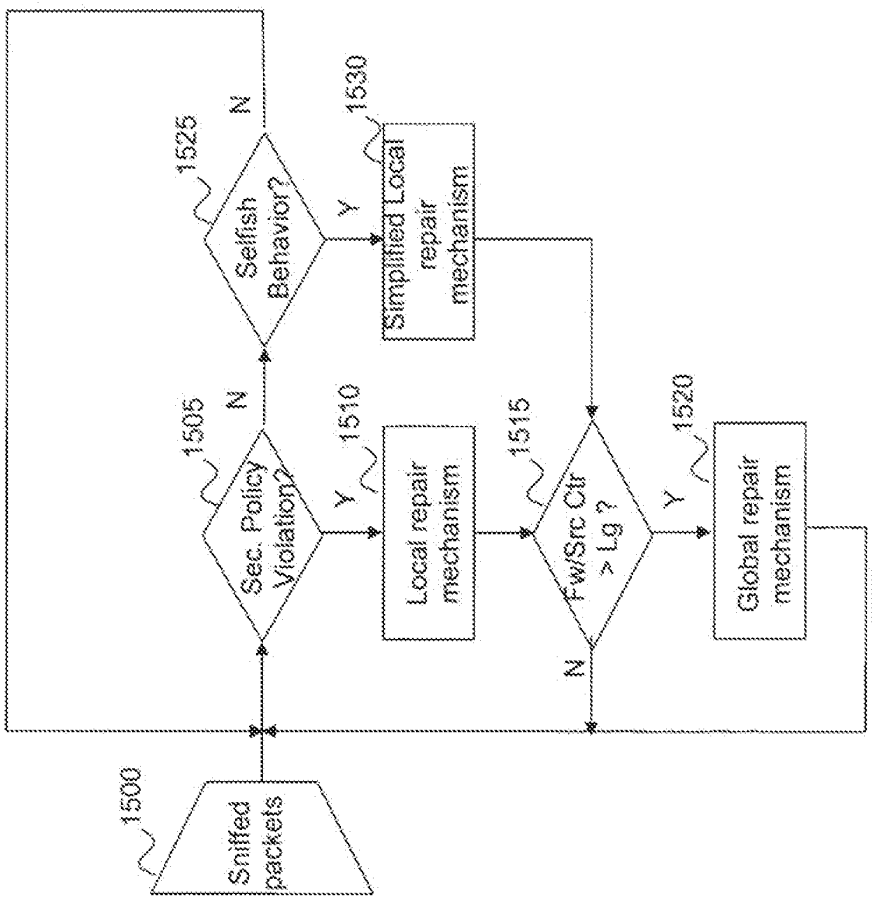


FIG. 16

FIG. 15


1500
Sniffed packets
1505
Sec. Policy Violation?
N
Y
1510
Local repair mechanism
1515
Fw/Src Ctr > Lg ?
N
Y
1520
Global repair mechanism
1525
Selfish Behavior?
N
Y
1530
Simplified Local repair mechanism

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/012606

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

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

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DJORDJEVIC I ET AL: "An architecture for dynamic security perimeters of virtual collaborative networks" NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 2004. NOMS 2004. IEEE/IFIP SEOUL, KOREA APRIL 19-23, 2004, PISCATAWAY, NJ, USA,IEEE, 19 April 2004 (2004-04-19), pages 249-262, XP010712587 ISBN: 0-7803-8230-7	1-9, 13-23, 27,28
A	the whole document	10-12, 24-26

-/--

[X] 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 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 August 2007	29/08/2007

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	Olaechea, Javier

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/012606

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RAMANUJAN R ET AL: "Intrusion-resistant ad hoc wireless networks" MILITARY COMMUNICATIONS CONFERENCE, MILCOM 2002. PROCEEDINGS. ANAHEIM, CA, OCT. 7 - 10, 2002, IEEE MILITARY COMMUNICATIONS CONFERENCE, NEW YORK, NY : IEEE, US, vol. VOL. 1 OF 2, 7 October 2002 (2002-10-07), pages 890-894, XP010631893 ISBN: 0-7803-7625-0	1-9, 13-23, 27,28
A	the whole document	10-12, 24-26
X	DJORDJEVIC I ET AL: "Architecture for secure work of dynamic distributed groups" CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE, 2004. CCNC 2004. FIRST IEEE LAS VEGAS, NV, USA 5-8 JAN. 2004, PISCATAWAY, NJ, USA,IEEE, 5 January 2004 (2004-01-05), pages 495-500, XP010696877 ISBN: 0-7803-8145-9	1-9, 13-23, 27,28
A	the whole document	10-12, 24-26
A	P.G. ARGYROUDIS,D.O'MAHONY: "Secure Routing for Mobile Ad hoc Networks"[Online] 23 August 2006 (2006-08-23), XP002447263 Retrieved from the Internet: URL:http://www.ctvr.ie/docs/EN_Pubs/secure-adhoc-routing.pdf> [retrieved on 2007-08-17] Sections 3, 4 and 5	1-28
A	CLAUSEN T ET AL: "Optimized Link State Routing Protocol (OLSR)" IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, October 2003 (2003-10), XP015009408 ISSN: 0000-0003 cited in the application the whole document	1-28

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
14 February 2008 (14.02.2008)

(10) International Publication Number
WO 2008/017837 A1

(51) International Patent Classification:
H04M 1/2745 (2006.01) *H04M 1/725* (2006.01)

(21) International Application Number:
PCT/GB2007/003011

(22) International Filing Date: 8 August 2007 (08.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0615844.8 9 August 2006 (09.08.2006) GB

(71) Applicant (*for all designated States except US*): **SYMBIAN SOFTWARE LIMITED** [GB/GB]; 2-6 Boundary Row, London SE1 8HP (GB).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): **SPOONER, David** [GB/GB]; Symbian Software Limited, 2-6 Boundary Row, London SE1 8HP (GB).

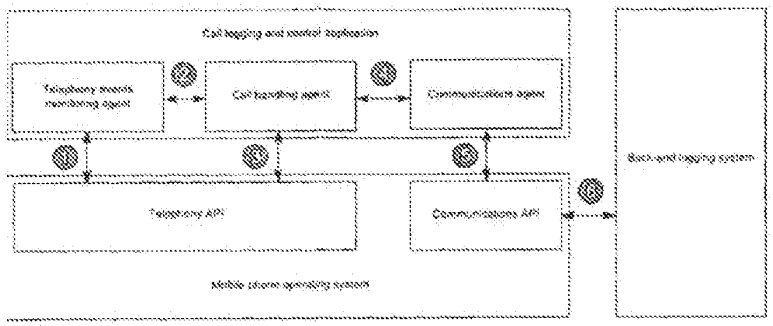
(74) Agent: KOEN, Sophia; Symbian Software Limited, 2-6 Boundary Row, London SE1 8HP (GB).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, 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, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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*

(54) Title: MOBILE COMMUNICATIONS DEVICE WITH EVENT LOGGING



(57) Abstract: This invention relates to a mobile communications device programmed to provide logging of telephony activity. In one implementation, the programme provides near real-time notification and control of mobile phone calls. The notification is to a back-end logging system.

WO 2008/017837 A1

MOBILE COMMUNICATIONS DEVICE WITH EVENT LOGGING

FIELD OF THE INVENTION

This invention relates to a mobile communications device programmed to provide logging of phone call activity. In one implementation, the programme provides near real-time notification and control of mobile phone calls. The notification is to a back-end logging system.

Current mobile telephones typically include a log of incoming and outgoing phone calls, generally indicating which incoming calls were answered and which were missed.

Many mobile telephones also offer users a function to automatically divert all incoming calls to voicemail, without ringing.

Techniques are also known for barring outgoing phone calls to certain destinations, such as high-rate phone lines.

It is desirable to provide a phone call monitoring and logging system that provides enhanced control of call activity and enhanced logging capabilities, to enable functions to be automated and to improve a user's experience.

SUMMARY

In accordance with a first aspect of the present invention there is provided a mobile communications device programmed with: (a) a telephony events monitoring agent, registered with a telephony API provided by an operating system of the device so as to receive notifications of any telephony related events; (b) a call handling agent for processing telephony events received from the telephony events monitoring agent and arranged to communicate with the telephony API based on a configured call handling policy, the call handling agent being arranged to store logs of device telephony activity; (c) a communications agent that uses a communications API of the operating system to communicate the logs stored by the call handling agent to a back-end logging system using available communications means provided by the communications API.

In accordance with a second aspect of the invention there is provided a method of enabling a mobile communications device to log calls, comprising the steps of: (a) a telephony events monitoring agent registering with a telephony API provided by an operating system of the mobile device in order to receive notifications of any telephony related events; (b) a call handling agent processing telephony events received from the telephony events monitoring agent and arranged to communicate with the telephony API based on a configured call handling policy, the step of processing including storing logs of device call activity; (c) a communications agent using a communications API of the operating system to communicate the logs stored by the call handling agent to a back-end logging system using available communications means provided by the communications API.

In accordance with a third aspect of the invention there is provided a system for enabling mobile device calls to be logged, the system comprising multiple mobile communications devices as defined above and a back-end logging system arranged to receive logs from the mobile devices.

Preferred features of the invention are set out in the dependent claims.

DESCRIPTION OF DRAWINGS

The invention will now be described by way of example with reference to the accompanying drawing, in which:

Figure 1 shows a call handling arrangement including a back-end logging system.

DETAILED DESCRIPTION

Embodiments of the present invention enable a mobile communications device to intelligently control the handling of calls and telephony events, by reporting telephony events to a logging system and implementing a call handling policy using that logging system. A call handling agent receives input from a telephony events monitoring agent, and the call handling agent communicates with a telephony API of the device to enforce a policy for handling calls and telephony events.

In the preferred embodiment, a method is provided by which 1) telephony events on mobile devices (e.g. making and receiving calls, conferencing, missed calls) can be

reported to a back-end logging system (which also receives logs from landline telephones), and 2) telephony activities on the device can be controlled based on a dynamic policy (call barring for outgoing and incoming calls, call cost control, etc.).

The following series of steps explains how an embodiment of the invention can be used on a mobile telephone. The steps are illustrated in Figure 1.

1) The "Telephony events monitoring agent" registers with the mobile phone operating system's Telephony API in order to receive notifications of any telephony related events:
    a. Outgoing call;
    b. Incoming call;
    c. Call status change – dialling, answering, connecting, ringing, connected, hanging up, hold, etc.
2) The "Telephony events monitoring agent" notifies the "Call handling agent" of telephony events received from the Telephony API.
3) The "Call handling agent" processes messaging events received from the "Telephony events monitoring agent" and responds to the Telephony API based on configured policy. Call handling policy may cover the following functions:
    a. Log outgoing phone call and content;
    b. Log incoming phone call and content;
    c. Automatically answer incoming calls;
    d. Automatically disconnect incoming calls;
    e. Automatically disconnect outgoing calls;
    f. Determine response based on dynamic properties including message content or properties, date, time, location (GSM network location and/or GPS), phone call origin or destination, associated contact information (in business contacts group or personal contacts group, etc.), diary information, selected profile, etc.;
    g. Capture additional state information such as network information (network name, GSM country, area and cell, signal level), device status (memory consumption, battery level, selected profile);
    h. Determine schedule for communicating log information to the "Back-end logging system" (after each call event, every specific amount of time, at

specific times, once a specific amount of log information has been captured, etc.);

i. Invoke alternative communications client on device (e.g. automatically disconnect outgoing phone call and invoke voice-over-IP client to initiate call).

4) The "call handling agent" communicates call logging information to the "Communications agent" based on scheduling policy. Information may be augmented with additional device information such as device identification (IMEI, IMSI), network information (network type and identification, country, area and cell information). The "Communications agent" notifies the "Call handling agent" of any call handling policy modification requests received from the "Back-end logging system".

5) The "Communications agent" uses the mobile phone operating system's communications API to communicate with the "Back-end logging system" using available communications means provided by the communications API:

a. A TCP/IP communication protocol (HTTP, FTP, SMTP, etc.)

b. A GSM communication channel such as SMS, MMS.

6) The "Back-end logging system" may control the "Message handling agent" policy by communicating policy modifications using available communications means via the "Communications agent".

The back-end logging system is preferably provided remotely from the device. In this arrangement, the relatively small quantity of storage memory available on current mobile phones need not be impacted by the logged telephony data. Large quantities of storage memory can be provided on remote servers without reducing the available storage on the mobile device. However, it is possible to implement an embodiment of the invention in which the back-end logging system is provided in the device itself. Such an arrangement would have certain advantages: for example, the time taken for data or instructions to be transferred between the logging system and the communications agent could be much shorter.

The communication between the communications agent on the mobile telephone and the logging system preferably involves delivering all recent events logged by the call handling agent to the logging system, and then deleting them from the call handling

agent's local log. Once received at the back-end logging system, the recent events are compared with those already stored at the logging system, and updates are made accordingly.

The call handling policy defines the manner in which calls and telephony events are dealt with in the mobile device. It includes a series of rules which specify what should be done in particular circumstances or in response to a particular event. It can be used to control the content of the logging system, the disconnection of certain phone calls, the transition of a call between different states, or any other activity relating to telephony on the device.

In the case where the back-end logging system is used to direct the call handling policy, it could feed back to either the telephony API or the communications agent. It could formulate and modify policy based on criteria such as the amount of storage space available for storing new telephony information, the communication networks available to the device or the battery level. It could also be capable of receiving input from a user in order that the user can influence policy decisions. Alternatively it may be preferred that the user cannot access the back-end logging system, since making it directly accessible from the application level could represent a security risk – malicious or malfunctioning applications could potentially obtain or modify information from the logging system, thereby compromising the user's personal call information.

In the preferred embodiment the call handling policy is enforced at the call handling agent, which receives directions from the communications agent. The call handling agent communicates directly with the Telephony API in order to implement aspects of the call handling policy; however, the call handling agent could alternatively communicate with the API indirectly, via the telephony events monitoring agent or another element. In one embodiment, a user of the device can define at least some aspects of the call handling policy by means of interaction with the call handling agent, either directly or indirectly.

The scheduling policy defines the manner in which data is passed to the back-end logging system. It can define the type of information provided to the back-end logging system, as well as the timing of transmissions to the logging system. The scheduling policy could be determined on a dynamic basis according to the usage of the device's telephony applications. For example, when the device is being used frequently for calls – perhaps

during a weekday while the user is away from his office – the communication to the back-end logging system could be performed relatively frequently, whereas during a period of low usage – perhaps during a weekday while the user is at his office desk and primarily using his office phone and computer to send and receive communications – the communication to the back-end logging system could be performed infrequently. This variation in scheduling policy could be achieved by the use of a usage monitoring or prediction agent arranged to determine the current or likely telephony behaviour of the device.

In the preferred embodiment, all of the agents described above – the telephony events monitoring agent, the call handling agent, the communications agent, and the usage monitoring agent – are provided as a single call logging and control application. Alternatively, the logging and control aspects could be provided by separate applications, or some or all of the functionality could be provided within the operating system.

A simple example of the operation of the call logging and control arrangement of the present invention will now be given.

A user of a mobile telephone makes an outgoing call to an overseas destination. The telephony events monitoring agent receives a notification from the Telephony API indicating that a call has been made, and indicating the time of the call and the destination phone number. The call handling agent is informed of this call handling event by the telephony events monitoring agent. The call handling agent stores the outgoing call as an event in a store of recent events: an entry is made in the store to include the nature of the event (outgoing phone call), the time of the call and the number to which it is directed.

At this time, the call handling agent does not communicate back to the Telephony API since no action needs to be taken by the Telephony API in response to this event.

The mobile telephone in the example is currently configured to alert a user when the duration of an outgoing overseas or premium rate call has exceeded ten minutes, in order to warn the user of potentially expensive calls. This configuration has been selected by the user, and could be switched off or altered if preferred. This policy setting is invoked

by means of the back-end logging system, with which the user can communicate by password access to change his call handling policy.

In accordance with this policy setting, the call handling agent begins a timer when the new outgoing call is connected. After ten minutes, the call handling agent triggers the Telephony API to cause an alert to be sent to the user in the form of an audible notification. The user can then choose whether to terminate the call and avoid excessive costs.

The scheduling policy in force for the mobile telephone is fixed, and requires that all telephony events stored by the call handling agent are transmitted to the back-end logging system at midnight every day. Thus, at midnight on the day the user made his overseas call, the communications agent retrieves the new entry in the call handling agent's store and sends it over a GSM network to a remote back-end logging system.

It can be seen from the above description that the present invention provides a flexible technique for controlling and logging telephony activity on a mobile device. It will be understood by the skilled person that alternative implementations are possible, and that various modifications of the methods and implementations described above may be made within the scope of the invention, as defined by the appended claims.

CLAIMS

1. A mobile communications device programmed with:

(a) a telephony events monitoring agent, registered with a telephony API provided by an operating system of the device so as to receive notifications of any telephony related events;

(b) a call handling agent for processing telephony events received from the telephony events monitoring agent and arranged to communicate with the telephony API based on a configured call handling policy, the call handling agent being arranged to store logs of device telephony activity;

(c) a communications agent that uses a communications API of the operating system to communicate the logs stored by the call handling agent to a back-end logging system using available communications means provided by the communications API.

2. The device of Claim 1 in which the telephony related events include one or more of:

a) Making an outgoing call;

b) Receiving an incoming call;

c) Call status change, where the statues include dialling, answering, connecting, ringing, connected, hanging up, hold, missing a call.

3. The device of Claim 1 or 2 in which the configured policy includes one or more of the following:

a) Log outgoing call information;

b) Log incoming call information;

c) Automatically answer incoming calls;

d) Automatically disconnect incoming calls;

e) Automatically disconnect outgoing calls;

f) Determine response based on dynamic properties including date, time, location, call origin or destination, associated contact information, diary information, or selected profile;

g) Capture additional state information such as network information or device status;

h) Determine schedule for communicating log information to the back-end logging system;

i) Invoke alternative communications client on device.

4. The device of any preceding Claim in which the call handling agent communicates call logging information to the communications agent based on a scheduling policy.

5. The device of Claim 4 in which the call logging information may be augmented with additional device information such as device identification or network information.

6. The device of any preceding Claim in which the communications agent notifies the call handling agent of any call handling policy modification requests received from the back-end logging system.

7. The device of any preceding Claim in which the available communications means provided by the communications API includes one of:

a) A TCP/IP communication protocol (HTTP, FTP, SMTP, etc.)

b) A GSM communication channel such as SMS, MMS.

8. The device of Claim 1, arranged such that the back-end logging system can dynamically control the call handling policy by communicating policy modifications to the call handling agent using available communications means via the communications agent.

9. A method of enabling a mobile communications device to log calls, comprising the steps of:

(a) a telephony events monitoring agent registering with a telephony API provided by an operating system of the mobile device in order to receive notifications of any telephony related events;

(b) a call handling agent processing telephony events received from the telephony events monitoring agent and arranged to communicate with the telephony API based on a configured call handling policy, the step of processing including storing logs of device call activity;

(c) a communications agent using a communications API of the operating system to communicate the logs stored by the call handling agent to a back-end logging system using available communications means provided by the communications API.

10. A system for enabling mobile device calls to be logged, the system comprising multiple mobile communications devices as claimed in Claim 1 and a back-end logging system arranged to receive logs from the mobile devices.

11. The system of Claim 10 in which the back-end logging system is also arranged to log telephone calls received from mobile telephone and from landline calls.

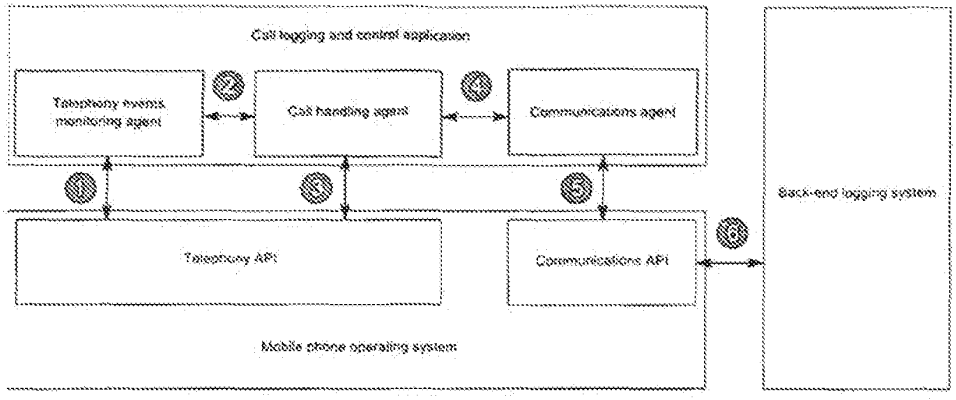

Call logging and control application
Telephony events monitoring agent
Call handling agent
Communications agent
Back-end logging system
Telephony API
Communications API
Mobile phone operating system

Figure 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2007/003011

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M1/2745 H04M1/725

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 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/130631 A1 (MAGUIRE MICHAEL [CA] ET AL.) 16 June 2005 (2005-06-16) abstract compounds 4-7 paragraph [0002] - paragraph [0004] paragraph [0011] - paragraph [0014] paragraph [0025] - paragraph [0034] paragraph [0037] - paragraph [0039] -/--	1-11

[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
6 November 2007	14/11/2007

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	Kim-Mayser, Michael

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2007/003011

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 2005/075097 A1 (LEHIKOINEN JAAKKO [FI] ET AL LEHIKOINEN JAAKKO [FI] ET AL) 7 April 2005 (2005-04-07) abstract figures 1-3c paragraph [0005] paragraph [0007] - paragraph [0010] paragraph [0016] - paragraph [0030] paragraph [0032] paragraph [0035]	1-11
A	US 2005/261003 A1 (FIEDLER RENO [US] ET AL) 24 November 2005 (2005-11-24) the whole document	1-11
A	EP 1 148 423 A (MITSUBISHI ELECTRIC CORP [JP]) 24 October 2001 (2001-10-24) the whole document	1-11
A	WO 02/078315 A (T MOBILE DEUTSCHLAND GMBH [DE]; VOEHRINGER GERRIT [DE]) 3 October 2002 (2002-10-03) the whole document	1-11

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2007/003011

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005130631 A1	16-06-2005	NONE	
US 2005075097 A1	07-04-2005	CN 1868202 A	22-11-2006
		EP 1671474 A2	21-06-2006
		WO 2005033828 A2	14-04-2005
		KR 20060085932 A	28-07-2006
US 2005261003 A1	24-11-2005	NONE	
EP 1148423 A	24-10-2001	CN 1335964 A	13-02-2002
		DE 60024230 D1	29-12-2005
		DE 60024230 T2	10-08-2006
		WO 0135229 A1	17-05-2001
		JP 3883869 B2	21-02-2007
		US 2001042103 A1	15-11-2001
WO 02078315 A	03-10-2002	AT 341897 T	15-10-2006
		CZ 20032905 A3	14-01-2004
		DE 10114964 A1	17-10-2002
		EP 1374551 A2	02-01-2004
		ES 2274031 T3	16-05-2007
		FI 362681 A1	02-11-2004
		US 2004116136 A1	17-06-2004

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2008 年8 月21 日 (21.08.2008)

PCT

(10) 国際公開番号
WO 2008/099802 A1

(51) 国際特許分類:
H04L 12/56 (2006.01)

(21) 国際出願番号: PCT/JP2008/052236

(22) 国際出願日: 2008 年2 月12 日 (12.02.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2007-031508 2007 年2 月13 日 (13.02.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 粟野 潤 (AWANO, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

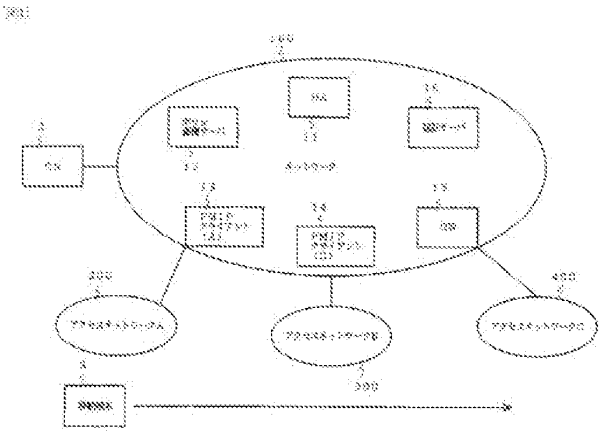
(74) 代理人: 宇高 克己 (UDAKA, Katsuki); 〒1010025 東京都千代田区神田佐久間町１－１４第二東ビル５階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): 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.

/続葉有/

(54) Title: MOBILE TERMINAL MANAGEMENT SYSTEM, NETWORK DEVICE, AND MOBILE TERMINAL OPERATION CONTROL METHOD USED FOR THEM

(54) 発明の名称: 移動端末管理システム、ネットワーク機器及びそれらに用いる移動端末動作制御方法



100 NETWORK
12 POLICY ACCUMULATION SERVER
16 AUTHENTICATION SERVER
13 PMIP CLIENT (A)
14 PMIP CLIENT (B)
200 ACCESS NETWORK A
300 ACCESS NETWORK B
400 ACCESS NETWORK C
3 MOBILE TERMINAL

(57) Abstract: Provided is a mobile terminal management system which can rapidly decide whether a mobile terminal is to execute a PMIP operation or a CMIP operation in accordance with a network administrator.A PMIP client (A) and a PMIP client (B) have: a function to decide whether the mobile terminal is to execute the PMIP operation or the CMIP operation in accordance with terminal capability request information transmitted from a mobile terminal and a policy acquired from a policy accumulation server; and a function to transmit terminal operation control information which can control operation of the mobile terminal and IP setting information required upon decision whether the mobile terminal is to execute the PMIP operation or the CMIP operation. The mobile terminal has a function to transmit to the network, a report containing a use request of the CMIP function in accordance with the terminal side policy such as the user setting and service contents upon connection to the access network or upon a handover.

(57) 要約: ネットワークの管理者のポリシに応じて移動端末がＰＭＩＰ動作するか、ＣＭＩＰ動作するかを高速に決定可能な移動端末管理システムを提供する。ＰＭＩＰクライアント（Ａ）及びＰＭＩＰク

/続葉有/

WO 2008/099802 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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).

添付公開書類:
— 国際調査報告書

ライアント（Ｂ）は、移動端末から送られた端末能力要求情報と、ポリシ蓄積サーバから取得したポリシに基づいて、移動端末をＰＭＩＰ動作とするか、ＣＭＩＰ動作とするかを決定する機能と、移動端末の動作を制御可能な端末動作制御情報と、移動端末がＰＭＩＰ動作、ＣＭＩＰ動作の何れとするかを決定した際に必要となるＩＰ設定情報とを含む通知を移動端末に送信する機能とを有する。移動端末は、アクセスネットワークに接続した際、あるいはハンドオーバした際等に、ユーザの設定やサービス内容等、端末側のポリシにしたがってＣＭＩＰ機能の使用要求を格納した通知をネットワークに送信する機能を有する。

明 細 書

移動端末管理システム、ネットワーク機器及びそれらに用いる移動端末動作制御方法

技術分野

[0001] 本発明は移動端末管理システム、ネットワーク機器及びそれらに用いる移動端末動作制御方法に関し、特にPMIP[Proxy MIP(Mobile Internet Protocol)]クライアントを配備したネットワークにおける移動端末の動作制御に関する。

背景技術

[0002] PMIPクライアントを配備したネットワークに、CMIP(Client MIP)機能[MIPv4(Mobile Internet Protocol version 4)機能]を備えた移動端末が接続した場合の動作例は、以下の通りである。

[0003] すなわち、移動端末がPMIPクライアントを有するネットワークに接続した場合には、MIPv4[RFC(Request For Comments)3344]に定義されたAA(Agent Advertisemet)を移動端末に対して送信し、移動端末がCMIP機能を備えているかどうかを確認する方法が考慮されている(例えば、非特許文献1参照)。

[0004] つまり、AAをCMIP端末が受信した場合には、それに反応してRRQ(Regisration Request:位置登録要求)を送信するが、このRRQが送信された場合、ネットワーク側は移動端末にCMIP機能があると判断し、移動端末はCMIPで動作する。

[0005] 一方、Simple IP(Internet Protocol)端末は、AAを理解できず、一般のIP端末がネットワークに接続した際と同様に、DHCP(Dynamic Host Configuration Protocol)によってアドレス取得を試みる。PMIPクライアントは、このDHCP requestを契機としてSimple IP端末の代わりにHA(Home Agent:ホームエージェント)に対して位置登録要求を送信する。

[0006] 上記の処理動作によれば、CMIP端末は固定的にCMIP動作することになる。但し、ネットワークを管理するオペレータによっては、CMIP端末に対してもPMIPで動作させたい場合がある。

[0007] しかしながら、現在、PMIP機能を有するネットワークにCMIP端末が接続した時に

は、移動端末側の要求やネットワークでのポリシを鑑みつつ、移動端末の動作(PMIP動作とするか、CMIP動作とするか)を行う仕組みが存在しない。

[0008] 非特許文献1:"WiMAX End-to-End Network Systems Architecture(Stage 2:Architecture Tenets, Reference Model and Reference Points)[Part2], 7.8 CSN Anchored Mobility Management"

非特許文献2:"Mobility Management using Proxy Mobile IPv4", http://www.ietf.org/internet-drafts/draft-leung-mip4-proxy-mode-01.txt

非特許文献3:"Proxy Mobile IPv6", http://www.ietf.org/internet-drafts/draft-sgundave-mipv6-proxymipv6-00.txt

非特許文献4:"Network Based Layer 3 Connectivity and Mobility Management for IPv6", http://www.ietf.org/internet-drafts/draft-chowdhury-netmip6-01.txt

発明の開示

発明が解決しようとする課題

[0009] PMIPクライアントを配備したネットワークに、MIP機能(MIPv4機能)を備えた移動端末が接続した場合の動作においては、移動端末に対して送信したAAに反応して移動端末が位置登録要求(RRQ)を送信してくるか、AAを無視してDHCPによってアドレス取得にくるかに応じて移動端末におけるMIP機能の有無を判定し、MIP機能がなければPMIPクライアントが移動端末に代わってRRQを送信し、MIP機能があればPMIPクライアントが移動端末の代理を行わず、移動端末自身がCMIP動作によってRRQを送信している。

[0010] 上記の処理動作によれば、CMIP端末は固定的にCMIP動作することになる。ネットワークを管理するオペレータによっては、CMIP端末に対してもPMIPで動作させたい場合があるが、CMIP端末がMIP機能を使わず、PMIP動作とするか、MIP機能を使ってCMIP動作とするかをネットワーク側から自由に制御する仕組みが存在しない。

[0011] そこで、本発明の目的は上記の問題点を解消し、ネットワークの管理者のポリシにし

たがって移動端末がPMIP動作するか、CMIP動作するかを高速に決定することができる移動端末管理システム、ネットワーク機器及びそれらに用いる移動端末動作制御方法を提供することにある。

課題を解決するための手段

[0012] 本発明による移動端末管理システムは、PMIP[Proxy MIP(Mobile Internet Protocol)]機能を持つネットワーク機器が配備されたネットワークにおいて移動端末の動作を制御する移動端末管理システムであって、 前記ネットワーク側から前記移動端末側に前記PMIP機能を提供可能か否かを通知している。

[0013] 本発明によるネットワーク機器は、PMIP[Proxy MIP(Mobile Internet Protocol)]機能を持つネットワーク機器が配備されたネットワークにおいて移動端末の動作を制御する移動端末管理システムを構成するネットワーク機器であって、

前記移動端末側に対して前記PMIP機能を提供可能か否かを通知している。

[0014] 本発明による移動端末動作制御方法は、PMIP[Proxy MIP(Mobile Internet Protocol)]機能を持つネットワーク機器が配備されたネットワークにおいて移動端末の動作を制御する移動端末管理システムに用いる移動端末動作制御方法であって、

前記ネットワーク側から前記移動端末側に前記PMIP機能を提供可能か否かを通知している。

発明の効果

[0015] 本発明は、上記のような構成及び動作とすることで、ネットワークの管理者のポリシにしたがって移動端末がPMIP動作するか, CMIP動作するかを高速に決定することができるという効果が得られる。

図面の簡単な説明

[0016] [図1]本発明の第1の実施の形態による移動端末管理システムの構成を示すブロック図である。

[図2]NVSEのフォーマットを示す図である。

[図3]図1の移動端末の構成例を示すブロック図である。

[図4]図1のPMIPクライアント(A)13の構成例を示すブロック図である。

[図5]図1のGWの構成例を示すブロック図である。

[図6]本発明の第1の実施の形態におけるNVSEが格納されたMIPv4信号を受信したMIPv4ノードの処理を示すフローチャートである。

[図7]本発明の第1の実施の形態において移動端末3がネットワークのポリシによってPMIP動作とする場合の動作を示すシーケンスチャートである。

[図8]本発明の第1の実施の形態において移動端末3からの要求とネットワークのポリシとによって移動端末3の動作を決定する手順を示すフローチャートである。

[図9]本発明の第1の実施の形態において移動端末3がアクセスネットワーク(A)200に接続した時にネットワークのポリシによってCMIP動作が許可される場合の動作を示すシーケンスチャートである。

[図10]本発明の第1の実施の形態において移動端末3がアクセスネットワーク(C)400に接続した場合の動作を示すシーケンスチャートである。

[図11]本発明の第2の実施の形態による移動端末管理システムの動作を示すシーケンスチャートである。

[図12]本発明の第2の実施の形態において移動端末3がアクセスネットワーク(A)200に接続した場合にネットワークのポリシによってCMIP動作が許可された場合の動作を示すシーケンスチャートである。

[図13]本発明の第2の実施の形態において移動端末3がアクセスネットワーク(C)400に接続した場合の動作を示すシーケンスチャートである。

符号の説明

[0017]

2 CN

3 移動端末

11 HA

12 ポリシ蓄積サーバ

13 PMIPクライアント(A)

14 PMIPクライアント(B)

15 GW

31 CMIP動作手段

32 Simple IP動作手段
33 接続・動作検出手段
34 ポリシ蓄積手段
35 端末動作要求送信手段
36 端末動作情報受信手段
37 動作決定手段
100 ネットワーク
131 PMIP動作手段
132 FA動作手段
133 端末動作要求受信手段
134 ポリシ通信手段
135 動作決定手段
136 認証処理手段
137 端末動作情報送信手段
151 GW動作手段
152 FA動作手段
153 端末動作要求受信手段
154 認証処理手段
155 端末動作情報送信手段
200 アクセスネットワーク(A)
300 アクセスネットワーク(B)
400 アクセスネットワーク(C)

発明を実施するための最良の形態

[0018] 本発明の移動端末管理システムは、移動端末がMIP(Mobile Internet Protocol)[以後、PMIP(Proxy MIP)に対してClient側のMIP機能であることを強調し、Client MIP(CMIP)とする]機能を有している場合(以下、この移動端末をCMIP端末とする)、CMIP端末がネットワークに接続した際、あるいはハンドオーバした際に、CMIP能力の通知及びCMIP機能の使用をネットワーク機器へ要求する機能を

、CMIP端末に備えている。

[0019] また、ネットワークでは、該ネットワークの管理者のポリシに基づいて、CMIP端末の動作を制御可能な情報、及びIP(Internet Protocol)設定情報を格納した通知をCMIP端末に対して行う。これにより、CMIP端末がPMIP端末(つまり、Simple IP端末)あるいはCMIP端末としての動作のいずれとするかを明確に決定することが可能となる。

[0020] さらに、PMIP端末として動作する場合、CMIP端末として動作する場合のいずれおいても、移動端末の各種IP情報[移動端末のHoA(Home Address)、CoA(Care-of Addres)、HA(Home Agent;ホームエージェント)アドレス]の設定を高速に完了することが可能となる。

[0021] そのため、本発明の移動端末管理システムでは、ネットワーク接続やハンドオーバ時において、サービス提供可能となるまでの時間を短縮することが可能となる。この時、端末能力通知、CMIP使用の要求、及びネットワークからの端末制御通知に、MIPv4(Mobile Internet Protocol version 4)の場合にはAS(Agent Solicitation)、AA(Agent Advertisement)、MIPv6(Mobile Internet Protocol version 6)の場合にはRS(Router Solicitation)、RA(Router Advertisement)といったMIPやIP端末が通常に使用するプロトコルを拡張して行うことで、本発明に対応した端末だけでなく、一般的なCMIP端末、あるいはSimple IP端末も同時に収容することが可能であり、現存するシステムへの本発明の適用も容易となる。

[0022] また、本発明の移動端末管理システムでは、端末とネットワークとの間の通知の数も削減可能となるために、通信帯域の効率的な使用が可能となる。移動通信では無線通信技術を使用するが、無線通信技術は、多くの場合、有線通信技術と比べて帯域的に劣るため、帯域の効率的な使用は特に重要となる。

[0023] このように、本発明の移動端末管理システムは、PMIP機能を備えたネットワークに、CMIP機能を備えたCMIP端末が接続した際に、CMIP端末のポリシによってCMIPでの動作を要求する通知を行う。一方、ネットワークがその通知によって取得したCMIP端末の要求とネットワーク側のポリシとによって、CMIP端末をCMIPで動作させるか、PMIPで動作させるかを制御可能な通知を行うと共に、通信に必要な情報(例

えば、IPアドレス情報)を通知することを特徴としている。

[0024] この結果、本発明の移動端末管理システムでは、CMIP端末がネットワークに接続した際、あるいはハンドオーバした際に、PMIP動作(ネットワーク側のPMIP機能を使用)とするか、CMIP動作(自らのCMIP機能を使用)とするかを決定することが可能となり、さらにIP設定を完了することが可能となるため、高速に通信可能な状態となり、電源投入後の快適なサービスの開始、あるいはハンドオーバ時のサービス途絶の回避ないしは途絶時間の短縮を可能とする。

[0025] 本発明の移動端末管理システムは、さらに以下の(1)～(3)の特徴を有している。

(1)本発明の移動端末管理システムでは、既存のMIPのプロトコル、あるいは一般に使用されるプロトコルを流用することで、既存のシステムへの変更を最小限とする。

(2)本発明の移動端末管理システムでは、本発明をサポートしたPMIPクライアントを配置したネットワークに、本発明をサポートしないCMIP端末やCMIP機能を備えない一般的なIP端末(以後、この端末をSimple IP端末とする)が接続した場合にも、それらの端末がネットワークに接続した際に発生する信号交換と共通化することが可能となり、一般的なIP端末及びCMIP端末との共存が可能であり、本発明を既存システム、あるいは既に検討が進んでいるシステムに適用することを容易とする。

(3)本発明をサポートしたネットワークに、本発明をサポートしたMIP端末が接続した場合には、ネットワーク側のポリシが許せば、MIP端末側の意図によって、PMIP動作とするか、CMIP動作とするかの動作モードを選択することが可能となる。これによって、端末側でハンドオーバタイミングを制御することが可能となる。また、端末が、サービスの種別によって、HA(Home Agent)を選択したり、複数のHAに位置登録をしたりすることが可能となり、ユーザに提供するサービスの幅を広げることが可能となる。

[0026] 尚、HAに相当するのは、3GPPにおいては、SAE－A(System Architecture Evolution－Anchor)である。3GPP2, WiMAX ForumではそのままHAと呼称される。また、PMIPクライアントに相当するのは、3GPPにおいては、3GPP－A(3GPP－Anchor)、MME(Mobility Management Entity)／UPE(User Plane Entity)、PDG(Packet Data Gateway)である。また、3GPP2では、PDS

N(Packet Data Serving Node)、PDIF(Packet Data Interworking Function)である。さらに、WiMAX ForumにおいてはASN(Access Service Network)－GWである。

[0027] 続いて、本発明の詳細について、以下に図面を参照して説明する。

[0028] 図1は本発明の第1の実施の形態による移動端末管理システムの構成を示すブロック図である。図1において、本発明の第1の実施の形態による移動端末管理システムは、ネットワーク100と、アクセスネットワーク(A)200と、アクセスネットワーク(B)300と、アクセスネットワーク(C)400と、CN(Correspondent Node)2と、移動端末3とから構成されている。

[0029] ネットワーク100内には、HA(Home Agent)11と、ポリシ蓄積サーバ12と、PMIP[Proxy MIP(Mobile Internet Protocol)]クライアント(A)13と、PMIPクライアント(B)14と、GW(GateWay)15とが設けられている。

[0030] ネットワーク100は、移動端末3に対して各種サービスを提供するプロバイダが管理するネットワークである。ネットワーク100は、例えば、3GPP(3rd Generation Partnership Project)においてCore Networkと呼ばれるネットワークに対応し、また、WiMAXにおいてはCSN(Connectivity Service Network)に対応するネットワークである。

[0031] HA11はRFC(Request For Comments)3344、あるいはRFC3775に定義されたHAであり、CMIP(Client MIP)端末、あるいはPMIPクライアントによる位置登録要求によって、移動端末のHome Address宛のパケットを、移動端末の移動先にカプセル化によって転送する機能を有している。

[0032] 本実施の形態でのHA11は、一般的なHAと同等の機能を有するものである。当該HAは、例えば、3GPPではSAE－A(System Architecture Evolution－Anchor)、3GPP－A(3GPP－Anchor)というように、MIPのHAの移動端末の移動先へパケットを転送する機能に加え、他の機能も一緒に実装されたり、異なる名称で呼ばれたりするが、MIPとしてのHA機能が実装されているノードは全て、HA11として示したノードの範疇に入る。

[0033] ポリシ蓄積サーバ12は、CMIP端末をSimple IP(Internet Protocol)端末とし

て動作させるか、CMIP端末として動作させるかといったネットワークのポリシが蓄積されたサーバであり、PMIPクライアント(A)13、PMIPクライアント(B)14からのポリシ要求によって、ネットワークのポリシを応答する。このポリシは、ネットワーク単位で共通のポリシとしても良いし、アクセスネットワーク単位でのポリシとしても良い。あるいは、ユーザ、あるいは移動端末単位で異なるポリシとしても良い。

[0034] アクセスネットワーク単位でポリシを適用する場合には、ポリシ要求に、PMIPクライアントあるいはGWの識別子を含める。また、ユーザ単位でポリシを適用する場合には、ポリシ要求に、RFC4282で規定されたユーザのNAI(Network Access Identifier)等のユーザ識別子を格納する。同様に、移動端末単位とする場合には、端末識別子をポリシ要求に格納する。

[0035] 一方、固定的に同一のポリシを適用する場合には、ポリシ蓄積サーバ12は省略することが可能である。この場合には、PMIPクライアント(A)13、PMIPクライアント(B)14、GW15各々の設定ファイルに、CMIP端末の動作ポリシを設定する。

[0036] ポリシ蓄積サーバ12に格納するポリシ情報は、例えば、CMIP端末にPMIPとして動作させることを強制する"PMIP強制"、CMIP端末にPMIP動作、あるいはCMIP動作の選択を許可する"CMIP許可"、CMIP端末にCMIP動作を強制する"CMIP強制"とすることができるが、これらに限らない。

[0037] PMIPクライアント(A)13及びPMIPクライアント(B)14は、一般的なPMIPクライアント機能に加え、移動端末3から送られた端末動作要求情報と、ポリシ蓄積サーバ12から取得したポリシに基づいて、移動端末3をPMIP動作とするか、CMIP動作とするかを決定する機能を備え、その後、移動端末3の動作を制御可能な端末動作制御情報と、移動端末3がPMIP動作、CMIP動作の何れとするかを決定した際に必要となるIP設定情報とを含む通知を移動端末3に送信する機能を有する。

[0038] ここで、一般的なPMIP機能とは、移動端末3に代ってCMIPの位置登録要求をHA11に送信する機能である。位置登録要求とは、MIPv4であればRRQ(Registration Request)であり、MIPv6であればBU(Binding Update)である。

[0039] PMIPクライアントの仕様は、MIPv4をベースにするか、MIPv6をベースにするか、あるいはIPv4、IPv6双方の端末を収容可能とするかどうか、位置登録要求を代理

送信する契機を何にするか、等いくつかの相違点を有する複数のドラフト(上記の非特許文献2～4)がIETF(Internet Engineering Task Force)に提出されている。

[0040] しかしながら、いずれにおいても、上述したように、端末の代理で位置登録要求をHA11に送信するPMIP機能を持つノードが規定されており、PMIP機能を有するノードが、本発明のPMIPクライアント(A)13, PMIPクライアント(B)14に相当する。今後新たなドラフトが提出される、あるいは正式な標準ができたとしてもPMIP機能を有するノードであれば、本発明の要素を盛り込めば、本実施の形態のPMIPクライアントに相当するノードとなる。

[0041] 本実施の形態では、上記のように、PMIPクライアント(A)13、PMIPクライアント(B)14は、一般的なPMIP機能と、本発明の移動端末3の動作制御情報を通知する機能とを共に備えたノードとしているが、これらの機能は別のノードとして実装されても構わない。

[0042] PMIPクライアント(A)13, PMIPクライアント(B)14はそれぞれ、ネットワーク100と、アクセスネットワーク(A)200、アクセスネットワーク(B)300との境界部に配置されるが、ユーザあるいは通信I／F(インタフェース)の認証を行うための認証機能を、さらにPMIPクライアント(A)13、PMIPクライアント(B)14に有する構成としても構わない。上記のような機能を含め、本発明のPMIPクライアントとしたノードの機能配備は、実施する状況によって様々なものが考えられ、本実施の形態で想定した機能配備には限らない。

[0043] GW15は、ネットワーク100とアクセスネットワーク(C)400との境界に配置されたルータであり、移動端末3がネットワーク100内のノードと通信するにあたって、ユーザ認証や、通信I／Fの認証を行うための認証機能を備えていても良い。上記のような一般的なルータ、あるいは認証GWとしての機能に加え、本発明のGW15は、移動端末3の動作がCMIPとなるような端末動作制御情報を移動端末3に送ると共に、移動端末3がCMIP動作をする際に必要となるIP設定情報を含む通知を移動端末3に送信する機能を有している。

[0044] PMIPクライアント(A)13、PMIPクライアント(B)14, GW15が、移動端末3に対し

て端末動作制御情報及びIP設定情報を通知する場合、本発明においては、MIPv4、MIPv6が一般的に使用するプロトコルを拡張して情報を格納する方法とする。

[0045] 具体的に説明すると、MIPv4の場合にはAA(Agent Advertisement)に、MIPv6の場合にはRA(Router Advertisemet)にそれぞれ情報を格納する。この時、必ずしも、AA、RAのような一般的に使用するプロトコルを使用する必要はないが、AA、RAを使用することで、(1)AAあるいはRAの他に新たな通知を送る必要がなく、通信帯域の効率的な使用が可能、(2)本発明をサポートしたCMIP端末以外にも、一般的なCMIP端末及びSimple IP端末も矛盾無く収容することが可能、(3)AA、RAに格納可能な一般的な情報要素に入れる情報を工夫することで、本発明をサポートしないCMIP端末でも、本発明をサポートするCMIP端末に対して効率や自由度の面で劣るものの、CMIP動作、PMIP動作の制御が可能、といったメリットが得られる。

[0046] 尚、MIPv4のAAあるいはRAを同一リンク内の複数の移動端末に送信する場合には、特定の端末のIP設定情報を含めることはできないが、本発明の好適な適用先として想定している3GPPや3GPP2、WiMAX Forumで検討されているネットワークは、PMIPクライアントやGWと、移動端末とが移動端末単位で個別のリンクで接続される、したがって、AA、RAは特定の移動端末に送信されることになり、特定の移動端末のIP設定情報を含むこととしても問題ない。

[0047] また、上記のような場合ではなく、一般的なネットワークに適用する場合においても、特定の移動端末によって送信されたASあるいはRSへの応答としてUnicastでAA、RAを送信する場合にもIP設定情報を含めることができる。いずれにせよ、本実施の形態ではAA、RAは特定の移動端末に送信される状況を想定している。但し、IP設定情報を含めず、移動端末の動作制御情報を格納する場合には、複数の移動端末にAAやRAが送信される場合にも適用することができる。

[0048] 認証サーバ160は、RADIUSやDIAMETER等の一般的な認証サーバであり、アクセスネットワーク(A)200、アクセスネットワーク(B)300、アクセスネットワーク(C)400に移動端末3が接続した場合には、それぞれ、PMIPクライアント(A)13、PMIPクライアント(B)14、GW15からの認証要求に応じて移動端末3のユーザ、あるいは

端末自身の認証処理を行い、結果を応答する機能を有している。

[0049] また、認証をパスした際には、MIPクライアント(A)13、PMIPクライアント(B)14、GW15は、移動端末3に割当てるべきHoA(Home Address)やHAアドレス、HAに位置登録要求を行う際に使用する鍵情報を認証サーバ16からダウンロードすることができる。これらの機能は、上記のRADIUSやDIAMETERによる一般的な認証サーバで実現できることであり、それらの詳細な説明については省略する。

[0050] この例では、HA11、ポリシ蓄積サーバ12、認証サーバ16は、ネットワーク100の中に配置されているが、別のネットワークに配置されたものを使用することもできる。例えば、ネットワーク100の管理者が行っているサービスの加入者の移動端末3が、別の管理者が管理するネットワークに接続する場合、HA11や認証サーバ16はネットワーク100内のものを使用して、ポリシ蓄積サーバは在圏のものが使用される場合が考えられる。

[0051] CN2は、移動端末3の通信相手となる端末、あるいはサーバである。移動端末3の通信相手となる端末の場合には、移動端末3と同等の機能を有する移動端末であっても良い。

[0052] 移動端末3は、一般的なMIPv4、あるいはMIPv6機能に加え、アクセスネットワークに接続した際、あるいはハンドオーバした際等に、ユーザの設定やサービス内容等、端末側のポリシにしたがってCMIP機能の使用要求を格納した通知をネットワークに送信する機能を備えている。

[0053] また、移動端末3は、上記のPMIPクライアント(A)13、PMIPクライアント(B)14、GW15がAAあるいはRAに格納した端末動作制御情報及びIP設定情報を読取る機能を備え、端末動作制御情報にしたがってPMIP動作とするか、CMIP動作とするかを決定する機能を備えている。さらに、移動端末3は、このとき読取ったIP設定情報によって自らのIP設定を行う機能を備えている。

[0054] アクセスネットワーク(A)200、アクセスネットワーク(B)300、アクセスネットワーク(C)400は、移動端末3がネットワーク100のノードと通信する際に経由するネットワークである。アクセスネットワークは、同一L2(Layer2)リンクでPMIPクライアント(A)13、PMIPクライアント(B)14、GW15に接続できる構成(すなわち、間にルータがな

い構成)であっても良いし、間にルータを配置した構成としても良い。

[0055] ここで、MIPv4のAS、AAに対し、それぞれ端末動作要求情報及び端末動作制御情報を格納する場合には、RFC3115で規定されたVSE(Vendor/Organization Specific Extension)を使用する例を示す。

[0056] VSEは、ベンダや組織固有の情報を格納する際に使用することができる。VSEは、さらに、CVSE(Critical Vendor/Organization Specific Extension)とNVSE(Normal Vendor/Organization Specific Extension)とが定義されている。

[0057] CVSEがRRQ、RRP、AA、ASといったMIPv4の信号に格納されていた場合には、これを認識しないMIPv4ノード[HA、FA(Foreign Agent)、CMIP端末、PMIPクライアント]が信号を破棄する。一方、NVSEの場合には、これを認識しないMIPv4ノードが、NVSE部位を無視して処理を継続する。

[0058] 本実施の形態では、本発明をサポートしないノードにおいてもMIPv4の処理が正しく行われるようにするため、NVSEを使用する。但し、CVSEを使用しても構わない。

[0059] NVSEのフォーマットを図2に示す。この拡張はMIPv4信号のいずれの拡張部位にも格納することができる。ここで、Typeは RFC3115によって「134」と定められている。Lengthには、Type及びLengthを含まない拡張データのバイト数が設定される。Vendor/Org-IDにはベンダあるいは組織を示す識別子が設定される。Vendor-NVSE-Typeには、ベンダあるいは組織毎に定義した拡張情報の種別を示す値が設定される。Vendor-NVSE-Valueには、Vendor-NVSE-Typeで示された拡張情報の値が設定される。

[0060] 図3は図1の移動端末3の構成例を示すブロック図である。図3において、移動端末3はCMIP動作手段31と、Simple IP動作手段32と、接続・動作検出手段33と、ポリシ蓄積手段34と、端末動作要求送信手段35と、端末動作情報受信手段36と、動作決定手段37とから構成されている。

[0061] CMIP動作手段31はRFC3344に規定されたMIPv4、あるいはRFC3775に規定されたMIPv6に準じた端末機能によってモビリティを実現する手段を備えている。

Simple IP動作手段32は一般的なIPv4、あるいはIPv6端末として動作するための手段を備えている。

[0062] 接続・移動検出手段33はレイヤ2の機能等によってリンクアップや異なるリンクに接続したことを検出する機能を備えている。これは、一般的な無線インタフェースでも実現することができ、本発明の特徴は含まない。ポリシ蓄積手段34はCMIP動作を要求するか、あるいはPMIP動作を要求するかのポリシ情報を格納する手段である。このポリシ情報はユーザが設定しても良いし、予め端末に設定しておくことにしても良い。

[0063] 端末動作要求送信手段35は接続・移動検出手段33によって、ネットワークへの接続、あるいは移動を検出した際に、移動端末3の動作モードをポリシ蓄積手段34に蓄積されたポリシ情報から取得し、その動作モードの情報を格納したAS(MIPv4の場合)、あるいはRS(MIPv6の場合)を送信する手段を備えている。

[0064] 例えば、移動端末3がCMIP動作を要求する場合には、CMIP動作要求を示す情報(例えば、CMIP動作要求に対応させたコード)をAS、あるいはRSに格納し、PMIP動作する場合には、一般的なAS、RSを送るようにすることが考えられる。

[0065] 但し、CMIP動作を要求しない場合でも、端末がCMIP機能を備えていることを通知したい場合には、CMIP機能を備えていることを示すコードをAS、あるいはRSに格納するようにしても良い。本実施の形態では、端末動作要求送信にAS(MIPv4の場合)、RS(MIPv6)を用いているが、それ以外のプロトコルを用いることとしても構わない。

[0066] 端末動作情報受信手段36はPMIPクライアント(A)13またはPMIPクライアント(B)14、あるいはGW15から送信されたAA、あるいはRAを受信し、それぞれに格納されかつPMIPクライアントが決定した移動端末3の動作モードや、決定された動作モードでの動作に必要な情報(HoA、HAアドレス等)を取得する手段を備えている。

[0067] 動作モードは、直接AA、RAに格納せずに前記決定された動作モードに必要な情報等から間接的に判定するようにしてもよい。本実施の形態では、端末動作情報受信にAA(MIPv4の場合)、RA(MIPv6)を用いているが、それ以外のプロトコルを用いることとしても構わない。

[0068] 動作決定手段37はAAあるいはRAで取得されたPMIPクライアントが決定した動作モードがCMIP動作であれば、CMIP動作手段31を有効化する機能を備えている。一方、動作決定手段37はPMIP動作であった場合、CMIP動作手段31を無効化し、Simple IP端末として動作するSimple IP動作手段32を有効化する機能を備えている。いずれの場合も、動作決定手段37はAAあるいはRAで取得した各動作に必要な情報の設定を行う機能も備える。

[0069] 尚、図示していないが、移動端末3は認証処理手段を有している。この認証処理手段はネットワークに接続したことが検出された際に、PMIPクライアントと認証処理を行う手段を備えている。この時、移動端末3は、RFC4282に規定されたNAI(Network Access Identifier)等の識別子を認証要求の中に格納する。

[0070] 図4は図1のPMIPクライアント(A)13の構成例を示すブロック図である。図4において、PMIPクライアント(A)13はPMIP動作手段131と、FA動作手段132と、端末動作要求受信手段133と、ポリシ通信手段134と、動作決定手段135と、認証処理手段136と、端末動作情報送信手段137とから構成されている。尚、図示していないが、PMIPクライアント(b)14はこのPMIPクライアント(A)13と同様の構成及び動作となっている。

[0071] PMIP動作手段131は上記の非特許文献2～4に規定された一般的なPMIPクライアントの動作をする手段を備えている。但し、PMIPクライアント(A)13が移動端末3に代わってRRQ(MIPv4の場合)、あるいはBU(MIPv6の場合)をHA11に送信する契機は、動作決定手段135から送信される通知を契機とする。

[0072] FA動作手段132はMIPv4の場合、RFC3344に規定されたFAとして動作するための機能も備えている。FA機能は、移動端末3にCMIP動作を許可した場合で、かつFAモードで動作させる際に使用される。但し、PMIP動作手段131が、移動端末3がFAモードで動作する際のように、RRQをFA経由でHA11に送る構成としても構わない。MIPv6の場合には、本手段は必要ない。

[0073] 端末動作要求受信手段133は移動端末3から送信されるAS(MIPv4の場合)あるいはRS(MIPv6)の場合を受信し、AS、あるいはRSに格納された移動端末3の動作要求情報を取得し、動作決定手段135に送信する機能を備えている。本実施の形

態では、端末が端末動作要求を送る手段としてAS(MIPv4の場合)、RS(MIPv6)を用いているが、それ以外のプロトコルを用いることとしても構わない。

[0074] ポリシ通信手段134はポリシ蓄積サーバ12に対し、接続した移動端末3の識別子をポリシ要求に格納し、そのポリシ要求を送信し、その結果として、ポリシ蓄積サーバ12から移動端末3をCMIP動作させるか、PMIP動作とするかのポリシ情報を取得する機能を備えている。ポリシ蓄積サーバ12に送信する情報には、当該PMIPクライアント(A)13の識別子や移動端末3の識別子以外にも、移動端末3の能力(CMIP端末を備えているか否か)等、他の情報を含むことにしても構わない。

[0075] PMIPクライアント識別子を含むことにした場合、ポリシ蓄積サーバ12は、どの移動端末かだけでなく、どのPMIPクライアント、あるいはどのアクセスネットワークに移動端末がいるかに依存してポリシを返すことができる。また、PMIPの識別子はPMIPの認証に用いることもできる。移動端末やPMIPの識別子としては、NAIを用いることができる。

[0076] 動作決定手段135はポリシ通信手段134で取得したポリシ情報と、端末動作要求[AS(RS)]受信手段133から取得した端末の動作要求情報とを基に移動端末3をPMIP動作とするか、CMIP動作とするかの動作モードを決定する機能を備えている。具体的な動作決定手順については後述する(図6参照)。

[0077] 移動端末3にCMIP動作させる場合で、かつMIPv4の場合には、さらに移動端末3がFAモードとCCoAモードとのどちらで動作すべきかを決定する。この決定のポリシとしては、例えば、PMIPクライアントがFAとしての機能を備えていればFAモード、FAとしての機能を備えていなければCCoAモードに決定する等とすることができる。但し、FAとしての機能を備えている場合でもCCoAモードを選択しても構わない。この場合、ポリシ蓄積サーバ12からFAモード、CCoAモードのどちらにするかのポリシを取得することで、どちらの動作にするかを決定するといった構成が考えられる。

[0078] 認証処理手段136は移動端末3から送られた識別子を用いて認証サーバ16と通信を行い、認証サーバ16から端末のHoA(CMIP端末の場合、Simple IP端末の場合にはHoAが単なるIPアドレス相当となる)、HA11のアドレス等の情報を取得する機能を備えている。この認証処理手段136は上記の非特許文献1にAuthenticat

orとして記載されている機能と同等ものであり、認証サーバ16としてRadiusサーバやDiameterサーバを使った構成が広く用いられている。

[0079] 端末動作情報送信手段137は動作決定手段135で決定した移動端末3の動作モードと、決定された動作モードで必要となるアドレス等の必要情報とをAA、RAに格納して移動端末3に送信する手段を備えている。アドレス等の必要情報は、認証処理手段16で取得した情報を用いる。本実施の形態では、PMIPクライアントが端末動作情報を送る手段としてAA(MIPv4の場合)、RA(MIPv6)を用いているが、それ以外のプロトコルを用いることとしても構わない。

[0080] 図5は図1のGW15の構成例を示すブロック図である。図5において、GW15はGW動作手段151と、FA動作手段152と、端末動作要求受信手段153と、認証処理手段154と、端末動作情報送信手段155とから構成されている。

[0081] GW動作手段151は一般的なルータとして動作する機能を備えている。また、GW動作手段151は移動端末3との間でIPsec(RFC4301に規定)によりセキュアな通信を確立する手段を備えていてもよい。いずれにせよ、GW動作手段151には本発明の特徴となる要素が含まれていない。FA動作手段152はMIPv4の場合、RFC3344に規定されたFAとして動作するための機能も備えている。FA機能は、移動端末3にFAモードで動作させる際に使用される。MIPv6の場合、このFA動作手段152は必要ない。

[0082] 端末動作要求受信手段153は移動端末3から送信されるAS(MIPv4の場合)あるいはRS(MIPv6の場合)を受信し、RS、あるいはASに格納された移動端末3の動作要求情報を取得する。但し、PMIP動作手段を備えていないため、"CMIP動作"が自動的に決定される。本実施の形態では、端末が端末動作要求を送る手段としてAS(MIPv4の場合)、RS(MIPv6)を用いているが、それ以外のプロトコルを用いることとしても構わない。

[0083] 認証処理手段154は移動端末3から送られた識別子を用いて認証サーバ16と通信を行い、認証サーバ16から端末のHoA(CMIP端末の場合、Simple IP端末の場合にはHoAが単なるIPアドレス相当となる)、HAのアドレス等の情報を取得する機能を備えている。この認証処理手段154は、上記の非特許文献1にAuthenticat

orとして記載されている機能と同等ものであり、認証サーバ16としてRadiusサーバやDiameterサーバを使った構成が広く用いられている。

[0084] 端末動作情報送信手段155は移動端末3にCMIP動作させるための動作モード"CMIP"と、認証処理手段154で取得した移動端末3に関連する情報(HoAやHAアドレス等の情報)、つまり移動端末3がCMIP端末として動作するために必要な情報を格納したAA、あるいはRAを移動端末3に送信する機能を備えている。移動端末3がMIPv4の場合には、さらに移動端末3がFAモードとCCoAモードとのどちらで動作すべきかも決定する。この決定のポリシとしては、例えば、GW15がFAとしての機能を備えていればFAモード、FAとしての機能を備えていなければCCoAモードに決定する等とすることができる。

[0085] 一方、GW15にFA機能を備えている場合にも、ポリシ蓄積サーバ12と通信する手段を備えることで、ポリシ蓄積サーバ12からFAモード、CCoAモードのどちらにするかのポリシを取得し、どちらの動作にするかを決定することにしても構わない。本実施の形態では、GW15が端末動作情報を送る手段としてAA(MIPv4の場合)、RA(MIPv6の場合)を用いているが、それ以外のプロトコルを用いることとしても構わない。

[0086] 図6は本発明の第1の実施の形態におけるNVSEが格納されたMIPv4信号を受信したMIPv4ノードの処理を示すフローチャートである。この図6を参照して、NVSEが格納されたMIPv4信号を受信したMIPv4ノードの処理について説明する。

[0087] MIPv4ノードは、MIPv4信号を受信した場合(図6ステップS1)、自ノードがNVSE Typeをサポートしているかどうかを判定し(図6ステップS2)、サポートしていなかった場合、NVSEを無視し、当該MIPv4信号にNVSEがなかったものとして処理を継続する(図6ステップS3)。

[0088] 一方、MIPv4ノードは、NVSE typeをサポートしている場合、次にVendor/Org-ID及びVendor-NVSE-Typeを認識可能であるかどうかを判定し(図6ステップS4)、いずかが認識できなかった場合、当該NVSEを無視し、当該NVSEがなかったものとして処理を継続する(図6ステップS5)。また、MIPv4ノードは、上記のステップS4の判定でいずれも認識可能であった場合、当該NVSEを適切に処理する(図

6ステップS6)。

[0089] このように、NVSEを使用することで、当該拡張を認識しないノードは、これを無視して当該拡張が格納された信号の処理を継続することが可能である。MIPv4においては、上述した端末動作要求情報、前記端末動作制御情報、IP設定情報といった情報を、NVSEを利用して送るものとする。

[0090] 一方、MIPv6の場合には、RAに移動端末の動作制御情報及びIP設定情報を格納するが、RAのoptionとして拡張情報を格納することで、拡張情報を認識するノードに情報を処理させ、それ以外のノードには当該情報を無視させることができる。

[0091] すなわち、この場合には、上記のMIPv4のNVSEを使用した場合と同様のことができる。したがって、MIPv6においては、上記の端末動作要求情報、前記端末動作制御情報、IP設定情報といった情報をRAのoptionを利用して送るものとする。

[0092] ここでは、移動端末3がMIPv4をサポートしており、HA11がMIPv4のHAであり、PMIPクライアント(A)13、PMIPクライアント(B)14がPMIPv4である場合を考慮し、また、図1の他のノードもIPv4に対応している状況を考慮する。

[0093] 本実施の形態において、ネットワーク100とアクセスネットワーク(A)200との境界に配置されたPMIPクライアント(A)13は、アクセスネットワーク(A)200の認証クライアント機能も備えている場合を想定する。さらに、PMIPクライアント(A)13は、FA機能も備えていてもよい、またFA機能を備えていない場合でも、FAのAS、AAをそれぞれ受信、送信する機能を備えているものとする。

[0094] 図7は本発明の第1の実施の形態において移動端末3がネットワークのポリシによってPMIP動作とする場合の動作を示すシーケンスチャートであり、図8は本発明の第1の実施の形態において移動端末3からの要求とネットワークのポリシとによって移動端末3の動作を決定する手順を示すフローチャートである。

[0095] また、図9は本発明の第1の実施の形態において移動端末3がアクセスネットワーク(A)200に接続した時にネットワークのポリシによってCMIP動作が許可される場合の動作を示すシーケンスチャートであり、図10は本発明の第1の実施の形態において移動端末3がアクセスネットワーク(C)400に接続した場合の動作を示すシーケンスチャートである。

[0096] はじめに、上記の図1及び図7を参照して、MIPv4機能を備えた移動端末3がアクセスネットワーク(A)200に接続した場合で、ネットワークのポリシによってPMIP動作とする場合の動作について説明する。

[0097] まず、移動端末3がアクセスネットワーク(A)200に接続すると、PMIPクライアント(A)13との間でアクセス認証処理を開始する。その際、移動端末3は認証のための秘密の情報と合わせて、ユーザを識別子するためのユーザ識別子をPMIPクライアント(A)13に送信する。

[0098] PMIPアクライアント(A)13は、移動端末3から受け取った認証情報を認証サーバ16に問合せることによって、移動端末3がアクセスの許可されたユーザかどうかを判定する。移動端末3がアクセスの許可されたユーザであると判定された場合、PMIPクライアント(A)13は、認証サーバ16から移動端末3に割当てるべきHoA(移動端末3がPMIP動作する場合には、HoAが移動端末3にとって単なるアドレスとみなされる)、アンカーとすべきHAアドレスをダウンロードする(図7のa1)。この時、上記の情報以外にも、HAに位置登録を行うための鍵情報等の他の情報もダウンロードするようにしても構わない。

[0099] 次に、移動端末3は、上記のa1の処理において、アクセス認証に成功した場合、ASをRFC1256に定義されたSolicitation Address(224. 0. 0. 2)、Mobile－Agents multicast group address(224. 0. 0. 11)、あるいはAddress(255. 255. 255. 255)宛に送信する(図7のa2)。

[0100] 移動端末3がCMIPを備えており、さらにCMIPとして動作することを希望する場合には、ASにCMIP要求を意味する情報を格納することができる。CMIP要求を意味する情報を送ることなく、CMIP要求の意思をPMIPクライアントに通知したい場合には、Address(224. 0. 0. 2)宛にASを送信した時にPMIP動作希望、Address(234. 0. 0. 11)宛にASを送信した時にCMIP動作希望、といったように宛先アドレスにPMIP要求、CMIP要求の対応関係を定義する方法とすることもできる。

[0101] 尚、移動端末3がCMIP動作を希望しない場合には、CMIP動作を希望しない情報をASに格納しても良いし、単なるASとしても良い。CMIP動作を希望しないもののネットワークに対し、CMIP機能が有ることを通知する場合には前者の方法とする。

[0102] 次に、PMIPクライアント(A)13は、ポリシ蓄積サーバ12に対してポリシ要求を送信する(図7のa3)。ここで、ポリシ蓄積サーバ12にPMIPクライアントやユーザ単位でのポリシ情報が蓄積されている場合には、PMIPクライアントの識別子と、上記のa1の処理で取得したユーザ識別子を送り、PMIPクライアントやユーザ個別のポリシ情報を要求することができる。尚、このa3の処理は、必ずしも上記のa2の処理の後である必要はない。

[0103] ポリシ蓄積サーバ12がa3の処理にてポリシ要求を受信した場合、PMIPクライアント(A)13に対し、予め設定されたポリシを通知する。ポリシ要求にPMIPクライアント識別子やユーザ識別子が格納されている場合には、それらに対応するポリシを検索し、検索された結果をPMIPクライアント(A)13に返す(図7のa4)。この動作例では、"PMIP強制"とのポリシをPMIPクライアント(A)13に応答する。

[0104] PMIPクライアント(A)13は、上記のa2の処理で得られた移動端末3の要求動作情報と、上記のa4の処理で得られたネットワークのポリシとによって、移動端末3の動作を決定する(図7のa5)。移動端末3の動作の決定手順については後述するが、ここでは、a4の処理において"PMIP強制"との応答を受信しているため、移動端末3に要求する動作はPMIPに決定される。

[0105] PMIPクライアント(A)13は、上記のa1の処理で取得した移動端末3のHoAと、自らのアドレスをCoAとして、同じくa1の処理で取得したHAアドレス宛にRRQを送信する(図7のa6)。

[0106] HA11は、a6の処理においてPMIPクライアント(A)13から送信されたRRQによって、HoA宛のパケットをカプセル化によってPMIPクライアント(A)13のアドレス宛に転送するためのBinding Cacheが作成される。その後、HA11は、RRQの応答としてRRPをPMIPクライアント(A)13に送信する(図7のa7)。

[0107] PMIPクライアント(A)13は、RRPを受信した場合、HA11からカプセル化によって送信されたパケットをデカプセルする用意をすると共に、移動端末3から送られたパケット(すなわち、送信元がHoAのパケット)をHA11宛にカプセル化して転送する用意を行う。

[0108] PMIPクライアント(A)13は、a7の処理でRRPを受信した後、AAを移動端末3に

送信する(図7のa8)。このAAには、NVSEを使って、PMIPとして動作すべきことを示す情報"PMIP"と、その際に移動端末3のアドレスとして使用すべきHoA、デフォルトGWアドレスを格納する。

[0109] さらに、AAの'H'フラグを'1'とし、さらにCoAフィールドにHAアドレスを格納することによって、本発明をサポートしないCMIP端末が当該AAを受信した場合にも、PMIP動作にすることができる。但し、この時点ではHAもHoAも未設定であり、Home戻りが検出できないため、RFC4433に規定された動的HA割当て手順が処理される。これによって、HoAを取得した時点でHome戻りが検出され、その後、PMIP動作(Simple IP端末としての動作)が可能となる。

[0110] このように、本発明をサポートしない移動端末の動作もPMIP動作となるように制御ができるが、本発明をサポート移動端末3と比較して信号の数や時間的に不利である。

[0111] 移動端末3は、a8の処理においてAAを受信した場合、AAに格納された"PMIP"情報によってPMIP動作することを決定する。さらに、移動端末3は、AAに格納されたHoA、デフォルトGWアドレス情報によってIP設定を完了する(図7のa9)。このa9の処理によって、アドレス設定が完了した後、移動端末3とCN2との間での通信が可能となる(図7のa10)。

[0112] ここで、a3の処理において、移動端末3からの要求とネットワークのポリシとによって移動端末3の動作を決定する手順について図8を参照して説明する。

[0113] まず、PMIPクライアント(A)13は自ノードのPMIP機能が有効かどうかを判定し(図8ステップS11)、PMIP機能が有効に動作していれば、図7のa4の処理で取得したネットワークポリシが"PMIP強制"であるかどうかを判定する(図8ステップS12)。ここで、ネットワークポリシが"PMIP強制"であった場合、PMIPクライアント(A)13は移動端末3の動作を"PMIP"とすることに決定する(図8ステップS13)。

[0114] ネットワークポリシが"PMIP強制"でなかった場合、PMIPクライアント(A)13はネットワークポリシが"CMIP許可"かどうかを判定する(図8ステップS14)。PMIPクライアント(A)13はネットワークポリシが"CMIP許可"であった場合、図7のa1の処理で取得した移動端末3の動作要求が"CMIP動作要求"かどうかを判定する(図8ステップ

S15)。

[0115] “PMIP動作要求”、あるいは、例えば、図7のa1の処理で単なるASを受信した場合等のように、CMIP要求動作が明示的に示されていない場合、PMIPクライアント(A)13は移動端末3の動作を“PMIP”とすることに決定する(図8ステップS13)。

[0116] “CMIP動作要求”が示されていた場合、PMIPクライアント(A)13は移動端末3の動作を“CMIP”に決定する(図8ステップS16)。上記のステップS14の処理で、ネットワークポリシが“CMIP許可”でなかった場合も、PMIPクライアント(A)13は移動端末3の動作を“CMIP”に決定する(図8ステップS16)。

[0117] この動作例において、PMIPクライアント(A)13では、上記のステップS11の判定結果が基本的に“YES”(PMIP機能有効)となる。しかしながら、PMIPクライアント(A)13において何らかの理由でPMIP機能が動作していない場合や、GW15のようにPMIP機能を備えていない場合には、上記のステップS11の判定結果が“NO”(PMIP機能無効)となるので、移動端末3の動作が“CMIP”に決定される。

[0118] 次に、MIPv4機能を備えた移動端末3がアクセスネットワーク(A)200に接続した時にネットワークのポリシによってCMIP動作が許可される場合の動作について図9を参照して説明する。

[0119] 図9のb1の処理からb4の処理までは、図7に示したPMIP強制の場合のa1の処理からa4の処理と同じである。但し、b4の処理でポリシ蓄積サーバ12から応答されるポリシは“CMIP許可”である。

[0120] 次に、PMIPクライアント(A)13は、図8で説明した移動端末3の動作の決定手順によって移動端末3の動作を“CMIP動作”に決定する(図9のb5)。PMIPクライアント(A)13は、このb5の処理で移動端末3の動作を“CMIP動作”に決定した場合、“PMIP強制”の場合とは異なり、RRQをHAに送ることはせず、AAを移動端末3に送信する(図9のb6)。

[0121] このAAには、NVSEを使って、移動端末3がCMIPとして動作すべきことを示す情報“CMIP”と、CMIPとして動作するために必要なHoA、CoA、及びFAモードとCCoA(Colocated－CoA)とのどちらで動作すべきかの情報を格納する。このFAモードとCCoAとのどちらで動作すべきかの情報は、ポリシ蓄積サーバ12から取得する構

成としても構わない。

[0122] さらに、AAの‘H’フラグを‘1’とし、さらにCoAフィールドにHAアドレスを格納する。この設定によって、本発明をサポートしないCMIP端末が当該AAを受信した場合には、PMIP動作にすることができる。但し、上記のように、この場合にはPMIP動作によって通信可能となるまでに、より多くの信号と時間とが使われる。

[0123] 移動端末3は、b6の処理においてAAを受信した場合、AAに格納された“CMIP”情報によってCMIP動作とすることに決定する。また、移動端末3は、AAに格納されたHoA, CoAによってIP設定を行い、さらにFA／CCoA情報によってFAモードで動作するか、CCoAモードで動作するかを決定する(図9のb7)。尚、図9に示す例ではFAモードで動作する場合を考慮する。

[0124] 移動端末3は、b7の処理でCMIP・FAモードで動作することを決定した後、HoA、CoAをHA11に登録するために、PMIPクライアント(A)13にRRQを送信する。PMIPクライアント(A)13は、移動端末3からのRRQをHA11に転送する〔この場合、PMIPクライアント(A)13がFA相当の動作を行う〕(図9のb8)。

[0125] HA11は、b8の処理においてRRQを受信した場合、HoA宛のパケットをカプセル化によってPMIPクライアント(A)13のアドレス宛に転送するためのBinding Cacheを作成する。その後、HA11は、RRQの応答としてRRPをPMIPクライアント(A)13に送信する。

[0126] PMIPクライアント(A)13は、HA11からのRRPを受信した場合、HA11からカプセル化によって送信されたパケットをデカプセルする用意を行うと共に、移動端末3から送られたパケット(すなわち、送信元がHoAのパケット)をHA11宛にカプセル化して転送する用意を行い、最後にRRPを移動端末3に転送する(図9のb9)。このb9の処理においてHA11への位置登録が完了した後、移動端末3とCN2との間での通信が可能となる(図9のb10)。

[0127] 次に、図1と図10とを参照して、移動端末3がアクセスネットワーク(C)400に接続した場合の動作について説明する。図10において、c1, c2の処理は、図7に示すPMIP強制の場合のa1, a2の処理と同じである。

[0128] GW15は、PMIPクライアント機能を備えていないため、c2の処理でASを受信する

と, CMIP動作が要求されているか否かに関わらず、移動端末3の動作を"CMIP"に決定する(図10のc3)。

[0129] 次に、GW15は, AAを移動端末3に送信する(図10のc4)。このAAには、NVSEを使って移動端末3がCMIPとして動作すべきことを示す情報"CMIP"と、CMIPとして動作するために必要なHoA, CoA、及びFAモードとCCoA(Colocated－CoA)とのどちらで動作すべきかの情報を格納する。

[0130] 例えば、GW15がFA機能を備えている場合にはFAモードとし、FA機能を備えていない場合にはCCoAとすることができる。ここでは、CCoAを選択した場合を考慮する。さらに、FAモードを選択した場合には、AAの'F'フラグを'1'とし、さらにCoAフィールドにGWアドレス(すなわち, FAアドレス)を格納する。

[0131] 一方, CCoAモードを選択した場合には, AAの'F'フラグと'R'フラグとを'1'とし、さらにCoAフィールドにはHA11からGW配下のネットワークに割り当てられた到達性のあるアドレスを格納する。この設定によって、本発明をサポートしないCMIP端末が当該AAを受信した場合でも、それぞれFAモードでの動作, CCoAモードでの動作とすることができる。いずれの場合も、その後、HoAを取得する処理が必要となる。CCoAモードで動作する場合には、本発明をサポートしないCMIP端末は、さらにHAアドレスを事前に設定しておくか、なんらかの方法でHAのアドレスを取得しなければならない。

[0132] 移動端末3は, c5の処理においてAAを受信した場合、AAに格納された"CMIP"情報及びCCoAモードで動作することを示す情報によってCCoAモードでCMIP動作することを決定する。また、移動端末3は, AAに格納されたHoA、CoAによって、IP設定を行い、同じくAAに格納されたHAアドレスを取得し, これを保持しておく。

[0133] 移動端末3は、上記のc5の処理で設定したHoAとCoAとを対応付けるためのRRQを、同じくc5の処理で取得したHAアドレスに対して送信する(図10のc6)。

[0134] HA11は、c6の処理においてRRQを受信した場合、HoA宛のパケットをカプセル化によって移動端末3のCoAに転送するためのBinding Cacheを作成する。その後、HA11は、RRQの応答としてRRPを移動端末3に送信する。移動端末3は、RRPを受信した場合, HA11からカプセル化によって送信されたパケットをデカプセル

する用意を行う(図10のc7)。また、移動端末3が送信するパケットをカプセル化してHA11に送るための用意を行う。このc7の処理においてHA11への位置登録が完了した後、移動端末3とCN2との間での通信が可能となる(図10のc8)。

[0135] 次に、移動端末3がハンドオーバする状況を考慮する。まず、移動端末3が、アクセスネットワーク(A)200からアクセスネットワーク(B)300へハンドオーバする場合のように、PMIPをサポートするアクセスネットワークへハンドオーバするケースについて考える。

[0136] この場合の動作は、図7あるいは図9のアクセスネットワーク(A)200に接続した場合と同じとして構わない。この場合、図7、図9のPMIPクライアントは、PMIPクライアント(B)14となる。但し、移動端末3がアクセスネットワーク(B)300に接続した際にPMIPクライアントや移動端末3がRRQを送信するために必要な情報(HoA、HAアドレス、HAへの位置登録をセキュアに行うための鍵情報等)を認証サーバ16に問合せるのではなく、ハンドオーバ元のPMIPクライアント(A)13から取得する方式としても構わない。

[0137] この時、ハンドオーバ元のPMIPクライアントがどれであるかは、アクセスネットワークに配置されたBS(Base Station)から通知することができる。あるいは、上記の非特許文献1に示されたASN Functional Entityのようなものを利用することができる。しかしながら、具体的な方法は、本発明に直接関係がないので、その詳細な説明については省略する。

[0138] また、ハンドオーバの場合には、移動端末3はHoAを既に取得しており、このHoAは通信を継続する間、保持し続けるアドレスであるため、a8の処理あるいはb6の処理においてAAに含める情報の中からHoAを省略しても構わない。

[0139] 次に、移動端末3が、アクセスネットワーク(B)300からアクセスネットワーク(C)400へハンドオーバする場合のように、PMIPがサポートしないアクセスネットワークへハンドオーバするケースについて考える。

[0140] この場合の動作は、図10のアクセスネットワーク(C)400に接続した場合と同じとして構わない。但し、移動端末3がアクセスネットワーク(C)400に接続した際に、移動端末3がRRQを送信するために必要な情報(HoA、HAアドレス、HAへの位置登録

をセキュアに行うための鍵情報等)を認証サーバ16に問合せるのではなく、ハンドオーバ元のPMIPクライアント(B)14から取得する方式としても構わない。また、ハンドオーバの場合には、移動端末3はHoAを既に取得しており、このHoAは通信を継続する間, 保持し続けるアドレスであるため、e4の処理においてAAに含める情報の中からHoAを省略しても構わない。

[0141] 本実施の形態では、移動端末3とPMIPクライアント(A)13、PMIPクライアント(B)14、GW15との間での情報のやり取りにAS、AAを利用することとしたが、必ずしもAS、AAである必要はなく, 例えば, IPCP(Internet Protocol Control Protocol configure－request, IPCP configure－Ackを使用することができる。

[0142] 本実施の形態で示した拡張情報を含むASの送信や拡張情報の含まれたAAの解釈をサポートする移動端末3は, CMIP機能を備えていることを想定しているが、これは、現実的にはSimple IP端末が一般的なIP端末と異なる動作をするとの前提を設けづらいためである。しかしながら、Simple IP端末が本発明の移動端末3であっても構わない。

[0143] また、本実施の形態では、移動端末3がCMIPで動作する要求を送信する場合を考慮したが、例えば、PMIP機能を提供可能なアクセスネットワークに接続した場合には必ずPMIPで動作するとのポリシとすれば, 移動端末3の送信するASは、本発明の拡張要素を含まない、一般的なASとしても構わない。この場合には、ポリシ蓄積サーバ12への問合せも省略することができる。

[0144] さらに, 本実施の形態ではAAによって, 移動端末3に通知するIP情報としてDNSサーバアドレスを含めていないが、DNSサーバアドレスを含めるようにしても構わない。

[0145] このように, 本実施の形態では、PMIPクライアントやGW15が、CMIP機能を備えた移動端末3の動作を制御するための情報を移動端末に通知することで、ネットワークの管理者のポリシにしたがって移動端末3がPMIP動作するか、CMIP動作するかを高速に決定することができる。

[0146] また、本実施の形態では、PMIPクライアントやGW15が、移動端末3の動作を制御するための情報とともに、それぞれの動作で必要となるIP設定情報も同時に移動

端末3に通知することで、移動端末3が動作の決定と同時に、IP設定をも完了することができ、高速に通信可能な状態にすることができる。

[0147] さらに、本実施の形態では、移動端末3もPMIP動作、CMIP動作のいずれかを希望する情報をネットワーク100に通知し、ネットワーク100が移動端末3の動作の希望と、ネットワーク100側のポリシの双方を鑑みて移動端末3の動作を制御することが可能となる。

[0148] 移動端末3の希望によってCMIP動作とした場合には、移動端末3側の意図によって、サービス毎に異なるHAをアンカーとして選択したり、移動端末3が複数の通信I／F(Interface)を備えていた場合に移動端末3がアクセスネットワークに接続した契機ではなく、端末を使用するユーザの意図するタイミング等で異なるI／Fへハンドオーバさせることが可能となる。異なるI／Fを同時に使用することも考えられる。

[0149] さらに、本実施の形態では、移動端末3の動作を制御するための情報や、MIP動作、CMIP動作のいずれかを希望する情報を一般的に使用されるプロトコルの信号(MIPv4の場合には、AS、AA)に格納することで、一般的な信号と本発明の情報を送るための信号とを別途送る必要がなく、通信帯域の効率利用を実現することができる。

[0150] さらにまた、本実施の形態では、一般的な信号の(本発明による拡張情報部位ではない)基本情報部分に本発明をサポートしていない一般的なCMIP端末の動作も制御可能な情報を格納することで、本発明をサポートしないCMIP端末の動作をも制御することができる。

[0151] したがって、本発明のPMIPクライアントは、本発明をサポートするCMIP端末、本発明をサポートしないCMIP端末、Simple IP端末を効率的に収容することが可能であり、現存するシステム、あるいは現在検討が進められているシステムへの適用が容易である。

[0152] 図11は本発明の第2の実施の形態による移動端末管理システムの動作を示すシーケンスチャートであり、図12は本発明の第2の実施の形態において移動端末3がアクセスネットワーク(A)200に接続した場合にネットワークのポリシによってCMIP動作が許可された場合の動作を示すシーケンスチャートであり、図13は本発明の第2

の実施の形態において移動端末3がアクセスネットワーク(C)400に接続した場合の動作を示すシーケンスチャートである。

[0153] 本発明の第2の実施の形態による移動端末管理システムの構成は、図1に示す本発明の第1の実施の形態による移動端末管理システムと同様の構成となっている。但し、本発明の第2の実施の形態では、移動端末3がMIPv6をサポートしており、HA1がMIPv6のHAであり, PMIPクライアント(A)13, PMIPクライアント(B)14がPMIPv6である場合を考慮している。また、図1の他のノードもIPv6に対応している状況を考慮している。

[0154] 本実施の形態において, ネットワーク100とアクセスネットワーク(A)200との境界に配置されたPMIPクライアント(A)13は, アクセスネットワーク(A)200の認証クライアント機能も備えている場合を想定する。最初に, 移動端末3がアクセスネットワーク(A)200に接続した場合で, ネットワークのポリシによってPMIP動作とする場合の動作を、図1と図11とを参照して説明する。

[0155] 図11には、移動端末3にPMIP動作を強制する場合の動作例を示しているが、d1の処理からd10の処理については、図7のa1の処理からa10の処理に対応しており、ほとんど同じ動作となる。但し、d2, d8の処理においてAS、AAではなく、RS、RAを使用している点が異なる。また, RAに格納する情報も異なる。

[0156] 尚、d6, d7の処理におけるBU(Binding Update)、BA(Binding Acknowledge)も図7のRRQ、RRPとは異なるが, HA11に対し、HoAとCoAとを対応付けた情報の保持とHoA宛のパケットをカプセル化によってCoA宛に転送することを要求する点で、それらの機能は同じである。

[0157] MIPv6ではAS, AAは使用せず、移動検出やCoA決定のためにRS、RAを使用する。したがって、本実施の形態では、RS, RAのoption部分に情報を格納する。このRS、RAのoption部に情報を格納した場合、これを認識できないノードは当該optionを無視する動きになり、MIPv4の場合のNVSEと同様の使い方が可能である。

[0158] 図11のd8の処理において、RAには、option部分にPMIPでの動作を指定するための"PMIP"との情報を格納する。そして、RAの基本情報部分には移動端末3がHoAを生成するためのHome prefixとPMIPクライアントのRAを送信したL/FのLin

klayerアドレスを格納する。

[0159] ここで、基本部分にHome prefixの情報を格納することで、移動端末3が、本発明の端末制御情報に対応していない場合でもPMIP動作とすることができる。但し、この場合、移動端末3はRFC3775に記述されたDynamic Home Agent Address Discoveryや事前に設定しておく等の方法でHAを発見し、さらにHoAを取得する処理が必要である。その処理の後、HoAを取得できた時点で、ようやく移動端末3にHome戻りを検出することができ、ここではじめてPMIP動作が可能となる。

[0160] このように、ネットワークと交換する信号の数や時間は、本発明の端末制御情報に対応した移動端末よりも多くかかることになる。

[0161] 図11のd9の処理では、移動端末3が、d8の処理での"PMIP"通知によって、PMIP動作することに決定する。この時、同じくd8の処理で取得したHome prefixと自らのI/F識別子[例えば、MAC(Media Access Control)アドレス]からアドレスを生成し、自らのアドレスとする。

[0162] また、デフォルトGWのアドレスとしてRAの送信元アドレスを設定し、さらにPMIPクライアントのRA送信元のLinklayerアドレスも取得し、RAの送信元アドレス(PMIPクライアントのアドレス)と対応付けて記憶しておく。これによって、初めてデフォルトGWにパケットを送る際にND(Neighbor Discovery)プロトコルの処理によってLinklayerアドレスを取得するための信号交換を省くことができ、効率が良くなる。但し、Linklayerアドレスを RAに含めないようにしても構わない。一方で、RAにDNSサーバアドレスを含む構成としても構わない。

[0163] d9の処理で、移動端末3はPMIP動作することを決定し、さらに必要なIPアドレス設定も完了した後、CN2との通信を開始することができる(図11のd10)。

[0164] 次に、移動端末3がアクセスネットワーク(A)200に接続した場合で、ネットワークのポリシによってCMIP動作を許可された場合の動作を、図1と図12とを参照して説明する。

[0165] 図12のe1からe3までの処理は、図11のd1からd3までの処理と同じである。e4の処理では、図11のd4の処理とは違い、ポリシ蓄積サーバ12から"CMIP許可"が応答される。

[0166] e5の処理では、e2の処理での移動端末3から送られた"CMIP要求"と、e4の処理で応答された"CMIP許可"の情報と、図8に示したPMIP、CMIP動作判定手順にしたがって移動端末3の動作を決定する。結果としては、"CMIP動作"が選択される。

[0167] e6の処理ではRAを移動端末3に送信する。RAには、option部分にCMIPでの動作を指定するための"CMIP"情報と、移動端末3がCMIP動作をするために必要なHAアドレスとForeign prefixとを格納する。そして、RAの基本情報部分には移動端末3がHoAを生成するためのHome prefixとPMIPクライアントのRAを送信したI/FのLinklayerアドレスとを格納する。この場合、上述したように、本発明の端末制御情報を認識できない移動端末はPMIP動作となる。

[0168] e6の処理で受信したRAの"CMIP"情報によって、移動端末3はCMIP動作することを決定する(図12のe7)。さらに、移動端末3はRAに格納されたHome prefix、Foreign prefixからそれぞれHoA、CoAを生成し、自らにHoA、CoAを割当てた後、同じくRAに格納されたHAアドレス宛にHoAとCoAとの対応を登録するためにBUを送信する(図12のe8)。移動端末3はBUの応答としてBAを受信し(図12のe9)、その後、CN2との通信を開始することができる(図12のe10)。

[0169] 次に、移動端末3がアクセスネットワーク(C)400に接続した場合の動作を、図1と図13とを参照して説明する。図13のf1, f2の処理は、図11のd1, d2の処理と同じである。

[0170] GW15は、PMIPクライアント機能を備えていないため、f2の処理でRSを受信すると、CMIP動作が要求されているか否かに関わらず、移動端末3の動作をCMIPに決定し(図13のf3)、RAを移動端末3に送信する(図13のf4)。RAには、option部分にCMIPでの動作を指定するための"CMIP"情報と、移動端末3がCMIP動作をするために必要なHAアドレスと、移動端末3がHoAを生成するために用いるHome prefixとを格納する。そして、RAの基本情報部分には移動端末3がCoAを生成するためのForeign prefixとPMIPクライアントのRAを送信したI/FのLinklayerアドレスとを格納する。

[0171] この場合、本発明の端末制御情報を認識できない移動端末はCMIP動作となる。但し、この場合、移動端末3はRFC3775に記述されたDynamic Home Agent

Address Discoveryや事前に設定しておく等の方法でHAを発見し、さらにHoAを取得する処理が必要となる。

[0172] f4の処理で受信したRAの"CMIP"情報によって、移動端末3はCMIP動作することを決定する(図13のf5)。さらに、移動端末3はRAに格納されたHome prefix、Foreign prefixからそれぞれHoA、CoAを生成し、自らにHoA、CoAを割当てた後、同じくRAに格納されたHAアドレス宛にHoAとCoAとの対応を登録するためにBUを送信する(図13のf6)。移動端末3はBUの応答としてBAを受信し(図13のf7)、その後、CN2との通信を開始することができる(図13のf8)。

[0173] 次に、移動端末3がハンドオーバする状況を考慮する。まず、移動端末3が、アクセスネットワーク(A)200からアクセスネットワーク(B)300へハンドオーバする場合のように、PMIPをサポートするアクセスネットワークへハンドオーバするケースについて考える。

[0174] この場合の動作は、図11あるいは図12のアクセスネットワーク(A)200に接続した場合と同じとして構わない。この場合、図11、図12のPMIPクライアントは、PMIPクライアント(B)14となる。但し、移動端末3がアクセスネットワーク(B)300に接続した際にPMIPクライアントや移動端末3がBUを送信するために必要な情報(HoA、HAアドレス、HAへの位置登録をセキュアに行うための鍵情報等)を認証サーバ16に問合せるのではなく、ハンドオーバ元のPMIPクライアント(A)13から取得する方式としても構わない。

[0175] この時、ハンドオーバ元のPMIPクライアントがどれであるかは、アクセスネットワークに配置されたBS(Base Station)から通知することができる。あるいは、上記の非特許文献1に示されたASN Functional Entityのようなものを利用することができる。しかしながら、具体的な方法は、本発明に直接関係がないので、その詳細な説明については省略する。

[0176] また、ハンドオーバの場合には、移動端末3がHoAを既に取得しており、このHoAは通信を継続する間、保持し続けるアドレスであるため、図11のd8の処理においてRAに含める情報の中からHome prefixを省略しても構わない。

[0177] 次に、移動端末3が、アクセスネットワーク(B)300からアクセスネットワーク(C)400

へハンドオーバする場合のようにPMIPがサポートしないアクセスネットワークへハンドオーバするケースについて考える。

[0178] この場合の動作は、図13のアクセスネットワーク(C)6に接続した場合と同じとして構わない。但し、移動端末3がアクセスネットワーク(C)6に接続した際に、移動端末3がBUを送信するために必要な情報(Home prefix、HAアドレス、HAへのBUをセキュアに行うための鍵情報等)を認証サーバ16に問合せるのではなく、ハンドオーバ元のPMIPクライアント(B)14から取得する方式としても構わない。

[0179] また、ハンドオーバの場合には、移動端末3がHoAを既に取得しており、このHoAは通信を継続する間、保持し続けるアドレスであるため、図13のf4の処理においてRAに含める情報の中からHome prefixを省略しても構わない。

[0180] 本実施の形態では、移動端末3とPMIPクライアント(A)13、PMIPクライアント(B)14、GW15との間での情報のやり取りに、RS、RAを利用することとしているが、必ずしもRS、RAである必要はなく、例えば、IPCPv6 configure－request、IPCPv6 configure－Ackを使用することができる。

[0181] 本実施の形態で示した拡張情報を含むRSの送信や拡張情報が含まれたRAの解釈をサポートする移動端末3は、CMIP機能を備えていることを想定しているが、これは、現実的にはSimple IP端末が一般的なIP端末と異なる動作をするとの前提を設けづらいためである。しかしながら、Simple IP端末が本発明の移動端末3としての機能を備えていても構わない。

[0182] また、本実施の形態では、移動端末3がCMIPで動作する要求を送信する場合を考慮しているが、例えば、PMIP機能を提供可能なアクセスネットワークに接続した場合は必ずPMIPで動作するとのポリシとすれば、移動端末3が送信するRSは、本発明の拡張要素を含まない一般的なRSとしても構わない。この場合は、ポリシ蓄積サーバ12への問合せも省略することができる。

[0183] さらに、本実施の形態ではRAによって、移動端末3に通知するIP情報としてDNS(Domain Name System)サーバアドレスを含めていないが、DNSサーバアドレスを含めるようにしても構わない。

[0184] このように、本実施の形態では、移動端末3の動作要求情報や端末の動作制御情

報をそれぞれ、RS、RAに格納することで、MIPv6を備えた移動端末3においても高速なPMIP、CMIP動作の決定とそれぞれでのIP設定が可能となる。

[0185] 上述した本発明は、3GPP(3rd Generation Partnership Project)や3GPP2、あるいはWiMAX Forumで策定しているモバイル向けネットワークのように、PMIP端末とCMIP端末とが共存する環境において有効である。

[0186] また、標準化団体によって、PMIPクライアントやモビリティアンカーの名称やモビリティ機能以外の機能配置等、異なる点はあるが、モビリティ機能はMIPv4、MIPv6プロトコルを使用しており、本発明の適用が可能である。さらに、先の標準化団体が検討しているネットワークは、数千万台程度の端末を収容するネットワークとなる。このようなネットワークでは信号交換の効率化やネットワークへの接続時、あるいはハンドオーバ時に迅速なサービス提供を可能とすることが極めて重要な課題となり、本が詰め胃によると、この課題の解決ないしは低減が可能となる。

[0187] 本出願は、2007年2月13日に出願された日本出願特願2007−031508号を基礎とする優先権を主張し、その開示の全てをここに取り込む。

請求の範囲

[1] PMIP[Proxy MIP(Mobile Internet Protocol)]機能を持つネットワーク機器が配備されたネットワークにおいて移動端末の動作を制御する移動端末管理システムであって,

前記ネットワーク側から前記移動端末側に前記PMIP機能を提供可能か否かを通知することを特徴とする移動端末管理システム。

[2] 前記移動端末は、自端末がCMIP(Client MIP)機能を備えている時に前記CMIP機能の通知及び前記CMIP機能の使用の要求のうちの少なくともいずれかを前記ネットワーク側に送信することを特徴とする請求項1記載の移動端末管理システム。

[3] 前記ネットワーク機器は、前記移動端末からの要求、前記ネットワーク側のポリシ、前記PMIP機能の有無、それらの組合せのいずれかによって前記移動端末をPMIP動作とするかCMIP動作とするかを決定する手段と、その決定した動作を前記移動端末に通知する手段とを含むことを特徴とする請求項2記載の移動端末管理システム。

[4] 前記ネットワーク機器は、前記決定した動作を前記移動端末に通知するとともに、前記決定した動作を実行する上で必要となる設定情報を前記移動端末に送出し、

前記移動端末は、前記PMIP動作とするかCMIP動作とするかを決定した際に、その動作に必要な設定を行うことを特徴とする請求項3記載の移動端末管理システム。

[5] 前記ネットワーク側と前記移動端末との間の通知を、MIP端末及びIP(Internet Protocol)端末において使用するプロトコルの拡張部分にかつ当該拡張部分を解釈できないノードにおいてその拡張部分が無視される性質を有する拡張部分に格納することを特徴とする請求項1から請求項4のいずれか記載の移動端末管理システム。

[6] 前記ネットワーク側と前記移動端末との間の信号に、前記通知をやり取りしないCMIP端末の動作を制御するための情報を格納することを特徴とする請求項5記載の移動端末管理システム。

[7] 前記プロトコルは、MIPv4(Mobile Internet Protocol version 4)を使用する場合に、AS(Agent Solicitation)、AA(Agent Advertisement)であることを特徴とする請求項5または請求項6記載の移動端末管理システム。

[8] 前記プロトコルは、MIPv6(Mobile Internet Protocol version 7)を使用する場合に、RS(Router Solicitation)、RA(Router Advertisement)であることを特徴とする請求項5または請求項6記載の移動端末管理システム。

[9] 前記ネットワーク機器は、3GPP－A(3GPP－Anchor)、MME(Mobility Management Entity)／UPE(User Plane Entity)、PDG(Packet Data Gateway)、PDSN(Packet Data Serving Node)、PDIF(Packet Data Interworking Function)、ASN(Access Service Network)－GW(GateWay)のいずれかであることを特徴とする請求項1から請求項8のいずれか記載の移動端末管理システム。

[10] PMIP[Proxy MIP(Mobile Internet Protocol)]機能を持つネットワーク機器が配備されたネットワークにおいて移動端末の動作を制御する移動端末管理システムを構成するネットワーク機器であって、

前記移動端末側に対して前記PMIP機能を提供可能か否かを通知することを特徴とするネットワーク機器。

[11] 前記移動端末がCMIP(Client MIP)機能を備えている時に前記CMIP機能の通知及び前記CMIP機能の使用の要求のうちの少なくともいずれかを前記移動端末から受信することを特徴とする請求項10記載のネットワーク機器。

[12] 前記移動端末からの要求、前記ネットワーク側のポリシ、前記PMIP機能の有無、それらの組合せのいずれかによって前記移動端末をPMIP動作とするかCMIP動作とするかを決定する手段と、その決定した動作を前記移動端末に通知する手段とを含むことを特徴とする請求項11記載のネットワーク機器。

[13] 前記決定した動作を前記移動端末に通知するとともに、前記決定した動作を実行する上で必要となる設定情報を前記移動端末に送出し、

前記移動端末が、前記PMIP動作とするかCMIP動作とするかを決定した際に、その動作に必要な設定を行うことを特徴とする請求項12記載のネットワーク機器。

[14] 前記移動端末との間の通知を、MIP端末及びIP(Internet Protocol)端末において使用するプロトコルの拡張部分にかつ当該拡張部分を解釈できないノードにおいてその拡張部分が無視される性質を有する拡張部分に格納することを特徴とする

請求項10から請求項13のいずれか記載のネットワーク機器。

[15] 前記移動端末との間の信号に、前記通知をやり取りしないCMIP端末の動作を制御するための情報を格納することを特徴とする請求項14記載のネットワーク機器。

[16] 前記プロトコルは、MIPv4(Mobile Internet Protocol version 4)を使用する場合に、AS(Agent Solicitation)、AA(Agent Advertisement)であることを特徴とする請求項14または請求項15記載のネットワーク機器。

[17] 前記プロトコルは、MIPv6(Mobile Internet Protocol version 7)を使用する場合に、RS(Router Solicitation)、RA(Router Advertisement)であることを特徴とする請求項14または請求項15記載のネットワーク機器。

[18] 3GPP－A(3GPP－Anchor)、MME(Mobility Management Entity)／UPE(User Plane Entity)、PDG(Packet Data Gateway)、PDSN(Packet Data Serving Node)、PDIF(Packet Data Interworking Function)、ASN(Access Service Network)－GW(GateWay)のいずれかであることを特徴とする請求項10から請求項17のいずれか記載のネットワーク機器。

[19] PMIP[Proxy MIP(Mobile Internet Protocol)]機能を持つネットワーク機器が配備されたネットワークにおいて移動端末の動作を制御する移動端末管理システムに用いる移動端末動作制御方法であって、

前記ネットワーク側から前記移動端末側に前記PMIP機能を提供可能か否かを通知することを特徴とする移動端末動作制御方法。

[20] 前記移動端末がCMIP(Client MIP)機能を備えている時に前記CMIP機能の通知及び前記CMIP機能の使用の要求のうちの少なくともいずれかを前記移動端末から前記ネットワーク側に送信することを特徴とする請求項19記載の移動端末動作制御方法。

[21] 前記ネットワーク機器が、前記移動端末からの要求、前記ネットワーク側のポリシ、前記PMIP機能の有無、それらの組合せのいずれかによって前記移動端末をPMIP動作とするかCMIP動作とするかを決定する処理と、その決定した動作を前記移動端末に通知する処理とを実行することを特徴とする請求項20記載の移動端末動作制御方法。

[22] 前記ネットワーク機器が、前記決定した動作を前記移動端末に通知するとともに、前記決定した動作を実行する上で必要となる設定情報を前記移動端末に送出し、

前記移動端末が、前記PMIP動作とするかCMIP動作とするかを決定した際に、その動作に必要な設定を行うことを特徴とする請求項21記載の移動端末動作制御方法。

[23] 前記ネットワーク側と前記移動端末との間の通知を、MIP端末及びIP(Internet Protocol)端末において使用するプロトコルの拡張部分にかつ当該拡張部分を解釈できないノードにおいてその拡張部分が無視される性質を有する拡張部分に格納することを特徴とする請求項19から請求項22のいずれか記載の移動端末動作制御方法。

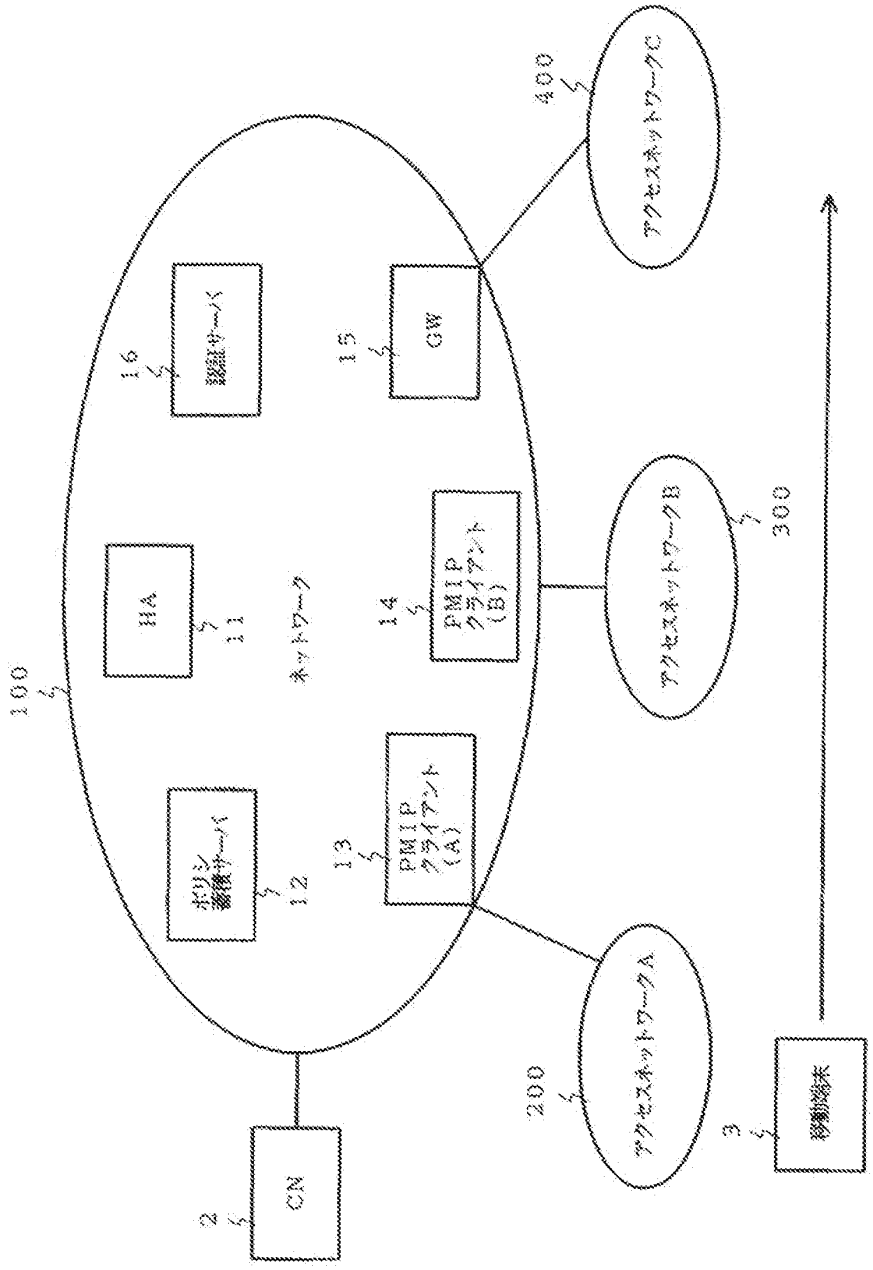
[24] 前記ネットワーク側と前記移動端末との間の信号に、前記通知をやり取りしないCMIP端末の動作を制御するための情報を格納することを特徴とする請求項23記載の移動端末動作制御方法。

[25] 前記プロトコルは、MIPv4(Mobile Internet Protocol version 4)を使用する場合に、AS(Agent Solicitation)、AA(Agent Advertisement)であることを特徴とする請求項23または請求項24記載の移動端末動作制御方法。

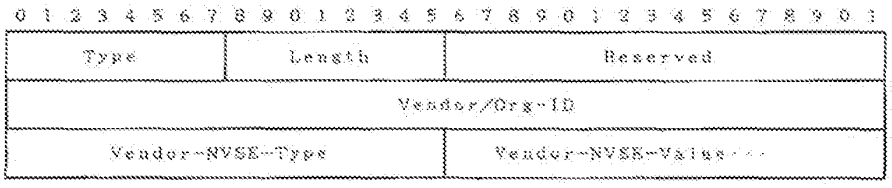
[26] 前記プロトコルは、MIPv6(Mobile Internet Protocol version 7)を使用する場合に、RS(Router Solicitation)、RA(Router Advertisement)であることを特徴とする請求項23または請求項24記載の移動端末動作制御方法。

[27] 前記ネットワーク機器は、3GPP－A(3GPP－Anchor)、MME(Mobility Management Entity)／UPE(User Plane Entity)、PDG(Packet Data Gateway)、PDSN(Packet Data Serving Node)、PDIF(Packet Data Interworking Function)、ASN(Access Service Network)－GW(GateWay)のいずれかであることを特徴とする請求項19から請求項26のいずれか記載の移動端末動作制御方法。

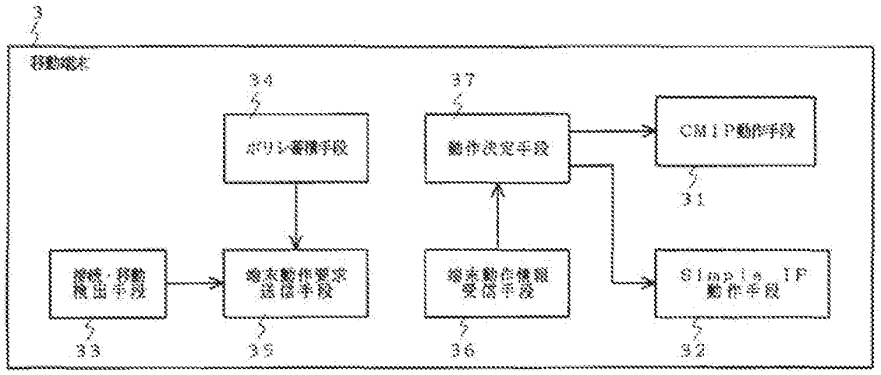
[図1]


100
ネットワーク
HA
11
AAA
認証サーバ
12
PMIP
クライアント
(A)
13
PMIP
クライアント
(B)
14
GW
15
認証サーバ
16
CN
2
アクセスネットワークA
200
アクセスネットワークB
300
アクセスネットワークC
400
移動端末
3

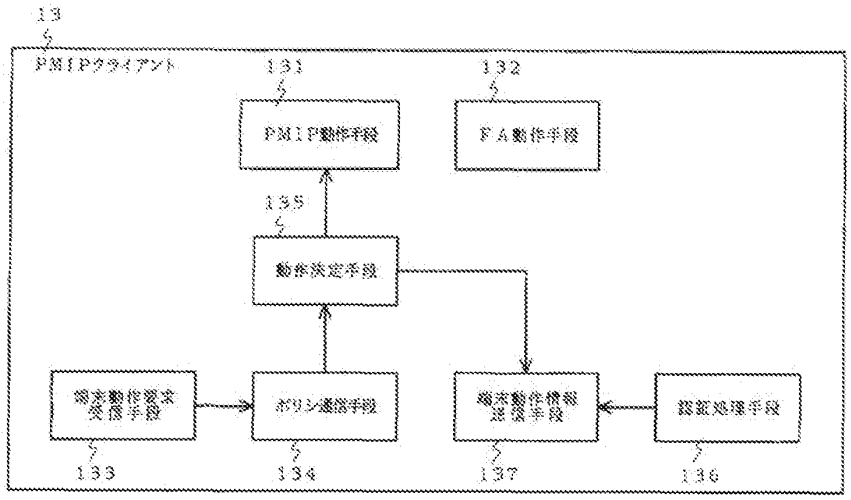
[図2]


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
Reserved
Vendor/Org-ID
Vendor-NVSE-Type
Vendor-NVSE-Value・・・

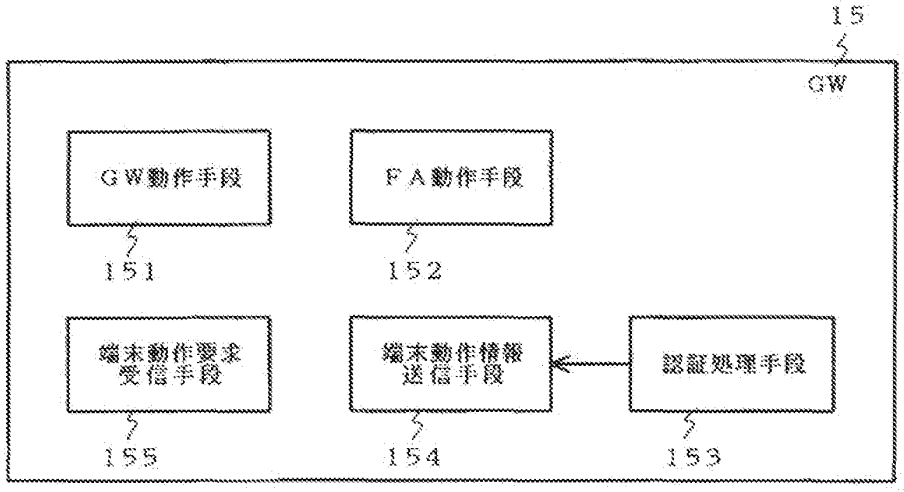
[図3]


3
34
37
CMIP動作手段
31
33
35
36
32

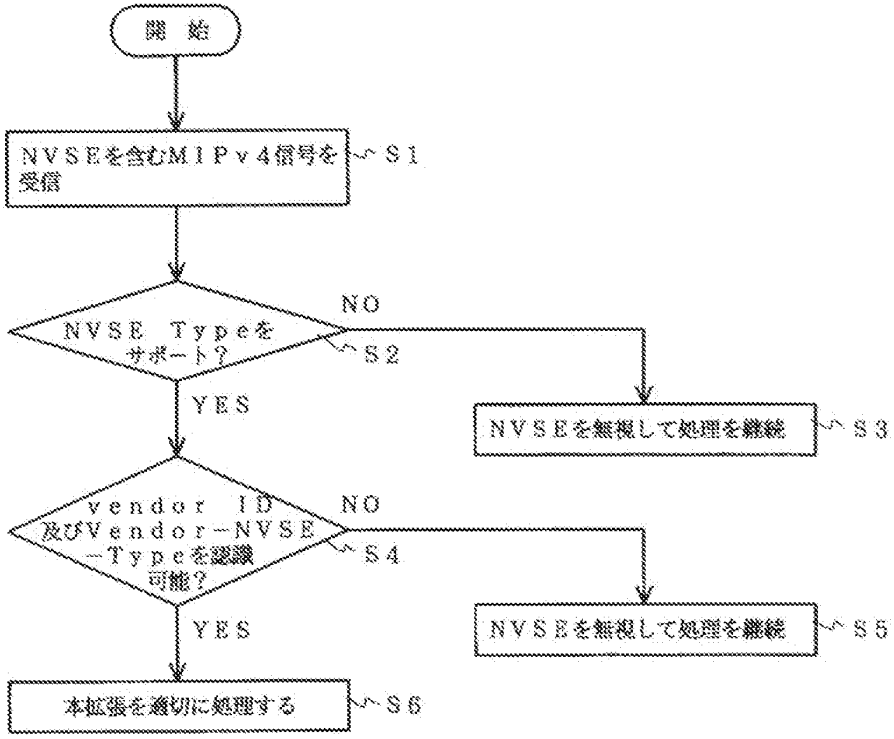
[図4]


13
PMIPクライアント
131
132
PMIP動作手段
FA動作手段
135
133
134
137
136

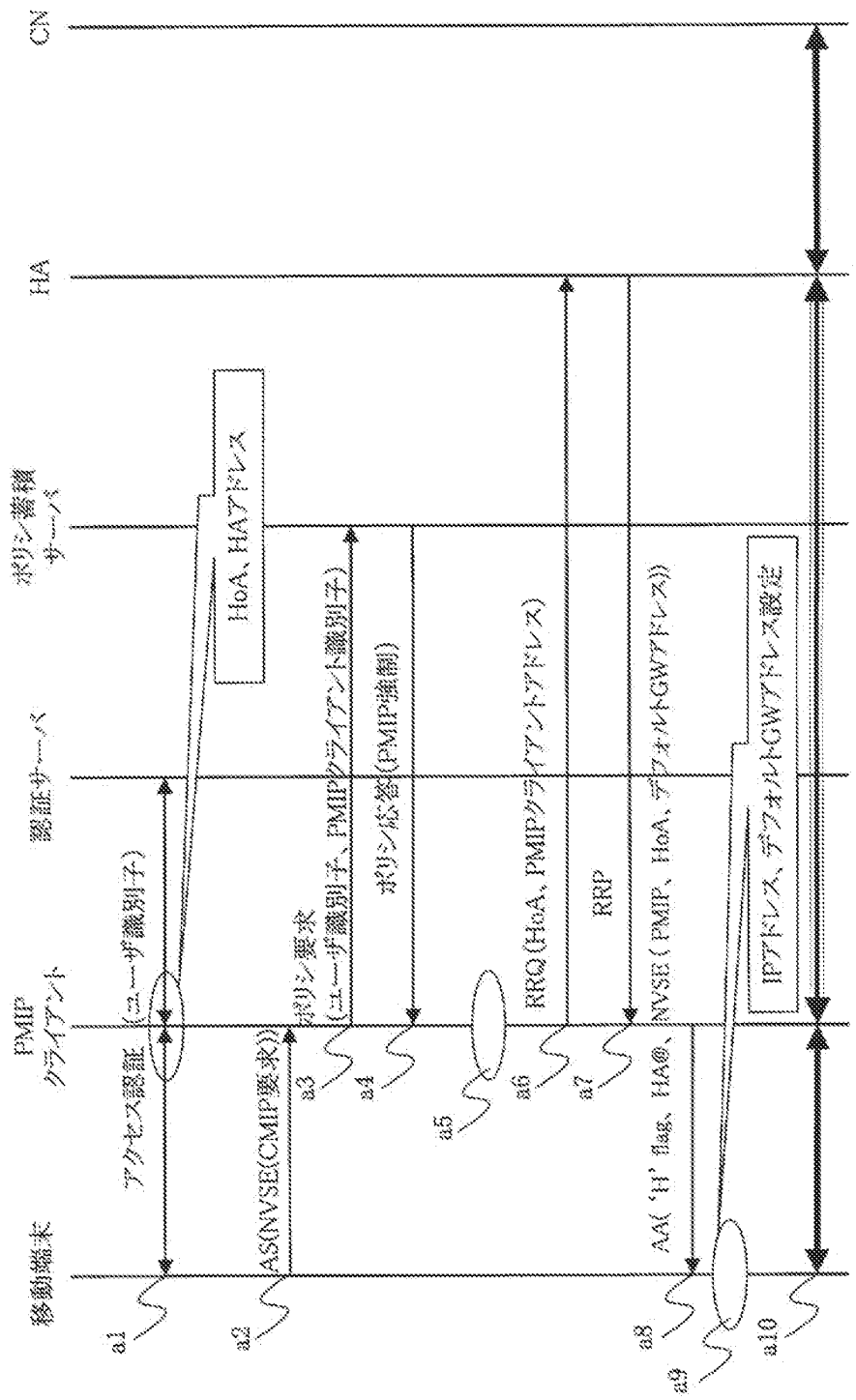
[図5]


15
GW
GW動作手段
FA動作手段
151
152
端末動作要求
受信手段
端末動作情報
送信手段
認証処理手段
155
154
153

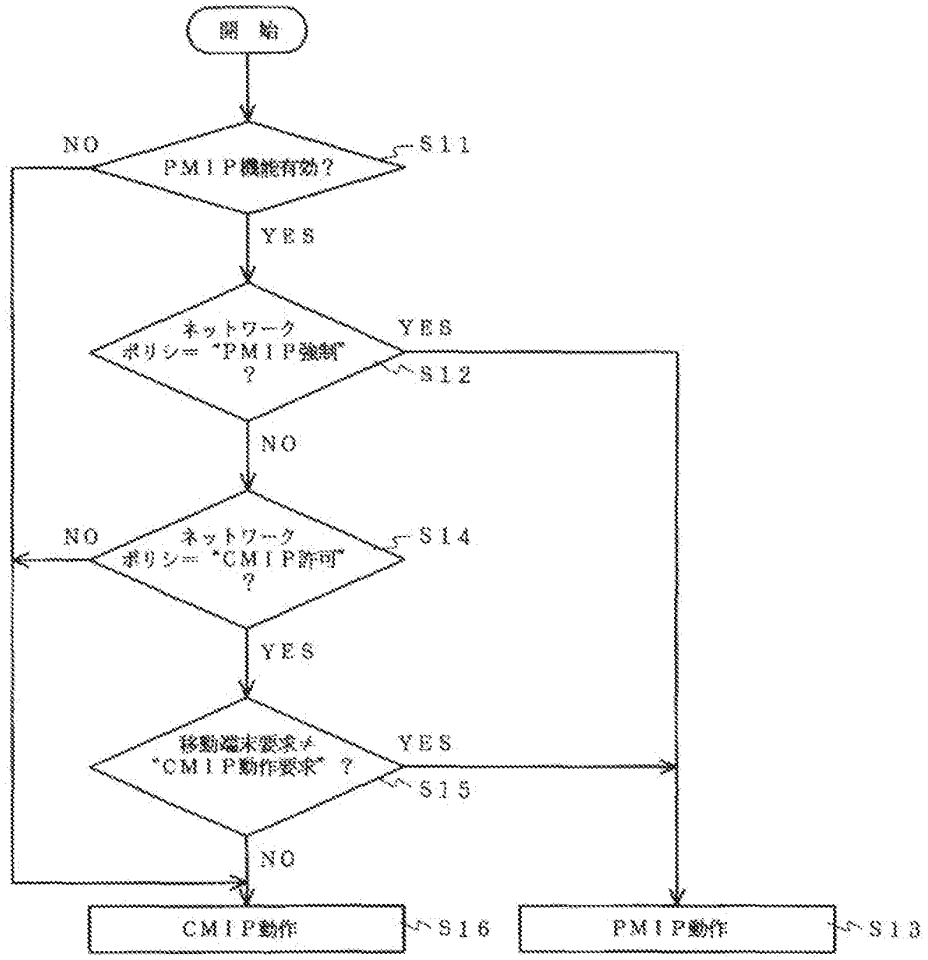
[図6]


開 始
NVSEを含むMIPv4信号を受信
S1
NVSE Typeをサポート?
NO
S2
YES
NVSEを無視して処理を継続
S3
Vendor ID及びVendor−NVSE−Typeを認識可能?
NO
S4
YES
NVSEを無視して処理を継続
S5
本拡張を適切に処理する
S6

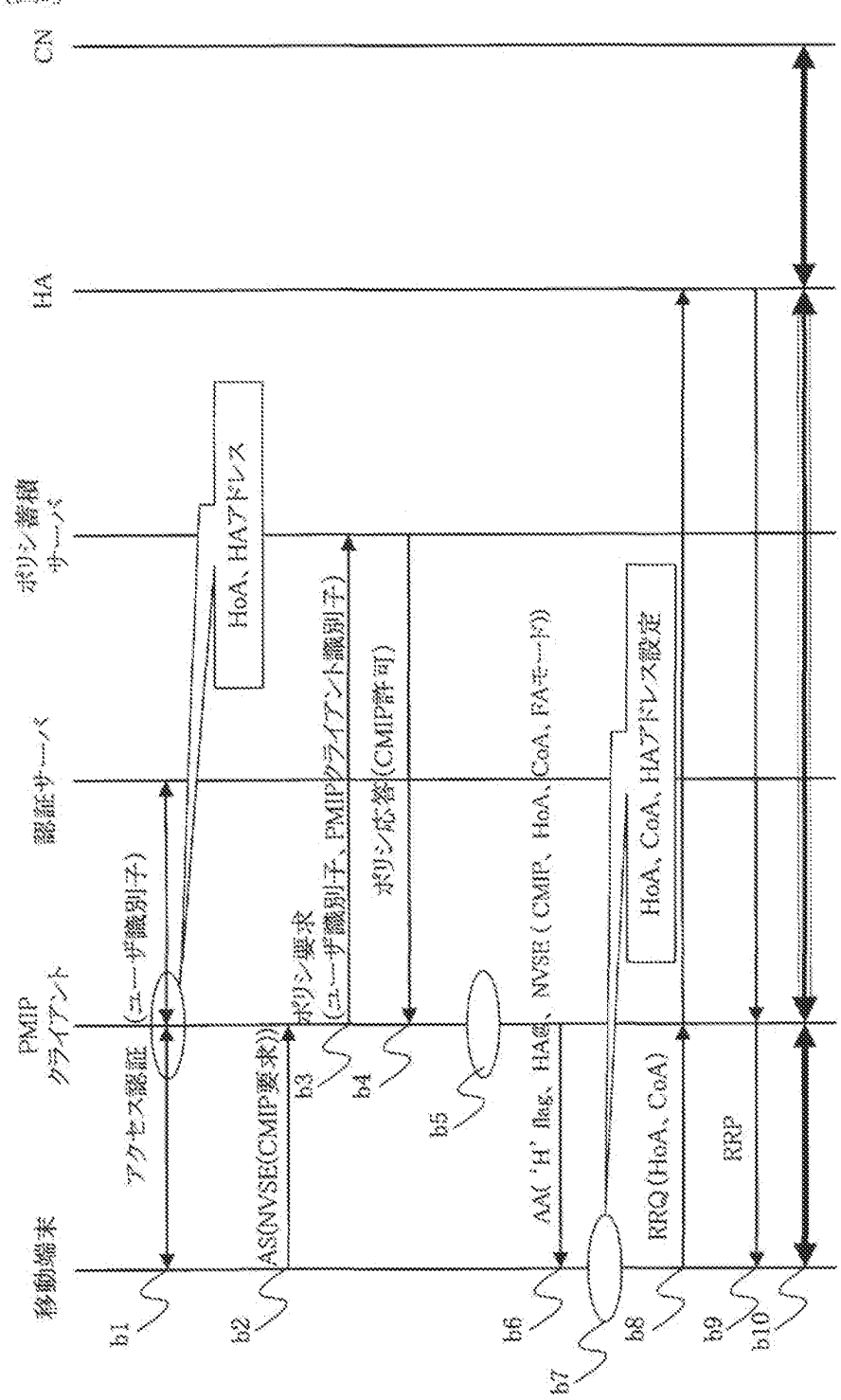
[図7]


CN
HA
ポリシ蓄積サーバ
認証サーバ
PMIPクライアント
移動端末
HoA、HAアドレス
アクセス認証（ユーザ識別子）
AS(NVSE(CMIP要求))
ポリシ要求（ユーザ識別子、PMIPクライアント識別子）
ポリシ応答(PMIP強制)
RRQ(HoA、PMIPクライアントアドレス)
RRP
AA('H' flag、HA@、NVSE(PMIP、HoA、デフォルトGWアドレス))
IPアドレス、デフォルトGWアドレス設定
a1
a2
a3
a4
a5
a6
a7
a8
a9
a10

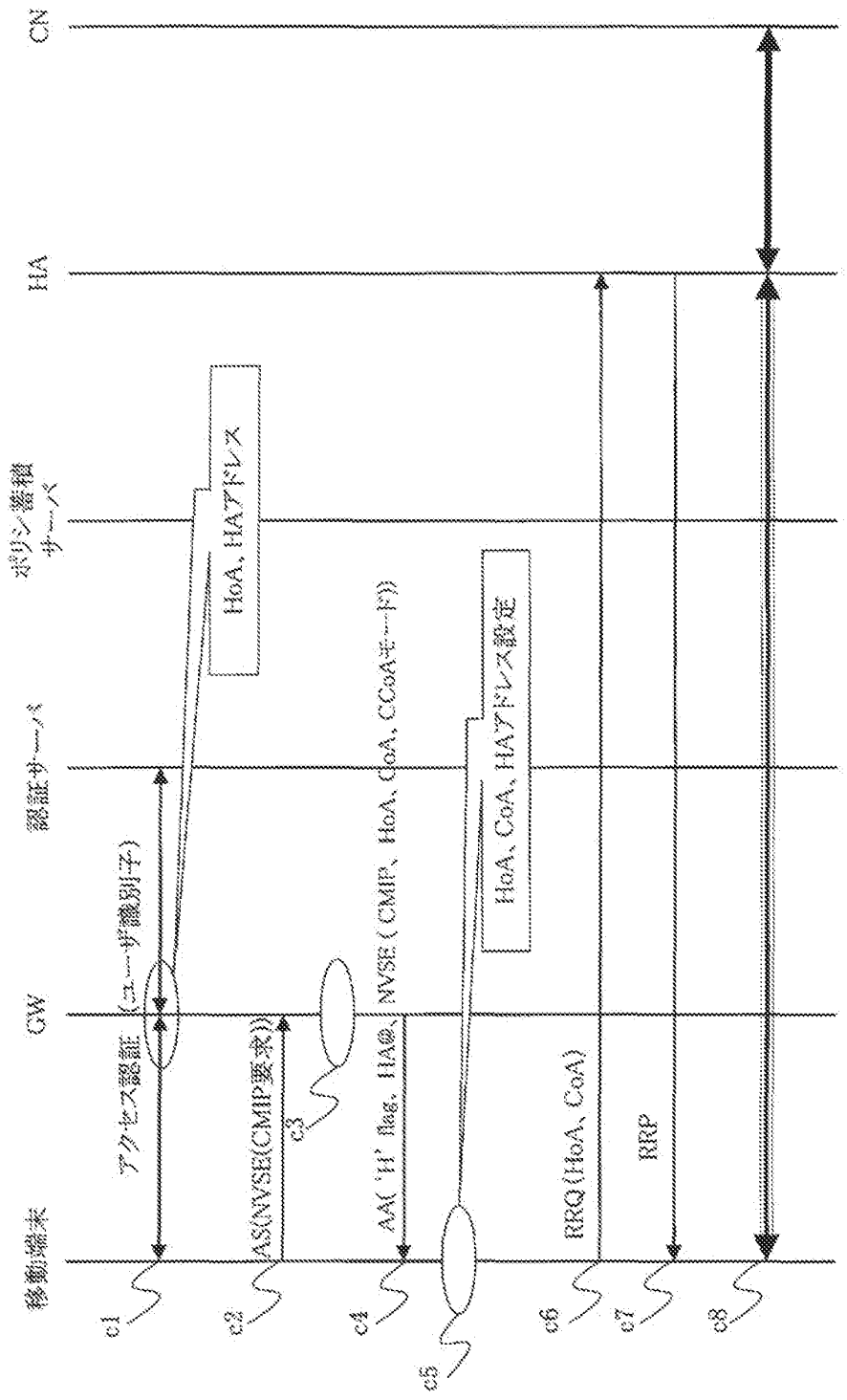
[図8]


開始
PMIP機能有効?
S11
NO
YES
ネットワークポリシー"PMIP強制"?
YES
S12
NO
ネットワークポリシー"CMIP許可"?
S14
NO
YES
移動端末要求が"CMIP動作要求"?
YES
S15
NO
CMIP動作
S16
PMIP動作
S13

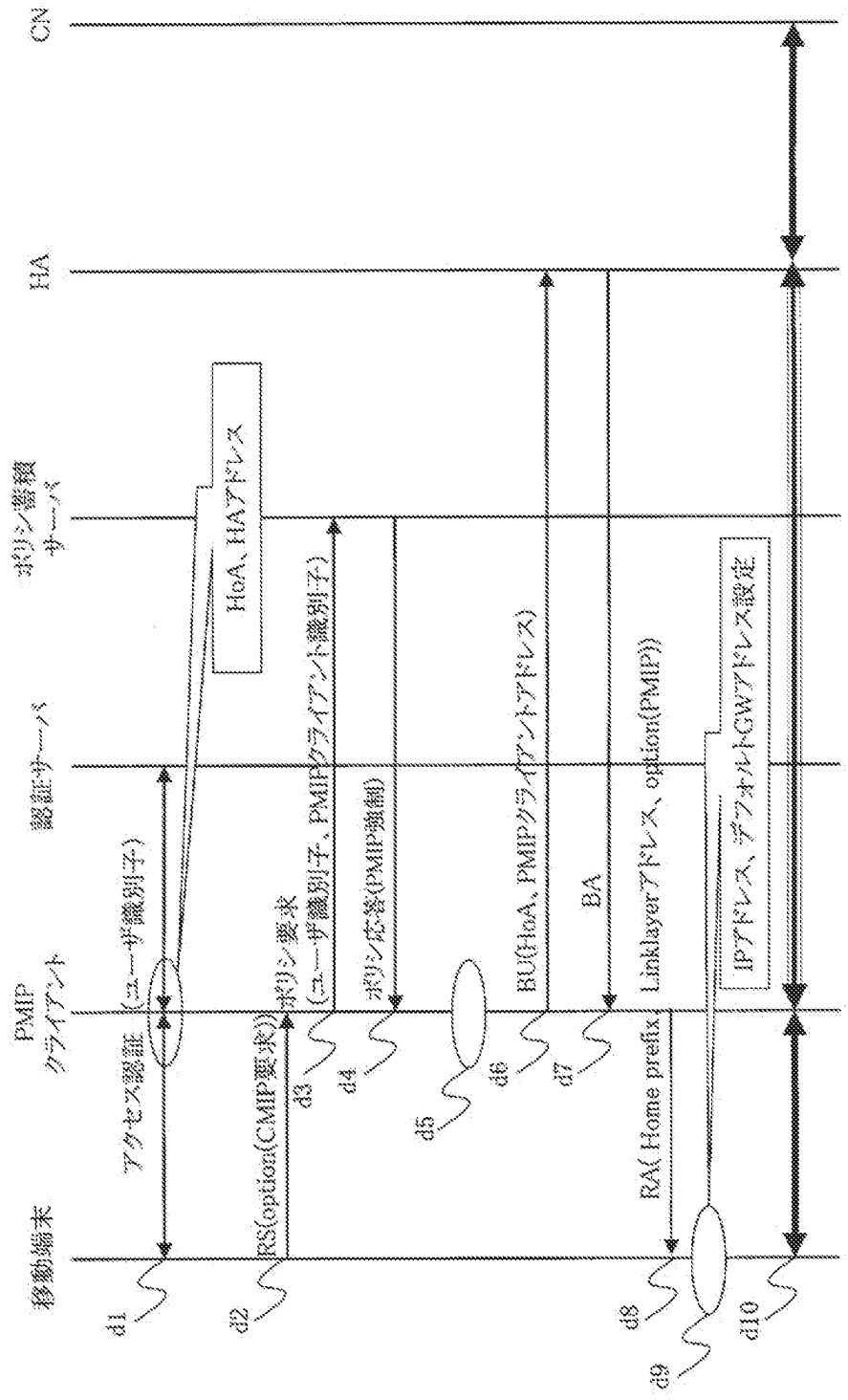
[図9]


CN
HA
ポリシー蓄積サーバ
認証サーバ
PMIPクライアント
移動端末
HoA、HAアドレス
アクセス認証
(ユーザ識別子)
AS(NVSE(CMIP要求))
ポリシー要求
(ユーザ識別子、PMIPクライアント識別子)
ポリシー応答(CMIP許可)
AA('H' flag、HAの、NVSE(CMIP、HoA、CoA、FAモード))
HoA、CoA、HAアドレス設定
RRQ(HoA、CoA)
RRP
b1
b2
b3
b4
b5
b6
b7
b8
b9
b10

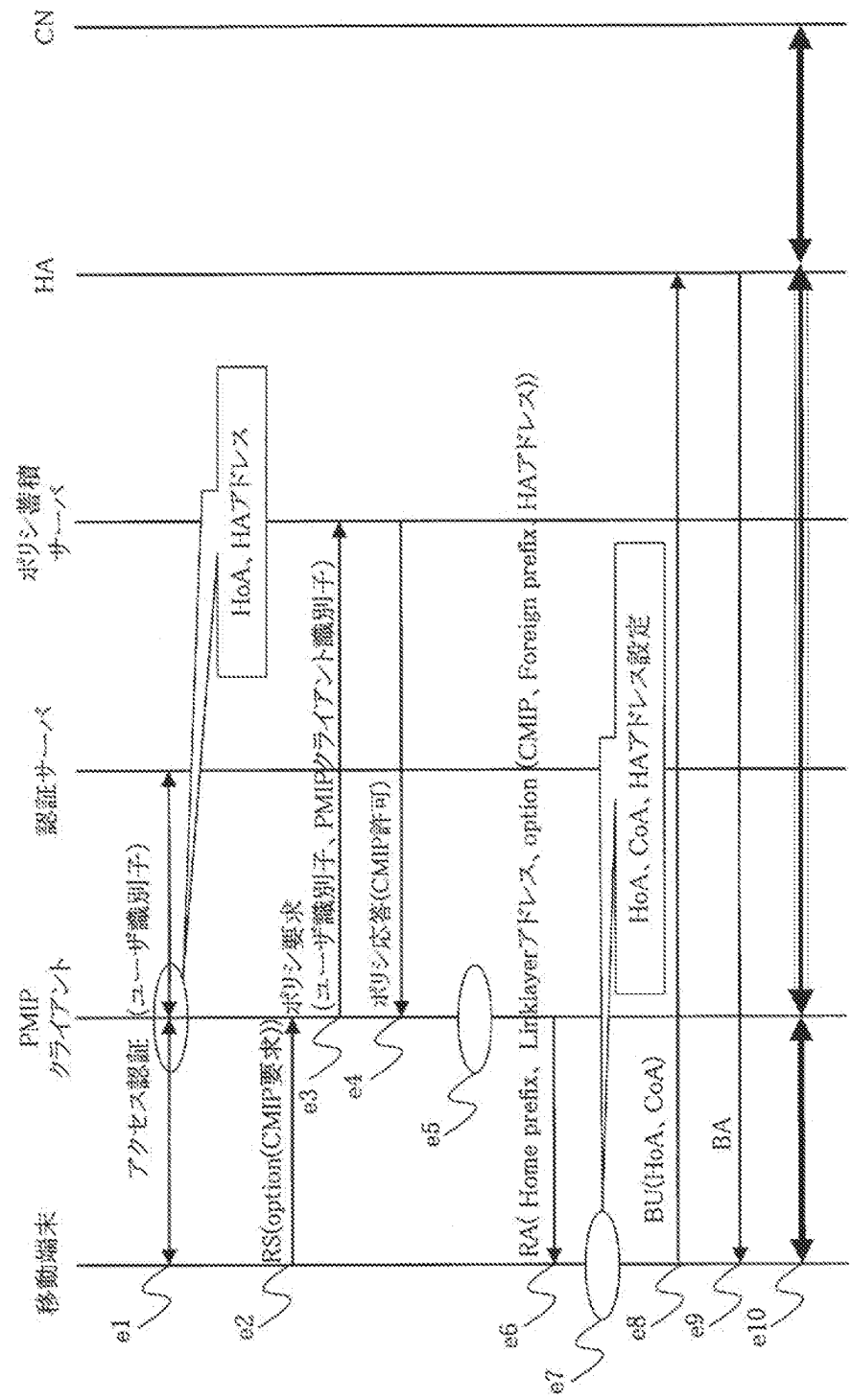
[図10]


CN
HA
ポリシ蓄積サーバ
認証サーバ
GW
移動端末
HoA、HAアドレス
アクセス認証（ユーザ識別子）
AS(NVSE(CMIP要求))
AA('1' flag、HA情報、NVSE(CMIP、HoA、CoA、CCoAキー))
HoA、CoA、HAアドレス設定
RRQ(HoA、CoA)
RRP
c1
c2
c3
c4
c5
c6
c7
c8

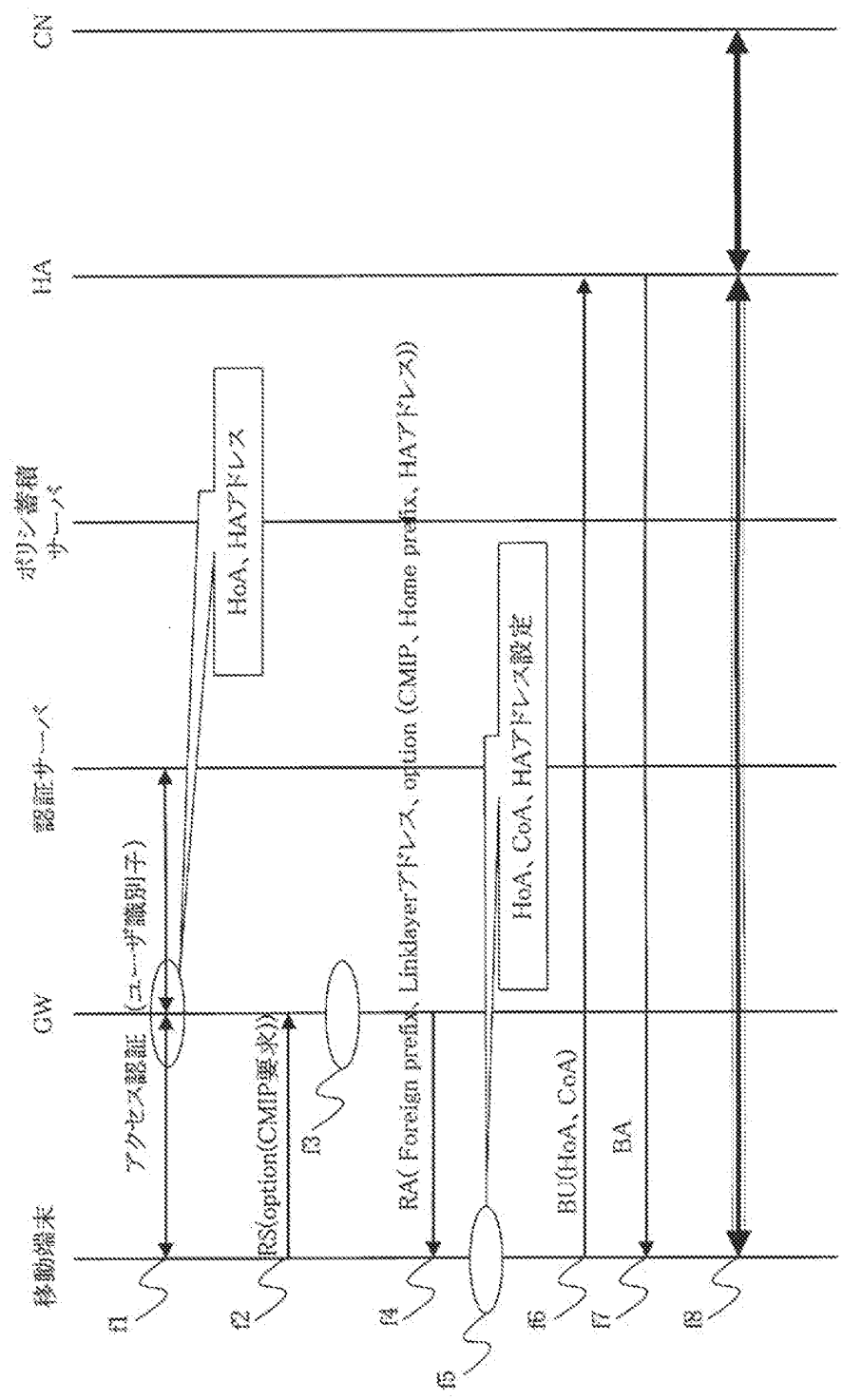
[図11]


CN
HA
ポリシー蓄積サーバ
認証サーバ
PMIPクライアント
移動端末
HoA、HAアドレス
アクセス認証
(ユーザ識別子)
RS(option(CMIP要求))
ポリシー要求
(ユーザ識別子、PMIPクライアント識別子)
ポリシー応答(PMIP強制)
BU(HoA、PMIPクライアントアドレス)
BA
RA(Home prefix
Linklayerアドレス、option(PMIP))
IPアドレス、デフォルトGWアドレス設定
d1
d2
d3
d4
d5
d6
d7
d8
d9
d10

[図12]


CN
HA
ポリシ蓄積サーバ
認証サーバ
PMIPクライアント
移動端末
HoA、HAアドレス
アクセス認証（ユーザ識別子）
RS(option(CMIP要求))
ポリシ要求（ユーザ識別子、PMIPクライアント識別子）
ポリシ応答(CMIP許可)
RA(Home prefix、Linklayerアドレス、option (CMIP、Foreign prefix HAアドレス))
HoA、CoA、HAアドレス設定
BU((HoA、CoA)
BA
e1
e2
e3
e4
e5
e6
e7
e8
e9
e10

[図13]


CN
HA
ポリシ蓄積サーバ
認証サーバ
GW
移動端末
アクセス認証（ユーザ識別子）
HoA、HAアドレス
RS(option(CMIP要求))
f3
RA(Foreign prefix、Linklayerアドレス、option (CMIP、Home prefix、HAアドレス))
HoA、CoA、HAアドレス設定
BU(HoA、CoA)
BA
f1
f2
f4
f5
f6
f7
f8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/052236

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/56(2006.01)i, H04Q7/38(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)
H04L12/56, H04Q7/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

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.
Y	S. Gundavelli et al., Proxy Mobile IPv6, draft-sgundave-mip6-proxymip6-01, IETF NETLMM WG, 2007.01.05, URL<http://www.watersprings.org/pub/id/draft-sgundave-mip6-proxymip6-01.txt> "6.9. Coexistence of CMIP & PMIP Nodes"	1-27
Y	JP 2005-160053 A (Matsushita Electric Industrial Co., Ltd.), 16 June, 2005 (16.06.05), Claims 16, 17; Par. Nos. [0056] to [0068] & EP 1603287 A1 & US 2006/0184692 A1 & WO 2005/039125 A1 & KR 6095729 A & CN 1788471 A	1-27

☒ 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
22 April, 2008 (22.04.08)	01 May, 2008 (01.05.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2007)

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2006-166456 A (Microsoft Corp.), 22 June, 2006 (22.06.06), Par. No. [0062] & KR 6063655 A & US 2006/0123128 A1 & EP 1667403 A2	5-8,14-17, 23-26
Y	WO 2005/125118 A1 (Matsushita Electric Industrial Co., Ltd.), 29 December, 2005 (29.12.05), Page 27, line 30 to page 28, line 11 & EP 1610502 A1 & JP 2008-503945	5-8,14-17, 23-26

国際調査報告	国際出願番号 PCT/JP2008/052226

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L12/56(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. H04L12/56

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2008年
日本国実用新案登録公報	1996－2008年
日本国登録実用新案公報	1994－2008年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	S. Gundavelli et al., Proxy Mobile IPv6, draft-sgundave-mip6-proxymip6-01, IETF NETLMM WG, 2007.01.05, URL<http://www.waterspring.org/pub/id/draft-sgundave-mip6-proxymip6-01.txt> "6.9. Coexistence of CMIP & PMIP Nodes"	1-27

☑ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
23.04.2008	01.05.2008

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5X	3865
日本国特許庁（ISA/JP） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	矢頭 尚之		
	電話番号 03-3581-1101 内線 3596		

様式PCT/ISA/210（第2ページ）（2007年4月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2005-160053 A（松下電器産業株式会社）2005.06.16, 請求項１６，１７および段落【００５６】－【００６８】 & EP 1603287 A1 & US 2006/0184692 A1 & WO 2005/039125 A1 & KR 6095729 A & CN 1788471 A	1-27
Y	JP 2006-166456 A（マイクロソフトコーポレーション）2006.06.22, 段落【００６２】 & KR 6063655 A & US 2006/0123128 A1 & EP 1667403 A2	5-8,14-17, 23-26
Y	WO 2005/125118 A1（松下電器産業株式会社）2005.12.29, 第２７ページ第３０行－第２８ページ第１１行 & EP 1610502 A1 & JP 2008-503945	5-8,14-17, 23-26

様式PCT/ISA/210（第2ページの続き）（２００７年４月）

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2007 (04.01.2007)

PCT

(10) International Publication Number
WO 2007/001833 A2

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2006/023005

(22) International Filing Date: 13 June 2006 (13.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/169,093 28 June 2005 (28.06.2005) US

(71) Applicant *(for all designated States except US)*: **SYMBOL TECHNOLOGIES, INC.** [US/US]; One Symbol Plaza, Holtsville, NY 11742 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LINSLEY-HOOD, Richard** [GB/GB]; 5 Park Lane, Bershire, Braclme RG42 4UL (GB). **D'AGOSTINO, Anthony** [US/US]; 57 Ridge Road, Smithtown, NY 11787 (US). **FAITH, Michael** [US/US]; 11 Woodrige Lane, Coram, NY 11727 (US). **LA ROSA, Dean, V.** [US/US]; 21 Westwind Drive, Bohemia, NY 11716 (US). **PERETZ, Eyal** [US/US]; 3 Singingwood Drive, Stony Brook, NY 11790 (US). **STILL, Gary** [US/US]; 44 Sherman Avenue, Plainview, NY 11803 (US). **UBRIACO, Charles** [US/US]; 1 Chris Court, Northport, NY 11768 (US). **ZANCOLA, Ronald** [US/US]; 2760 Lindenmere Drive, Merrick, NY 11566 (US).

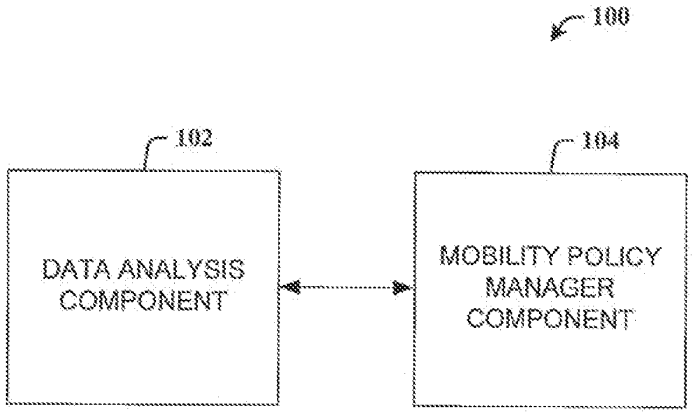
(74) Agents: **AMIN, Himanshu, S.** et al.; Amin & Turocy, LLP, 1900 E. 9th Street, 24th Floor, National City Center, Cleveland, OH 44114 (US).

(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, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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,

[Continued on next page]

(54) Title: MOBILITY POLICY MANAGER FOR MOBILE COMPUTING DEVICES



(57) Abstract: A mobile computing device that dynamically and automatically manages all network adapters on the device to obtain the best and most effective balance of network connectivity and power consumption without requiring operator or user application intervention. Performance is increased by lowering power consumption (longer battery life) and decreasing transaction latencies, providing a device that has flexibility and ease of use. According to one aspect is a system that includes a data analysis component that monitors parameters associated with a device and a mobility policy manager component that provides balance of network connectivity and power consumption based at least in part upon the monitored stimuli.

WO 2007/001833 A2

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.

Title: MOBILITY POLICY MANAGER FOR MOBILE COMPUTING DEVICES

TECHNICAL FIELD

[0001] The following description relates generally to computer systems, and more specifically to balancing network connectivity and managing power consumption of mobile computing devices.

BACKGROUND OF THE INVENTION

[0002] The usage of mobile communication systems utilizing mobile devices has become widespread. Mobile devices such as telephones, pagers, personal digital assistants (PDAs), data terminals, *etc.* are designed to be carried by those who travel from place to place. Each mobile device is capable of communicating by wireless communication between the mobile device and an access point to which the mobile device is registered. As the mobile device roams from one cell or geographic region to another, the mobile device will typically deregister with the access point of the previous cell and register with the access point associated with the new cell.

[0003] In general, when one network component transmits a signal to another network component, the transmitting network component typically expects a response from the receiving network component within a reasonable time frame. If a response is not received within the reasonable time (*e.g.*, lapsed time-out), communication usually terminates. In order to respond to such transmissions in a timely manner, many devices continuously operate in a high power (*e.g.*, full power) mode such that a device can continuously, periodically and/or on demand, monitor, receive and respond to incoming transmissions.

[0004] Current industry trend, however, is to minimize power consumption. Common techniques that mitigate power consumption include automatic power management utilities that transition a device to a lower power or "off" state. For example, many devices utilize standard power management technologies, such as Advanced Configuration and Power Interface (ACPI), which enable system software/firmware (*e.g.*, operating system or application) to control power by automatically transitioning the device to a low power state (*e.g.*, Standby, Suspend, Hibernate, Sleep, Deep Sleep…) when full power is not required. Typically, when the device transitions to the lower power state, network connections are terminated and power is removed from the CPU, volatile memory, transceivers, *etc.* The

foregoing can conserve power consumption and battery life, however, the device essentially is inoperable to communicate with the outside world until it transitions back to a higher power state.

[0005] Mobile computing devices lack the ability to configure and/or automatically and dynamically manage power consumption of multiple network adapters and cost of, or options for, use of network connectivity. This places a burden upon a user to either statically predict and set or manually configure the nominal operating mode periodically. This does not facilitate flexibility and/or adaptability during operation of the device. Therefore, what is needed is an optimum power-connectivity trade-off that can be continuously obtained and updated automatically and/or dynamically on a device.

SUMMARY OF THE INVENTION

[0006] The following presents a simplified summary of the invention in order to provide a basic understanding of some aspects of the invention. This summary is not an extensive overview of the invention. It is intended to neither identify key or critical elements of the invention nor delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented later.

[0007] The invention disclosed and claimed herein, in one aspect thereof, comprises a portable and/or mobile communication device that includes a data analysis component and a mobility policy manager component. The data analysis component monitors stimuli associated with a device. The stimuli can be at least one of network traffic, an internet protocol address, and a port number. The mobility policy manager (MPM) component provides balancing of network connectivity and power consumption based at least in part upon the monitored stimuli. The MPM component can include a policy module that determines a policy based at least in part on the monitored stimuli. The MPM component can include an alter module that alters at least one policy to provide an optimal device power consumption. Further included in the MPM component is a tolerance parameter module that ensures the policy remains within a predetermined power consumption range and/or a hysteresis module that prevents excessive altering between multiple device states. According to a further aspect, the MPM component can include a persistence module that allows the device to remain in a non-optimal state during a communication. Also included

can be a route module that hinders traffic in the absence of an appropriate route. The route module can include a firewall module that restricts traffic if an appropriate route is not available.

[0008] Still another aspect is a communication architecture including a network that includes a plurality of resources, a data analysis component that captures data about the plurality of resources, and a mobility policy manager (MPM) component. The MPM component can determine a policy to obtain efficient network connectivity and power consumption based at least in part on the captured data. The captured data includes at least one statistic based on network traffic associated with an Internet Protocol address or a port number end point. The MPM component can dynamically alter a predefined policy based at least in part upon the captured data.

[0009] According to a further aspect is a method for dynamically managing network connection performance. The method includes creating an initial policy, monitoring the initial policy, and automatically altering the initial policy to achieve at least one policy objective. The initial policy is created based upon at least one statistic derived from device conditions. Automatically altering the initial policy includes determining a state of a connection, ascertaining if the connection is complete, and maintaining the connection state until communication is complete.

[0010] Yet another aspect is a computer readable medium of a portable and/or mobile device to efficiently manage network connections. The computer readable medium includes a data analysis component operable to monitor device conditions and a mobility policy manager component that dynamically alters a policy to achieve at least one policy objective. The mobility policy manager provides balance of network connectivity and power consumption based at least in part on the monitored device conditions.

[0011] The following description and the annexed drawings set forth in detail certain illustrative aspects of the invention. These aspects are indicative, however, of but a few of the various ways in which the principles of the invention may be employed and the invention is intended to include all such aspects and their equivalents. Other advantages and novel features of the invention will become apparent from the following detailed description of the invention when considered in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 illustrates a system for managing network connectivity and power consumption.

[0013] FIG. 2 illustrates exemplary modules associated with a system that facilitates managing power consumption and network connectivity.

[0014] FIG. 3 illustrates exemplary modules associated with a system that facilitates managing power consumption and network connectivity.

[0015] FIG. 4 illustrates modules associated with a system that facilitates managing power consumption and network connectivity.

[0016] FIG. 5 illustrates a system for managing power consumption utilizing an artificial intelligence component.

[0017] FIG. 6 illustrates a flow chart of a methodology for optimal network connectivity and minimum power consumption utilizing one or more policies based on external and/or internal device conditions.

[0018] FIG. 7 illustrates a flow chart of a methodology for dynamically and automatically managing power consumption and enhancing network connectivity

[0019] FIG. 8 illustrates a flow chart of a methodology for determining transition of power states between a plurality of adapters.

[0020] FIG. 9 illustrates a schematic block diagram of a computer operable to execute the disclosed systems and/or methods.

[0021] FIG. 10 illustrates an exemplary device operative to execute the systems and/or methods disclosed herein.

[0022] FIG. 11 illustrates an exemplary networking environment that can be employed in connection with the invention.

[0023] FIG. 12 illustrates an exemplary operating environment that can be employed in connection with the invention.

DESCRIPTION OF THE INVENTION

[0024] The subject invention is now described with reference to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It may be evident, however, that the invention may be practiced without these specific details.

In other instances, well-known structures and devices are shown in block diagram form in order to facilitate describing the invention.

[0025] As used in this application, the terms "component," "module" and "system" are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution. For example, a component may be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components may reside within a process and/or thread of execution and a component may be localized on one computer and/or distributed between two or more computers.

[0026] The word "exemplary" is used herein to mean serving as an example, instance, or illustration. Any aspect or design described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other aspects or designs.

[0027] Furthermore, the invention may be implemented as a method, apparatus, or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof to control a computer to implement the disclosed invention. The term "article of manufacture" as used herein is intended to encompass a computer program accessible from any computer-readable device, carrier, or media. For example, computer readable media can include but are not limited to magnetic storage devices (*e.g.*, hard disk, floppy disk, magnetic strips…), optical disks (*e.g.*, compact disk (CD), digital versatile disk (DVD)…), smart cards, and flash memory devices (*e.g.*, card, stick). Additionally it should be appreciated that a carrier wave can be employed to carry computer-readable electronic data such as those used in transmitting and receiving electronic mail or in accessing a network such as the Internet or a local area network (LAN). Of course, those skilled in the art will recognize many modifications may be made to this configuration without departing from the scope or spirit of the subject invention.

[0028] Artificial intelligence based systems (*e.g.*, explicitly and/or implicitly trained classifiers) can be employed in connection with performing inference and/or probabilistic determinations and/or statistical-based determinations as in accordance with one or more aspects of the subject invention as described hereinafter. As used

herein, the terms "infer" and "inference" refer generally to the process of reasoning about or inferring states of the system, environment, and/or user from a set of observations as captured *via* events and/or data. Inference can be employed to identify a specific context or action, or can generate a probability distribution over states, for example. The inference can be probabilistic - that is, the computation of a probability distribution over states of interest based on a consideration of data and events. Inference can also refer to techniques employed for composing higher-level events from a set of events and/or data. Such inference results in the construction of new events or actions from a set of observed events and/or stored event data, whether or not the events are correlated in close temporal proximity, and whether the events and data come from one or several event and data sources. Various classification schemes and/or systems (*e.g.*, support vector machines, neural networks, expert systems, Bayesian belief networks, fuzzy logic, data fusion engines…) can be employed in connection with performing automatic and/or inferred action in connection with the subject invention.

[0029] Referring initially to FIG. 1, illustrated is a system 100 for managing network connectivity and power consumption. The system 100 can be implemented on any mobile device, such as a personal digital assistant (PDA), a mobile phone, a smart phone, a palm pilot, a personal data assistant, a mobile computer, a scanner, an RFID device, a laptop (or desktop) computer, a wearable computer device or any other mobile computing device.

[0030] The system 100 includes a data analysis component 102 that interfaces with a mobility policy manager component 104. The data analysis component 102 is adapted to receive, obtain, monitor, record, *etc.* stimuli and/or data (both internal and external to the device) that relates to connectivity and power consumption of the device. The data analysis component 102 is further adapted to analyze and evaluate such data and can provide statistics generated from such data. For example, the data analysis component 102 can obtain information relating to network traffic to and/or from an Internet Protocol address and/or port number end points or end point pairs. Port numbers allow different applications on the same device to utilize network resources without interfering with each other. The data analysis component 102 can further monitor power consumption to ensure that, through a policy, the power consumption remains within a predetermined range.

[0031] The data analysis component 102 interfaces with the mobility policy manager component 104 to allow a mobile computing device to dynamically and automatically manage all wide-area network (WAN), local-area network (LAN), personal area network (PAN), cradle, modem or other network adapters on a device. This facilitates an efficient and optimum balance of network connectivity and power consumption. In such a way, operator and/or user application interaction is mitigated after initial device configuration.

[0032] The mobility policy manager 104 receives the analyzed data from the data analysis component 102, such as in the form of statistics. The statistics are utilized to either create a predetermined fixed policy and/or to allow the mobility policy manager 104 to automatically evaluate the cost versus the performance requirements of the system to create and/or dynamically alter and maintain any such policy. The policy or set of policies are generated for use on the portable and/or mobile communication device and identify what actions should and/or should not be taken for a given set of stimuli. The policy, written in software, can be generated for use in a particular mobile communication environment. The policy can treat physical network adapters that allow multiple power settings internally as multiple separate logical adapters.

[0033] With reference now to FIG. 2, illustrated are modules associated with a system 200 that facilitates managing power consumption and network connectivity of a mobile computing device. The modules illustrated are exemplary and it is to be understood that more or less modules can be utilized and fall within the scope of the specification and appended claims. The mobility policy manager component 104 can include a policy module 202, an alter module 204 and/or a parameter module 206 that interface with each other and with the external data analysis component 102.

[0034] The policy module 202 can receive information, such as from the external data analysis component 102 and, based upon derived statistics, determine a policy to achieve an optimal balance of network connectivity and power consumption. The statistics can be collected ahead of time to allow for creating an initial policy. Thus, the policy can be predetermined and fixed, allowing no changes or alterations to such policy. Alternatively or in addition, the policy can be dynamic allowing the device to automatically evaluate the cost versus performance requirements of the device. The policy can be created and/or dynamically altered to maintain a policy that facilitates network connectivity and reduces power consumption.

[0035] An alter module 204 allows the policy to be dynamically updated based upon changing conditions (both internal and external) as received from the data analysis component 102. The alter module 204 utilizes the statistics, for example, and may limit or force particular modifications to a policy depending on the situation, such as allowing minimum and maximum outcomes to be predetermined through an interface with a parameter module 206. Thus, the policy can be dynamically altered to ensure that the policy is within an expected range or set of circumstances that provide the device with optimum connectivity and reduced power consumption.

[0036] FIG. 3 illustrates exemplary modules associated with a system 300 that facilitates managing power consumption and network connectivity. The exemplary modules illustrated can be utilized in conjunction with the one or more modules discussed with reference to FIG. 2 or they can be utilized separately. Included are a packet route management module 302, hysteresis module 304, duration module 306, persistence module 308, and/or route module 310. The mobility policy manager component 104 utilizes various parameters of a device to ensure that power consumption is reduced while allowing optimum network connectivity and device functionality. The mobility policy manager component 104 can specify an initial policy to establish and/or maintain the connectivity and/or functionality objectives and further can dynamically and/or autonomously update, modify, *etc.* the policy to ensure the objectives are met. This can be accomplished through the one or more modules associated with the system 300.

[0037] The packet route management module 302 is adapted to allow more than one network adapter associated with a device to be powered or active at any given time, such as a substantially similar time. In such a situation, the packet route management module 302 can analyze the various network adapters and routes and alter a policy to control the connectivity of the device. For example, each network adapter may be analyzed separately or concurrently with the other adapters to determine needed policy changes, if any, to ensure that each network adapter has optimum connectivity. The packet route management module 302 can be further adapted to stop a connection, either permanently or temporarily, if a particular connection is interfering with one or more other connections, or if a particular connection is experiencing problems, such as too much traffic on the network, slow network performance, unresponsive network connections, *etc.*

[0038] Another module associated with the mobility policy manger component 104 is a hysteresis module 304 that analyzes one or more network connections and determines the state of each connection. For example, the state of a network connection can be described as various levels of power consumption. These levels can include "off," "listening for network availability," "connected to a network," "receiving data", "transmitting data," *etc.* It is to be understood that each of these levels can include addition levels relating to, for example, the geographic distance between the terminal and an infrastructure transmitter depending on the network type. The levels can also be described as being hierarchically ordered, for example, from the least power consumption ("off") to the highest power consumption ("transmitting data"). The hysteresis module 304 is further adapted to prevent inefficient, continuous alternating between multiple states and may force the device into a particular state to improve device efficiency.

[0039] The duration module 306 is adapted to measure, obtain, determine, *etc.* the time interval/range spent at each of the power levels for any given connection. The time interval/range can include the amount of time taken to get to a particular state and the dwell time to transition out of such state. The time interval/range can also be measured as including the time spent in a particular state. Thus, the duration module 306 can construct a "total duty cycle" of power consumption for a given connection based on the time spent at a given power level and the power used at that level. This can be incorporated into the profile and/or statistic(s) where appropriate and any subsequent attempt to connect can be matched against such existing profile(s) to determine the most power effective manner to complete that connection. It should be understood that the measurement does not have to be "time" provided there is a measurement means that can determine the range in which a given connection is at a particular power level.

[0040] The hysteresis module 304 and the duration module 306 provide the mobility policy manager component 104 information to determine whether to switch to the next lower power usage adapter and/or whether to switch to a higher power usage adapter. The capacity to determine if it is valid to transition from a lower power state to the next higher one, or vice versa, is part of the consideration of the overall switching characteristics of the mobility policy manager component 104. The decision to switch to a next lower (or higher) power usage adapter can be determined by leaving it in a particular state and determining its availability at that level before,

moving it to a lower (or higher) state. A higher power usage adapter can then be transitioned to a lower power consumption state possible after some dwell time to allow for a degree of hysteresis.

[0041] A persistence module 308 is adapted to monitor one or more network connections and can work separately or in conjunction with the hysteresis module 304. The persistence module 308 can monitor the one or more network connections. If a particular connection is not complete (*e.g.*, data, information, messages, text is still being transferred to/from the device) the persistence module 308 can force the device to remain in a particular state for the duration of that particular connection. For example, it may be determined that the state of a particular connection is non-optimal. By non-optimal it is meant that the connection is inefficient, consumes excessive resources, is not the best configuration, *etc.* The persistence module 308 analyzes the connection and can determine that, although in a non-optimal state, the particular state should be maintained for the duration of that particular connection or connections. This allows for the correct completion of that particular communication. After the communication is complete, the persistence module 308 can allow the device to switch to a more optimal state.

[0042] A route module 310 is provided that can determine a network connection route, alter an existing route, force a particular route, and/or block or reject traffic if no appropriate route is available. Exemplary modules associated with the route module 310 are illustrated in FIG. 4 and can include an override module 402, a categorization module 404, and/or a firewall module 406. The exemplary modules 402-406 interface with each other and the other modules of the mobility policy manager 104 to provide systems and/or methods that balance network connectivity and manage power consumption of mobile devices.

[0043] The override module 402 provides input to the mobility policy manager 104 to alter the policy to allow for designated connections based upon one or more policy goal(s) and/or objective(s). The designated connections can be determined based upon statistics relating to such network connections. A determination can be made to designate a particular route or outcome by overriding other choices as determined by analysis of the statistics and/or policy. The override module 402 facilitates forcing the particular outcome or route though utilization of the designated connections. For example, if there is more than one adapter on a device, each having a different degree of power consumption, the mobility policy manager

component 104 is adapted to determine which adapter to utilize and can transition between the adapters, depending on the requirements of a particular connection. For example, if it is desired to download a large amount of data onto a device, the mobility policy manager component 104 can determine that speed is more important than power conservation (since more power generally equals more speed). In such a situation, the device will transition to the highest power/speed adapter, regardless of any policy power conservation requirements and/or objectives.

[0044] The connections can also be categorized though utilization of a categorization module 404. Such a categorization can analyze the requirements of creating a new route and/or maintaining an existing route. The categorization module 404 can prefer one requirement over the other. For example, the categorization module 404 can treat the requirements for creating a new route differently than the requirements of utilizing an existing route. In some situations, a new route can be preferred, while in other situations the existing route may be preferred. The categorization module 404 is adapted to analyze the requirements of both in relation to the policy goals, objectives, statistic information, and/or information obtained from other modules of the mobility policy component 104 and/or data analysis component 102.

[0045] There are some circumstances in which particular traffic may be blocked and/or rejected though utilization of a firewall module 406. If a determination is made that no appropriate route for a network connection exists, such a connection may be refused and/or hindered and connectivity not allowed. In this situation, the connection will need to be made or attempted at a different time when an appropriate route is available.

[0046] FIG. 5 illustrates a system 500 for managing power consumption that employs artificial intelligence (AI) which facilitates automating one or more features in accordance with the subject invention. The AI can be effected *via* AI component 502, as illustrated, that interfaces with an external data analysis component 102 and a mobility policy manager component 104.

[0047] The subject invention (*e.g.*, in connection with managing power consumption) can employ various AI-based schemes for carrying out various aspects thereof. For example, a process for determining the best and most effective balance of network connectivity and power consumption can be facilitated *via* an automatic classifier system and process. Moreover, where network adapters are employed

having the same or similar resources, the classifier can be employed to determine which network adapter to employ in a particular situation.

[0048] A classifier is a function that maps an input attribute vector, x = (x1, x2, x3, x4, *xn*), to a confidence that the input belongs to a class, that is, f(x) = *confidence(class)*. Such classification can employ a probabilistic and/or statistical-based analysis (*e.g.*, factoring into the analysis utilities and costs) to prognose or infer an action that a user desires to be automatically performed.

[0049] A support vector machine (SVM) is an example of a classifier that can be employed. The SVM operates by finding a hypersurface in the space of possible inputs, which hypersurface attempts to split the triggering criteria from the non-triggering events. Intuitively, this makes the classification correct for testing data that is near, but not identical to training data. Other directed and undirected model classification approaches include, *e.g.*, naïve Bayes, Bayesian networks, decision trees, neural networks, fuzzy logic models, and probabilistic classification models providing different patterns of independence can be employed. Classification as used herein also is inclusive of statistical regression that is utilized to develop models of priority.

[0050] As will be readily appreciated from the subject specification, the subject invention can employ classifiers that are explicitly trained (*e.g.*, *via* a generic training data) as well as implicitly trained (*e.g.*, *via* observing user behavior, receiving extrinsic information). For example, SVM's are configured *via* a learning or training phase within a classifier constructor and feature selection module. Thus, the classifier(s) can be used to automatically learn and perform a number of functions, including but not limited to determining according to a predetermined criteria when to grant access, which stored procedure to execute, which policy objective/goal to conform to or override, *etc.* The criteria can include, but is not limited to, the amount of data or resources to accessed *via* a call, the type of data, the importance of the data, *etc.*

[0051] In view of the exemplary systems shown and described above, methodologies, which may be implemented in accordance with one or more aspects of the invention, will be better appreciated with reference to the diagram of FIGS. 6, 7, and 8. The systems and/or methodologies automatically and dynamically increase performance of a device while lowering power consumption (longer battery life) and decreasing transaction latencies, providing ease-of-use and device flexibility. While,

for purposes of simplicity of explanation, the methodologies are shown and described as a series of function blocks, it is to be understood and appreciated that the invention is not limited by the order of the blocks, as some blocks may, in accordance with the invention, occur in different orders and/or concurrently with other blocks from that shown and described herein. Moreover, not all illustrated blocks may be required to implement a methodology in accordance with one or more aspects of the invention. It is to be appreciated that the various blocks may be implemented *via* software, hardware, a combination thereof or any other suitable means (*e.g.* device, system, process, component) for carrying out the functionality associated with the blocks. It is also to be appreciated that the blocks are merely to illustrate certain aspects of the invention in a simplified form and that these aspects may be illustrated *via* a lesser and/or greater number of blocks.

[0052] FIG. 6 illustrates a flow chart of a methodology 600 for optimal network connectivity and minimum power consumption utilizing one or more policy based on external and/or internal device conditions. The method starts, at 602, where a policy is determined. The policy can be a fixed policy or a configurable policy and can be based on statistics derived prior to the policy being implemented. The statistics can be derived from network traffic to and/or from an Internet Protocol address and/or port number end points or end point pairs. The statistics can alternatively or in addition be derived from other stimuli, information, data, *etc.* derived from both an internal and/or an external environment of the device. For example, the stimuli can be information derived from a plurality of resources in a communication architecture. The plurality of resources can be other devices, data being communicated, network adapters, *etc.*

[0053] The statistics can be monitored and/or automatically evaluated, at 604, such that the policy can be altered to allow minimum and maximum outcomes to be pre-determined. The policy can be evaluated to ensure that the connectivity of a particular connection is at an optimal level, and if not at an optimal level to determine if the connection should be maintained based on other factors, such as a continuing communication. An objective of the policy can be to automatically evaluate the cost versus the performance requirements to create and/or dynamically alter and maintain any such policy.

[0054] At 606, the policy is altered, maintained, created, *etc.* based upon the evaluation performed. For example, the policy can be altered to control the

connectivity of the device, maintain the current device connectivity, *etc.* The policy can be modified to determine a particular network connection route, alter an existing route, force a particular route, and/or block or reject traffic if no appropriate route is available.

[0055] Referring now to FIG. 7, illustrated is a flow chart of a methodology 700 for dynamically and automatically managing power consumption of multiple network adapters and cost of, or options for, use of network connectivity. The method starts, at 702, where external and/or internal stimuli is gathered and, based on such stimuli, statistics are created. The statistics can relate to connectivity and/or power consumption of a mobile computing device. For example, the data can be related to network traffic to and/or from an Internet Protocol address and/or port number end points or end point pairs. The network traffic data can be utilized to derive statistics regarding network connectivity and the optimal connections, routes, options, *etc.* to both achieve efficient network communication and reduce costs associated with operating and maintaining a mobile computing device.

[0056] A policy is created based upon the derived statistics, at 704. The policy can be a fixed policy that does not allow changes or an adaptable policy that allows automatic evaluation of cost versus performance requirements. An automatic evaluation allows dynamic creation, alteration, maintenance, *etc.* of the policy to ensure that network connectivity and power consumption is at optimum levels.

[0057] Data relating to the operation, connectivity, power consumption, *etc.* of a mobile device is periodically and/or constantly analyzed, at 706, to ensure the objectives established by the one or more policies is being met. The performance of the device and its network connectivity is evaluated, at 708, based upon the analyzed data. The policy can be altered, at 710, if necessary to conform to the policy requirements. For example, the policy can be altered to allow for persistence of a non-optimal state for the duration of a particular connection or connections to allow for the correct completion of communication. The policy can allow for appropriate hysteresis to prevent inefficient or continuous alternating between multiple states that would otherwise result in inefficient communication. The policy can allow designated connections that override other choices to force a particular outcome or route. The policy can treat physical network adapters that allow multiple power settings internally as multiple separate logical adapters. The policy can be modified or adapted to establish and achieve objective relating to device connectivity and

reduced power consumption. The policy can further be utilized to perform other functions relating to conserving power while maintaining optimum network connectivity and data transfer.

[0058] With reference now to FIG. 8, illustrated is a flow chart of a methodology 800 for determining transition of power states between a plurality of radio or network adapters. For illustration purposes, the methodology will be discussed with reference to three network adapters ("A," "B," and "C"). It is to be understood that this methodology can be applied to two or more network adapters and is not to be limited by the following detailed description.

[0059] The method starts, at 802, with receipt of network adapter power requirements. The power requirements of each adapter can be ranked from the adapter with the highest power usage ("A") to the adapter with the lowest power usage ("C"). Methods of distinguishing between the states of each adapter other than a ranking can be utilized. It is also to be understood that adapters may have similar power usages and can be classified together.

[0060] At 804, the state of each adapter is received. The state can refer to the power level consumption and can be categorized in ranges consisting of an hierarchical order, such as 1 being the lowest power consumption and 5 being the highest power consumption. For example, the states can be "off" = 1; "listening for network availability" = 2; "connected to a network" = 3; "receiving data" = 4; and "transmitting data" = 5. It is to be understood that more or less power level consumption states can be utilized as well as each level having additional levels included therein. For example, the additional levels can relate to the geographic distance between the terminal and the infrastructure transmitter depending on the network type.

[0061] The method continues, at 806, where the availability of a particular adapter to transition to a lower or higher state is received. With continuing reference to the example above, adapter "A" consumes the most power and adapter "C" the least power. Thus, it would be advantageous to keep adapter "A" at the lowest power consumption state possible and adapter "C" in the highest power consumption state, if required. For example, the adapters can have the following initial state: adapter "A" = 1 (off); adapter "B" = 3 (connected to a network); and adapter "C" = 2 (listening for network availability). If adapter "C" indicates that it is capable of transiting to state 3, then the option to switch the state of adapter "C" becomes valid and adapter "C" can

change states with an adapter with a higher power consumption rate. Adapter "A", having the highest power consumption, would change to state 3 only if the adapter(s) having the lower power consumption (adapters "B" and "C" in this illustration) indicate it is no longer in coverage and is now unusable.

[0062] At 808, the adapters are changed to the appropriate state to comply with optimal power consumption and network connectivity as determined by policy goals and/or objective. For example, when adapter "C" transitions to state 3, adapter "B" can, in turn, transition to a lower state, such as state 1 or 2. By way of example, the initial states of the adapters could be "A" is in state 3; adapter "B" is in state 2; and adapter "C" is in state 1. Thus, the method would determine that the adapter with the highest power consumption ("A") is in the highest power state (3) and thus, if adapter "B" and/or adapter "C" is available, such adapter should transition to state 3 and adapter "A" transition to state 2 or lower. In this situation, the ideal transition would be for adapter "A" to transition to state 1 and adapter "C" to transition to state 3. However, policy objectives and/or goals might not allow such minimum levels of power consumption.

[0063] Referring now to FIG. 9, illustrated is a schematic block diagram of a portable and/or mobile hand-held terminal device 900 (similar to the portable scanning device 1000 as illustrated in FIG. 10) according to one aspect of the invention, in which a processor 902 is responsible for controlling the general operation of the device 900. The processor 902 is programmed to control and operate the various components within the device 900 in order to carry out the various functions described herein. The processor 902 can be any of a plurality of suitable processors. The manner in which the processor 902 can be programmed to carry out the functions relating to the invention will be readily apparent to those having ordinary skill in the art based on the description provided herein.

[0064] A memory 904 connected to the processor 902 serves to store program code executed by the processor 902, and serves as a storage means for storing information such as user credential and receipt transaction information and the like. The memory 904 can be a non-volatile memory suitably adapted to store at least a complete set of the information that is displayed. Thus, the memory 904 can include a RAM or flash memory for high-speed access by the processor 902 and/or a mass storage memory, *e.g.*, a micro drive capable of storing gigabytes of data that comprises text, images, audio, and video content. According to one aspect, the

memory 904 has sufficient storage capacity to store multiple sets of information, and the processor 902 could include a program for alternating or cycling between various sets of display information.

[0065] A display 906 is coupled to the processor 902 *via* a display driver system 908. The display 906 can be a color liquid crystal display (LCD), plasma display, or the like. In this example, the display 906 is a ¼ VGA display with sixteen levels of gray scale. The display 906 functions to present data, graphics, or other information content. For example, the display 906 can display a set of customer information, which is displayed to the operator and can be transmitted over a system backbone (not shown). Additionally, the display 906 can display a variety of functions that control the execution of the device 900. The display 906 is capable of displaying both alphanumeric and graphical characters.

[0066] Power is provided to the processor 902 and other components forming the hand-held device 900 by an onboard power system 910 (*e.g.*, a battery pack). In the event that the power system 910 fails or becomes disconnected from the device 900, a supplemental power source 912 can be employed to provide power to the processor 902 and to charge the onboard power system 910. The processor 902 of the device 900 induces a sleep mode to reduce the current draw upon detection of an anticipated power failure.

[0067] The terminal 900 includes a communication subsystem 914 that includes a data communication port 916, which is employed to interface the processor 802 with a remote computer. The port 916 can include at least one of Universal Serial Bus (USB) and IEEE 1394 serial communications capabilities. Other technologies can also be included, for example, infrared communication utilizing an infrared data port.

[0068] The device 900 can also include a radio frequency (RF) transceiver section 918 in operative communication with the processor 902. The RF section 918 includes an RF receiver 920, which receives RF signals from a remote device *via* an antenna 922 and demodulates the signal to obtain digital information modulated therein. The RF section 918 also includes an RF transmitter 924 for transmitting information to a remote device, for example, in response to manual user input *via* a user input device 926 (*e.g.*, a keypad) or automatically in response to the completion of a transaction or other predetermined and programmed criteria. The transceiver section 918 facilitates communication with a transponder system, for example, either

passive or active, that is in use with product or item RF tags. The processor 902 signals (or pulses) the remote transponder system *via* the transceiver 918, and detects the return signal in order to read the contents of the tag memory. In one implementation, the RF section 818 further facilitates telephone communications using the device 900. In furtherance thereof, an audio I/O section 928 is provided as controlled by the processor 902 to process voice input from a microphone (or similar audio input device) and audio output signals (from a speaker or similar audio output device). In another implementation, the device 900 can provide voice recognition capabilities such that when the device 900 is used simply as a voice recorder, the processor 902 can facilitate high-speed conversion of the voice signals into text content for local editing and review, and/or later download to a remote system, such as a computer word processor. Similarly, the converted voice signals can be used to control the device 900 instead of using manual entry *via* the keypad 926.

[0069] Onboard peripheral devices, such as a printer 930, signature pad 932, and a magnetic strip reader 934 can also be provided within the housing of the device 900 or accommodated externally through one or more of the external port interfaces 916.

[0070] The device 900 can also include an image capture system 936 such that the user can record images and/or short movies for storage by the device 900 and presentation by the display 906. Additionally, a dataform reading system 938 is included for scanning dataforms. It is to be appreciated that these imaging systems (936 and 938) can be a single system capable of performing both functions.

[0071] FIG. 10 is provided to assist in understanding and to provide context to an embodiment of the invention. Specifically, FIG. 10 illustrates an example of a handheld terminal 1000 operative to execute the systems and/or methods disclosed herein.

[0072] The handheld terminal 1000 includes a housing 1002 which can be constructed from a high strength plastic, metal, or any other suitable material. The handheld terminal 1000 includes a display 1004. As is conventional, the display 1004 functions to display data or other information relating to ordinary operation of the handheld terminal 1000 and/or mobile companion (not shown). For example, software operating on the handheld terminal 1000 and/or mobile companion can provide for the display of various information requested by the user. Additionally, the display 1004 can display a variety of functions that are executable by the handheld