PTO-1390 (06-13)
Approved for use through 6/30/2013. OMB 0651-0021
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.

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	U.S. Application No. (if known, see 37 CFR 1.5)
15-686-WO-US	

International Application No.	International Filing Date	Priority Date Claimed
PCT/EP2013/074440	November 22, 2013	November 22, 2012

Title of Invention
System to Detect Behaviour in a Telecommunications Network

First Named Inventor
Frank MULLER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☑ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.
2. ☑ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. ☑ is attached.
   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☑ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. ☑ A preliminary amendment.
11. ☑ An Application Data Sheet under 37 CFR 1.76.
12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. ☐ A power of attorney and/or change of address letter.
14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
15. ☐ Assignment papers *(cover sheet and document(s))*. Name of Assignee: _____
16. ☐ 37 CFR 3.73(c) Statement *(when there is an Assignee)*.

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. 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 15 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. APPLN. No. (if known – see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
	PCT/EP2013/074440	15-686-WO-US

17. ☑ Other items or information:

Copy of published PCT application WO2014/079960;
PCT International Search Report (PCT/ISA/210);
Notification of Transmittal of Priority Document (PCT/IB/304);
Notice Informing Applicant of Communication of International Application (PCT/IB/308); and
Notification of the Recording of a Change (PCT/IB/306).

The following fees have been submitted.	CALCULATIONS	PTO USE ONLY
18. ☑ Basic national fee (37 CFR 1.492(a)) **$280**	$ 280.00	
19. ☑ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** All other situations **$720**	$ 720.00	
20. ☑ Search fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority .....**$120** International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB .....**$480** All other situations **$600**	$ 480.00	
TOTAL OF 18, 19, and 20 =	$ 1,480.00	
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof **$400**		

Total Sheets	Extra Sheets	Number of each addition 50 or fraction thereof (round **up** to a whole number)	RATE	
- 100 =	/ 50 =		x **$400**	$

Surcharge of **$140.00** for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	- 20 =		x **$80**	$	
Independent claims	- 3 =		x **$420**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			**+ $780**	$	
Processing fee of **$140.00** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)). **+**				$	
TOTAL OF ABOVE CALCULATIONS =				$ 1,480.00	
☐ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.					
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.					
TOTAL NATIONAL FEE =				$ 1,480.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property. **+**				$	
TOTAL FEES ENCLOSED =				$ 1,480.00	
				Amount to be refunded:	$
				Amount to be charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☑ Please charge my Deposit Account No. 13-2490 in the amount of $ 1,480.00 to cover the above fees.

c. ☑ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 13-2490 as follows:

i. ☑ any required fee.

ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File)Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE 1: By providing this statement under 37 CFR 1.55 or 1.78, **this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA**.

NOTE 2: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☑ The address associated with Customer Number: 20306 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone			
Email					

Signature	/David A. Grabelsky/	Date	May 21, 2015
Name (Print/Type)	David A. Grabelsky	Registration No. (Attorney/Agent)	59,208

Privacy Act Statement

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

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

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

PTO/AIA/14 (07-14)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Frank		Muller	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Delft	Country of Residence i	NL

Mailing Address of Inventor:

Address 1	Hopstraat 59		
Address 2			
City	Delft	**State/Province**	
Postal Code	2611 TB	**Country** i	NL

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	20306		
Email Address	docketing@mbhb.com	Add Email	Remove Email

Application Information:

Title of the Invention	System to Detect Behaviour in a Telecommunications Network		
Attorney Docket Number	15-686-WO-US	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	3	**Suggested Figure for Publication (if any)**	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	20306		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2013/074440	2013-11-22

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country	Filing Date (YYYY-MM-DD)	Access Code (if applicable)
12193884.9	EP	2012-11-22	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (07-14)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

○ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
◉ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Koninklijke KPN N.V.

Mailing Address Information For Applicant:

Address 1	Maanplein 55		
Address 2			
City	The Hague	**State/Province**	
Country [i]	NL	Postal Code	2516 CK
Phone Number		Fax Number	

PTO/AIA/14 (07-14)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Applicant 2 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

○ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
◉ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :	

If the Applicant is an Organization check here. ☒

Organization Name	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO

Mailing Address Information For Applicant:

Address 1	Anna van Buerenplein 1		
Address 2			
City	's-Gravenhage	**State/Province**	
Country [i]	NL	Postal Code	2595 DA
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Koninklijke KPN N.V.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	Maanplein 55		
Address 2			
City	The Hague	**State/Province**	
Country i	NL	Postal Code	2516 CK
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Assignee 2

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	Anna van Buerenplein 1		
Address 2			
City	's-Gravenhage	**State/Province**	
Country i	NL	Postal Code	2595 DA
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (07-14)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	15-686-WO-US
	Application Number	
Title of Invention	System to Detect Behaviour in a Telecommunications Network	

Signature:

Remove

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

Signature	/David A. Grabelsky/			Date (YYYY-MM-DD)	2015-05-21
First Name	David A.	Last Name	Grabelsky	Registration Number	59208

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

  filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Frank Muller Date (Optional) :_____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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.

Privacy Act Statement

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	TBA
Examiner Name	TBA
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060288407	A1	2006-12-21	NASLUND et al.	
	2	20110185419	A1	2011-07-28	BOTELER et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2 139 279	EP	A1	2009-12-30	TELEFONAKTIEBOLAGET LM ERICSSON		☐
	2	98/33340	WO	A2	1998-07-30	AT&T WIRELESS SERVICES, INC.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	TBA
	Examiner Name	TBA
	Attorney Docket Number	15-686-WO-US

	3	98/33340	WO	A3	1998-07-30	AT&T WIRELESS SERVICES, INC.		☐
	4	2006/104752	WO	A1	2006-10-05	LUCENT TECHNOLOGIES INC.		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	European Search Report, European Patent Application No. 12193884.9, dated March 1, 2013.	☐
	2	MULLINER, Collin et al., "Taming Mr. Hayes: Mitigating Signaling Based Attacks on Smartphones", IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), 2012, pp. 1-12.	☐
	3	PCT International Search Report, PCT International Application No. PCT/EP2013/074440, dated February 7, 2014.	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	TBA
	Examiner Name	TBA
	Attorney Docket Number	15-686-WO-US

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2015-05-21
Name/Print	David A. Grabelsky	Registration Number	59,208

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

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

(11) EP 2 139 279 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.12.2009 Bulletin 2009/53

(51) Int Cl.:
H04W 24/10 (2009.01)

(21) Application number: **09161710.0**

(22) Date of filing: **02.06.2009**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR

(30) Priority: **27.06.2008 US 147960**

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)**
164 83 Stockholm (SE)

(72) Inventors:
- **Kenehan, Noel**
  113 49, STOCKHOLM (SE)
- **Westerberg, Erik**
  122 38, ENSKEDE (SE)
- **Berquist, Gunnar**
  164 45, KISTA (SE)
- **Olsson, Andreas**
  112 45, STOCKHOLM (SE)

(74) Representative: **Hasselgren, Erik Joakim**
Ericsson AB
Patent Unit LTE
Torshamnsgatan 23
164 80 Stockholm (SE)

(54) Systems and methods for monitoring performance of a communication system

(57) Monitoring the performance of communication systems is an important part of network operations. In one aspect the invention provides a method for monitoring the performance by collecting data pertaining to a mobile terminal accessing the system. In some embodiments, the method includes receiving an identifier for identifying the mobile terminal; using the identifier to detect the UE accessing the network via an access point; and in response to detecting the UE accessing the network, transmitting to the access point a message comprising an encrypted version of the identifier with a command to initiate the collection of data pertaining to the mobile terminal.

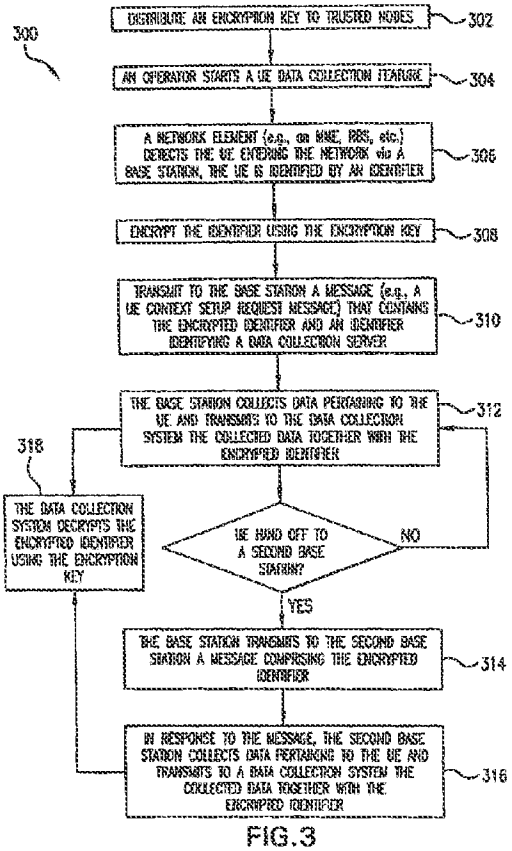


FIG.3

EP 2 139 279 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to performance monitoring of a communications network.

BACKGROUND

[0002] Monitoring the performance of communication systems (e.g., monitoring the performance of user equipment (UE), network elements, etc.) has always been a very important part of network operations. For example, performance monitoring may enable a network operator to identify bottlenecks and take appropriate actions to improve quality.

[0003] In performance monitoring, there is an inherent trade off between the granularity (or resolution) of the performance information and the amount of performance information that needs to be sent from a node (e.g. a base station).

[0004] Typically, there are two types of performance information: (1) aggregate information and (2) trace information. Aggregate information has the lowest resolution in that it is the aggregate of a large amount of data into a single number (e.g., the total number of dropped calls in a cell). Trace information has the highest resolution in that a large amount of information about a single UE is recorded and sent to a performance monitoring system. In contrast to aggregate information, trace information can include information such as, for example, when and why a particular UE dropped its calls.

[0005] To create useful aggregate information it is important how large amount of data is aggregated into a single number. For instance, number of dropped calls is an interesting measurement, but an even more interesting measurement is the number of UEs (i.e. subscribers) that had a dropped call.

[0006] The above described measurements are possible in systems like UMTS and GSM because the producer of the aggregate information has access to a unique UE identity, but not in other systems, such as a system like long term evolution (LTE), which is in an early stage of development, that do not have access to a unique UE identity, but only to identities that can change over time. Thus, there exists a need to overcome this problem of providing the aggregate information producer with a unique UE identity.

[0007] An operator may initiate a trace (i.e., initiate the collection of trace information) for a UE by using a network management system (NMS) to select the UE (e.g., the operator may select an IMSI or IMEI associated with a UE) and other trace configuration parameters. In response, the NMS transmits to a domain manager (DM) (e.g., an operational support system (OSS)) a trace start request message that includes a globally unique trace reference (the trace reference may be made globally unique by making the PLMN ID part of the trace reference) and other trace configuration data. The trace reference is a temporary alias that is used to avoid the security risk of using the IMSI or IMEI to identify a UE.

[0008] The DM receives the trace start request from NMS and orders a network element (NE) (e.g., a mobility management entity (MME), home subscriber server (HSS), serving GPRS support node (SGSN), etc.) to enable the trace by transmitting to the NE trace configuration data that includes the trace reference. When the UE to be traced enters the network, an initial UE message is sent from the UE to the NE via a radio base station (RBS).

[0009] The NE, at reception of the initial UE message, determines whether the UE should be traced. If it determines that the UE should be traced, then the NE creates a trace recording session identifier (TRSID). This TRSID in conjunction with the trace reference is referred to as a UE trace ID (UETID). The NE then adds the UETID and other trace configuration data to an initial context setup message pertaining to the UE, which is then sent to the RBS. Upon receipt of the setup message, the RBS will start tracing (i.e., will start recording information pertaining to the UE to which the setup message pertains). The recorded trace information is stored in a file that is transmitted from the RBS to a trace collection entity (TCE). The trace file will include or otherwise be associated with the UETID. Tracing is deactivated for the UE by sending a deactivate message to the RBS.

[0010] The above described process works well in a fully integrated, completely standard, compliant system, but does not work well in other systems, such as a system like long term evolution (LTE), which is in an early stage of development.

[0011] In such systems, at least with respect to the early phases of system deployment, there may be a situation where several different NEs can create trace references without cooperation with each other. For example, an operator could start a UE Trace directly on an MME for UE-1 with trace ref x and directly from another MME for UE-2 also with trace ref x. This is problematic if both UEs are in the same RBS because it means that there is no guarantee that a trace reference will be globally unique. This could cause a receiver of the different trace data to process the trace data as though it pertained to only a single UE, when in fact it pertains to multiple UEs.

[0012] In such systems, it is also possible that a UE trace is started in one DM and the trace files are collected by another DM. This creates a situation where the collecting entity has no knowledge of the mapping between the trace reference and the IMSI/IMEI of the UE. This makes it difficult for an operator to analyze the collected data.

[0013] There exists a need to overcome at least one or more of the above described problems.

ERICSSON EXHIBIT 1005, Page 20

SUMMARY

[0014] In one aspect, the patent provides a method for collecting data pertaining to a user equipment (UE) (e.g., trace data, aggregate data, and or other data). In some embodiments, the method includes: receiving an encryption key for use in encrypting an identifier for identifying the UE; encrypting the identifier using the encryption key; detecting the UE accessing a network via an access point (a trusted access point or an un-trusted access point); and in response to detecting the UE accessing the network, transmitting to the access point a message (e.g., a context setup request or a trace activation request) comprising the encrypted identifier.

[0015] The access point may be a base station and the step of detecting the UE may include receiving a message from the base station. The message received from the base station may be an initial S1 interface message transmitted by the base station in response to receiving a communication from the UE. The step of receiving the encryption key may include receiving the encryption key from a domain manager (DM) (e.g., an OSS or CN-OSS). In some embodiments, the step of receiving the key from the DM may include pulling the key from the DM or having the DM push the key.

[0016] In some embodiments, the message may further include an identifier identifying a data collection node, and the method further includes the step of transmitting the key to the data collection node, wherein the key is transmitted to the data collection node from the DM. The access point is configured to collect data pertaining to the UE in response to receiving the message and is further configured to transmit to the data collection node the collected data together with the encrypted identifier. The data collection node may use the encryption key to decrypt the encrypted identifier.

[0017] In some embodiments, the method further includes receiving an instruction to collect data pertaining to the UE, wherein the encrypted identifier is transmitted to the access point only if the instruction has been received.

[0018] In some embodiments, the method is performed by a network element, and the network element is an MME or SGSN.

[0019] In some embodiments, the method further includes: transmitting, from the access point, a message to a second access point, wherein the message includes the encrypted identifier and the step of transmitting the message is performed as part of a hand off of the UE from the first access point to the second access point.

[0020] In another embodiment, the method includes: receiving an identifier for identifying the UE and an encrypted version of the identifier; using the identifier to detect the UE accessing a network via an access point; and in response to detecting the UE accessing the network, transmitting to the access point a message comprising the encrypted version of the identifier.

[0021] In another aspect, the present invention pertains to a network element. In some embodiments, the network element includes: a receiver for receiving an encryption key; a data storage unit storing computer instructions; and a processor coupled to the data storage unit for executing the computer instructions, wherein the computer instructions comprise: computer instructions that are configured to use the received encryption key to encrypt an identifier that identifies a user equipment (UE); computer instructions that are configured to detect the UE accessing a network via an access point; and computer instruction configured to transmit to the access point a message comprising the encrypted identifier.

[0022] In another aspect, the present invention pertains to a communication system. In some embodiments, the communication system includes: a network element storing an encryption key; a data collection node storing the encryption key; and a base station for providing network access to a user equipment (UE), wherein (1) an identifier identifies the UE, (2) the network element is configured to: (a) use the encryption key to encrypt the identifier and (b) transmit to the base station a message containing the encrypted identifier and an identifier identifying the data collection node, (3) the base station is configured to: (a) collect data pertaining to the UE and (b) transmit to the data collection node the collected data together with the encrypted identifier, and (4) the data collection node is configured to decrypt the encrypted identifier using the encryption key.

[0023] In some embodiments, the network element is further configured to detect when the UE accesses the network via the base station and is configured to transmit the encrypted identifier to the base station in response to detecting the UE accessing the network.

[0024] In some embodiments, the communication system further includes a domain manager (e.g., a CN-OSS). The domain manager may be configured to transmit the encryption key to the network element. The system may further include a network management system. The NMS may be configured to transmit the encryption key to the network element through the DM.

[0025] In some embodiments, the base station is configured to transmit to a second base station a message comprising the encrypted identifier as part of a process of handing off the UE to the second base station.

[0026] The above and other aspects and embodiments are described below with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] The accompanying drawings, which are incorporated herein and form part of the specification, illustrate various embodiments of the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the pertinent art to make and use the invention. In the drawings, like reference numbers indicate identical or functionally similar elements.

ERICSSON EXHIBIT 1005, Page 21

[0028] FIG. 1. illustrates a communication system according to embodiments of the invention.

[0029] FIG. 2 illustrates the delivery of encryption keys to trusted nodes.

[0030] FIG. 3 is a flow chart illustrating a process according to some embodiments of the invention.

[0031] FIG. 4 is a flow chart illustrating a process according to some embodiments of the invention.

[0032] FIG. 5 is a functional block diagram of a network element according to some embodiments.

DETAILED DESCRIPTION

[0033] Referring to FIG. 1, FIG. 1 illustrates a communication system 100 according to some embodiments of the invention. As illustrated in FIG. 1, communication system 100 includes a network management server 102, a domain manager (DM) 104 (e.g., an operational support system (OSS) such as a core network OSS (CN-OSS)), a trusted network element (106) (e.g., a mobility management entity (MME), home subscriber server (HSS), etc.), a data collection system (DCS) 108, radio base stations 110a and 110b, and a mobile terminal 112, which may be referred to as user equipment (UE) 112.

[0034] When a network operator wants to collect information (e.g., trace information) about UE 112, the network operator may initiate the trace using any one of, for example, NMS 102, DM 104 or NE 106. The network operator may initiate the trace by inputting or selecting from a list an identifier identifying UE 112 and issuing an activate trace command. The identifier identifying UE 112 that is input or selected by the network operator may be an international mobile equipment identity (IMEI), an international mobile subscriber identity (IMSI), IMEI and software version number (IMEIsv), or other similar identifier.

[0035] In some embodiments, when an operator initiates a trace using NMS 102, NMS 102 may transmit to NE 106 via DM 104 a trace activate command together with an encryption key and the UE identifier (e.g., the IMEI, IMSI, IMEIsv). The command and encryption key may be transmitted to NE 106 using a Northbound Interface (itf-N).

[0036] The NE 106, in response to receiving the command monitors the network so as to detect when UE 112 enters system 100. NE 106 may detect this event by receiving a message from the base station 110 that UE 112 is currently using to access system 100 (we will assume that this base station is base station 110a). This message may be an initial S1 interface message.

[0037] In response to detecting UE 112 accessing system 100, NE 106 may transmit to base station 110a a message that includes an encrypted UE identifier. For example, when NE 106 receives the trace command from NMS 102, NE 106 may use the encryption key to encrypt the UE identifier included in the message, and when NE 106 detects UE 112 entering the network, NE 106 transmits the encrypted UE identifier to base station 110a. In some embodiments, NE 106 transmits the encrypted UE identifier to base station 110a by including the encrypted identifier in a UE context setup request message or a trace activation message that is transmitted to the base station. In addition to including the encrypted identifier, the message sent to base station 110a may also include an identifier identifying a DCS (e.g., DCS 108).

[0038] In response to receiving the message from NE 106, base station 110a starts collecting data pertaining to UE 112. This data may be stored in a file. At some point (e.g., after a certain amount of time has expired or after a certain amount of data has been collected), base station 110a transmits the collected data along with the encrypted identifier to the identified DCS without the DCS requesting the data. Additionally, if base station 110a hands off UE 112 to base station 110b, base station 110a may transmit to base station 110b the encrypted UE identifier and a command instructing base station 110b to collect information pertaining to UE 112. The command would preferably include the identifier identifying the DCS so that base station 110b can push to the DCS the collected data together with the encrypted identifier. Alternatively, instead of the base stations 110 pushing to the DCS the collected data and encrypted identifier, the base stations may send a message to the DCS informing the DCS that the base station has data for the DCS to collect. In response to this message, the DCS may then retrieve the collected data and encrypted identifier from the base station. For example, in some embodiments, in response to the message from the base station 110, the DCS may pull the data from the base station (e.g., the DCS may send a request for the data to the base station, which will then transmit the data to the DCS).

[0039] The DCS that receives the collected data, uses an encryption key (e.g., the encryption key used to encrypt the identifier or another key) to decrypt the encrypted UE identifier that accompanies the data to recover the UE identifier. As illustrated in FIG. 2, a key distributor 202 distributes an encryption key to trusted nodes (e.g., DCS 108, NE 106 and DM 104), but not to the un-trusted node NE 204, which may be an access point (e.g., an RBS). As further illustrated in FIG. 2 and as was described above, NE 106 may send to NE 204 a UE identifier that has been encrypted using the encryption key. In some embodiments, key distributor 202, which may be part of NMS 102, periodically (e.g., daily) distributes a new encryption key to the trusted nodes.

[0040] Because the UE identifier is globally unique, the DCS will not suffer from the problem of receiving different trace data for different UEs were the different trace data is associated with the same trace reference. Further, DCS will not face a situation where it has no knowledge of the mapping between the trace reference and the identifier (e.g., IMSI/IMEI) of the UE because, in the embodiments described above, the encrypted UE identifier is the trace reference and the DCS will have the encryption key needed to decrypt the encrypted UE identifier. Moreover, because the base station receives the encrypted

ERICSSON EXHIBIT 1005, Page 22

UE identifier and not the actual UE identifier, un-trusted base stations (e.g., NE 204) can be used to collect data pertaining to a UE without violating any privacy concerns.

[0041] Referring now to FIG. 3, FIG. 3 is a flow chart illustrating a process 300 according to some embodiments of the invention. Process 300 may begin in step 302, wherein an encryption key is distributed to a set of trusted nodes (e.g., NE 106 and DCS 108). As described above, this step may be performed periodically by key distributor 202. In some embodiments, instead of the key distributor distributing the keys to the trusted nodes, the trusted nodes may receive the key by pulling the key from the key distributor (e.g., a trusted node may send a key request message to the key distributor, which, in response, may transmit a key to the trusted node).

[0042] In step 304, an operator activates a data collection feature for UE 112. For example, the operator may perform this step at NE 106 or DM 104. If performed at DM 104, the DM 104 transmits an identifier for UE 112 (e.g., an IMSI) to NE 106. If performed at NE 106, the operator my input or select the UE 112 identifier.

[0043] In step 306, NE 106 detects UE 112 entering the network via base station 110a (e.g., NE 106 may receive from base station 110a an initial UE message). In step 308, NE 106 encrypts the UE 112 identifier. In step 310, NE 106 transmits to base station 110a a message (e.g., an initial context setup request for UE 112) that contains the identifier encrypted in step 308, a command to initiate data collection for UE 112, and an identifier identifying DCS 108 (e.g., an IP address of DCS 108).

[0044] Next (step 312), base station 110a collects data pertaining to UE 112 and transmits to DCS 108 a file containing the collected data and the encrypted identifier. The encrypted identifier may be included in the file. If base station 110a hands off UE 112 to base station 110b, then process 300 may proceed to step 314, otherwise it may proceed back to step 312.

[0045] In step 314, base station 110a transmits to base station 110b a message comprising the encrypted identifier that was transmitted to base station 110a in step 310. In response to the message, base station 110b collects data pertaining to UE 112 and transmits to DCS 108 a file containing the collected data and the encrypted identifier (step 316). Next (step 318), DCS 108 uses an encryption key to decrypt the encrypted identifier so as to identify the unique UE to which the collected data pertains.

[0046] Referring now to FIG. 4, FIG. 4 is a flow chart illustrating a process 400 according to some embodiments of the invention. Process 400 may begin in step 402, where, in response to an operator using NMS 102 to initiate a data collection feature (e.g., a trace) for UE 112, NMS 102 transmits to NE 106 via DM 104 a UE 112 identifier and an encryption key or an encrypted UE 112 identifier. The data may be transmitted to NE 106 using an itf-N interface. In step 404, if an encryption key was sent in step 402 rather than the encrypted UE 112 identifier, NE 106 encrypts the identifier using the encryption key. After step 404, steps 310-318 are performed. These steps are described above with reference to FIG. 3.

[0047] Referring now to FIG. 5, FIG. 5 is a functional block diagram illustrating some components of NE 106 according to some embodiments. As illustrated in FIG. 5, NE 106 includes: circuitry 502 for enabling NE 106 to communicate with DM 104 and key generator 202; circuitry 508 for enabling NE 106 to communicate with NE 110a/204; a data storage 504 (e.g., non-volatile memory, disk drive, etc) storing software 506; and a processor 512 for executing software 506. Software 506 is configured such that, when it is executed by processor 512, it causes NE 106 to perform the functions described above.

[0048] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments.

Additionally, while the processes described above and illustrated in the drawings are shown as a sequence of steps, this was done solely for the sake of illustration. Accordingly, it is contemplated that some steps may be added, some steps may be omitted, and the order of the steps may be re-arranged.

Claims

1. A method for collecting data pertaining to a user equipment (UE), the method comprising:

   receiving an encryption key for use in encrypting an identifier for identifying the UE;
   encrypting the identifier using the encryption key;
   detecting the UE accessing a network via an access point; and
   in response to detecting the UE accessing the network, transmitting to the access point a message comprising the encrypted identifier.

2. The method of claim 1, wherein the access point is a base station and the step of detecting the UE comprises receiving a message from the base station.

3. The method of claim 2, wherein the message received from the base station is an initial S1 interface message transmitted by the base station in response to receiving a communication from the UE.

4. The method of claim 1, 2 or 3 wherein the step of receiving the encryption key comprises receiving the encryption key from a domain manager (DM).

5. The method of claim 4, wherein the message further includes an identifier identifying a data collection

ERICSSON EXHIBIT 1005, Page 23

node, and the method further comprises the step of transmitting the key to the data collection node, wherein the key is transmitted to the data collection node from the DM.

6. The method of claim 5, wherein the access point is configured to collect data pertaining to the UE in response to receiving the message and is further configured to transmit to the data collection node the collected data together with the encrypted identifier, wherein the data collection node uses the encryption key to decrypt the encrypted identifier.

7. The method of any of the preceding claims wherein the method is performed by a network element, and the network element is an MME or SGSN.

8. The method of claim 1, wherein the message is a UE context setup request or a trace activation request.

9. A network element, comprising:

a receiver for receiving an encryption key;
a data storage unit storing computer instructions; and
a processor coupled to the data storage unit for executing the computer instructions, wherein the computer instructions comprise:

computer instructions that are configured to use the received encryption key to encrypt an identifier that identifies a user equipment (UE);
computer instructions that are configured to detect the UE accessing a network via an access point; and
computer instruction configured to transmit to the access point a message comprising the encrypted identifier.

10. The network element of claim 9, wherein the access point is a base station, the network element further includes an interface for communicating with the base station, and the computer instructions configured to detect the UE comprise computer instructions for processing a message that was transmitted from the base station and received by the network element via the interface.

11. The network element of claim 10, wherein the message received from the base station is an initial S1 interface message transmitted by the base station in response to receiving a communication from the UE.

12. The network element of claim 9, 10 or 11, wherein the encryption key is received by the network element from a domain manager (DM).

13. The network element of claim 9, wherein the message further includes an identifier identifying a data collection node.

14. The network element of claim 9, wherein the message is a UE context setup request or a trace activation request.

15. The network element of claim 9, wherein the computer instruction configured to transmit to the access point the message comprising the encrypted identifier are configured to transmit the message in response to detecting the UE accessing the network, and the computer instructions that are configured to use the received encryption key to encrypt the identifier are configured to encrypt the identifier using the key in response to detecting the UE accessing the network.

16. A communication system, comprising:

a network element storing an encryption key;
a data collection node storing the encryption key; and
a base station for providing network access to a user equipment (UE), wherein
an identifier identifies the UE,
the network element is configured to: (a) use the encryption key to encrypt the identifier and (b) transmit to the base station a message containing the encrypted identifier,
the base station is configured to: (a) collect data pertaining to the UE and (b) transmit to the data collection node the collected data together with the encrypted identifier, and
the data collection node is configured to decrypt the encrypted identifier using the encryption key.

17. The communication system of claim 16, wherein the network element is further configured to detect when the UE accesses the network via the base station and is configured to transmit the encrypted identifier to the base station in response to detecting the UE accessing the network.

18. The communication system of claim 16, wherein the message further includes an identifier identifying the data collection node.

19. The communication system of claim 16, wherein the message is a UE context setup request or a trace activation request.

20. The communication system of claim 16, wherein the network element is an MME or SGSN.

ERICSSON EXHIBIT 1005, Page 24

21. The communication system of claim 16, further comprising a domain manager, wherein the domain manager (DM) is configured to transmit the encryption key to the network element.

22. A method performed by a network element (NE) for collecting data pertaining to a user equipment (UE), the method comprising:

receiving an identifier for identifying the UE and an encrypted version of the identifier;
using the identifier to detect the UE accessing a network via an access point; and
in response to detecting the UE accessing the network, transmitting to the access point a message comprising the encrypted version of the identifier.

23. The method of claim 22, wherein the access point is a base station and the step of detecting the UE comprises receiving a message from the base station.

24. The method of claim 23, wherein the message received from the base station is an initial S1 interface message transmitted by the base station in response to receiving a communication from the UE.

25. The method of claim 22, wherein the message further includes an identifier identifying a data collection node.

26. The method of claim 22, wherein the message is a context setup request or a trace activation request.

ERICSSON EXHIBIT 1005, Page 25

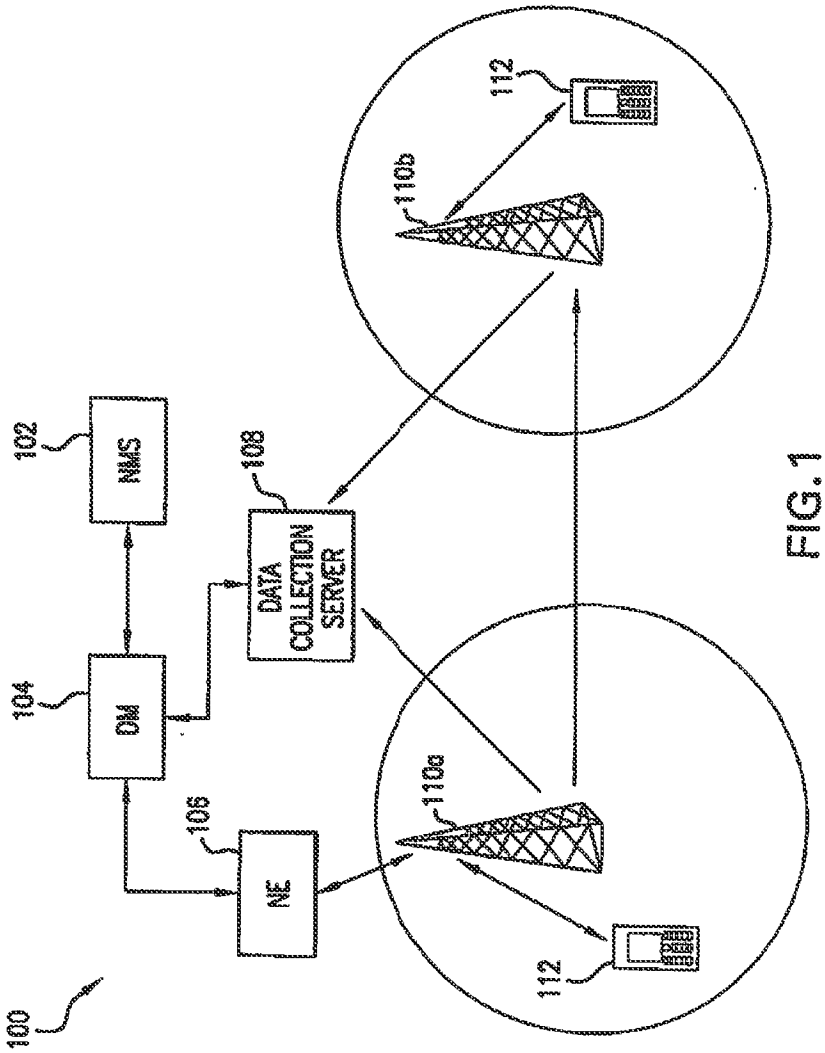


FIG. 1

ERICSSON EXHIBIT 1005, Page 26

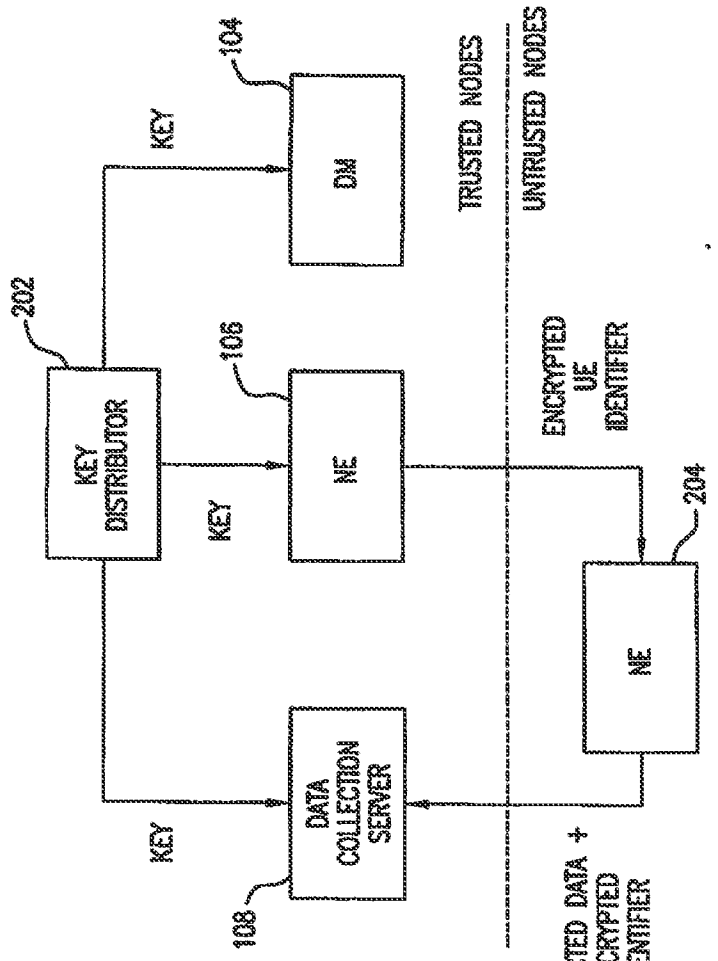


FIG. 2

ERICSSON EXHIBIT 1005, Page 27

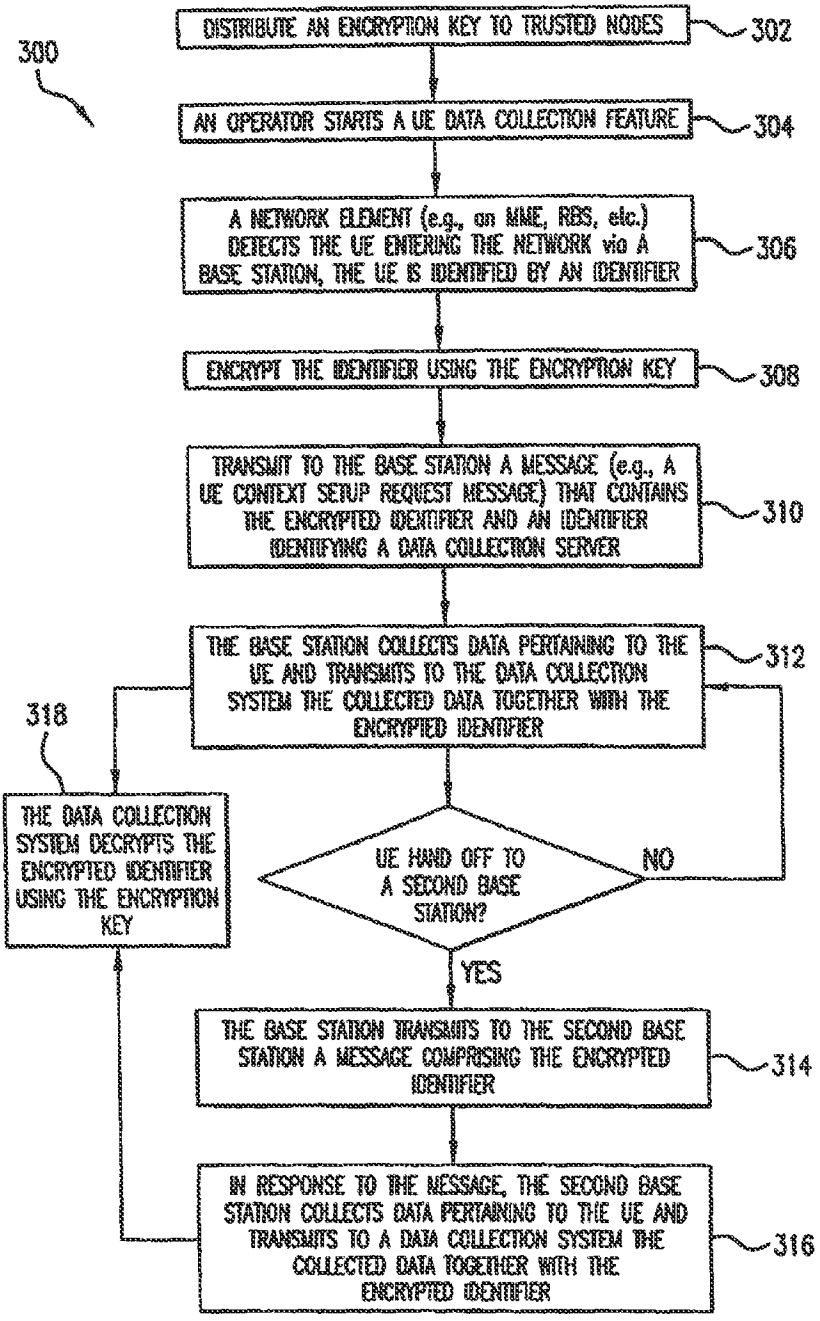


FIG.3

ERICSSON EXHIBIT 1005, Page 28

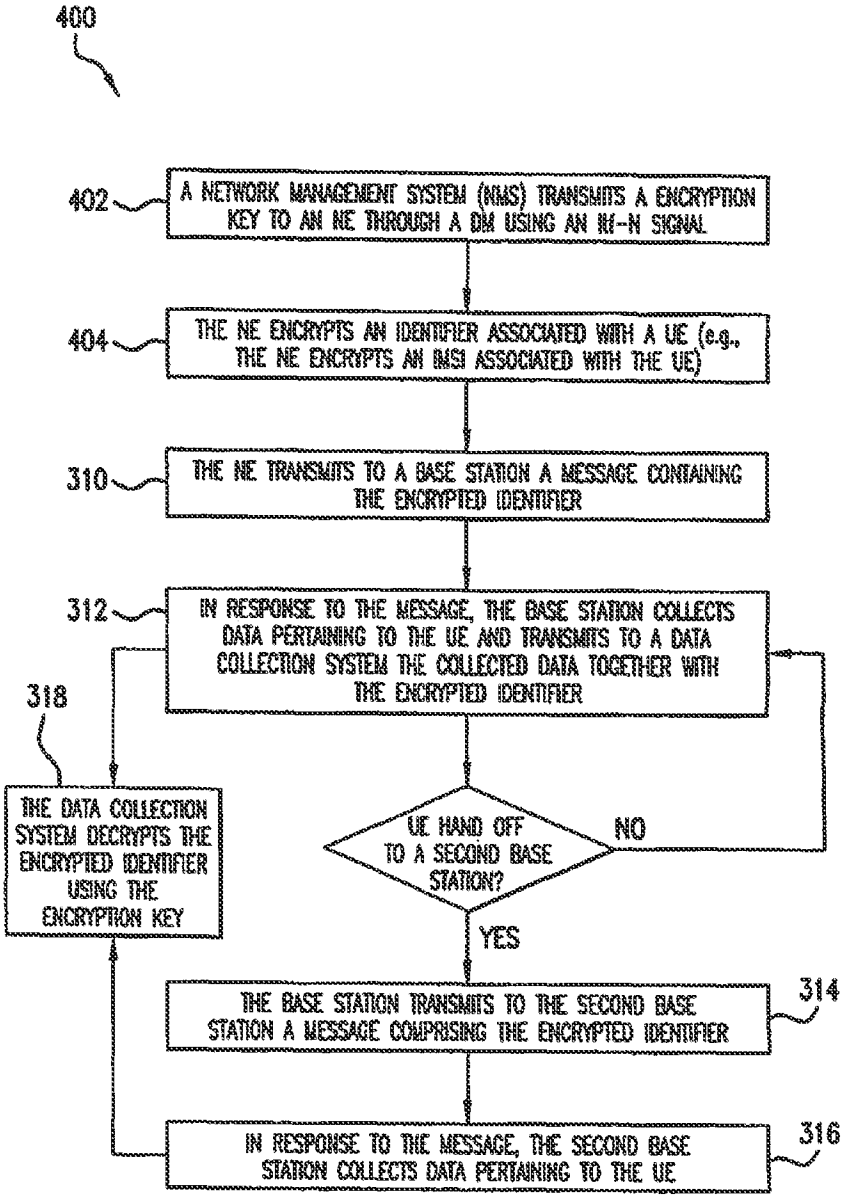


FIG.4

ERICSSON EXHIBIT 1005, Page 29

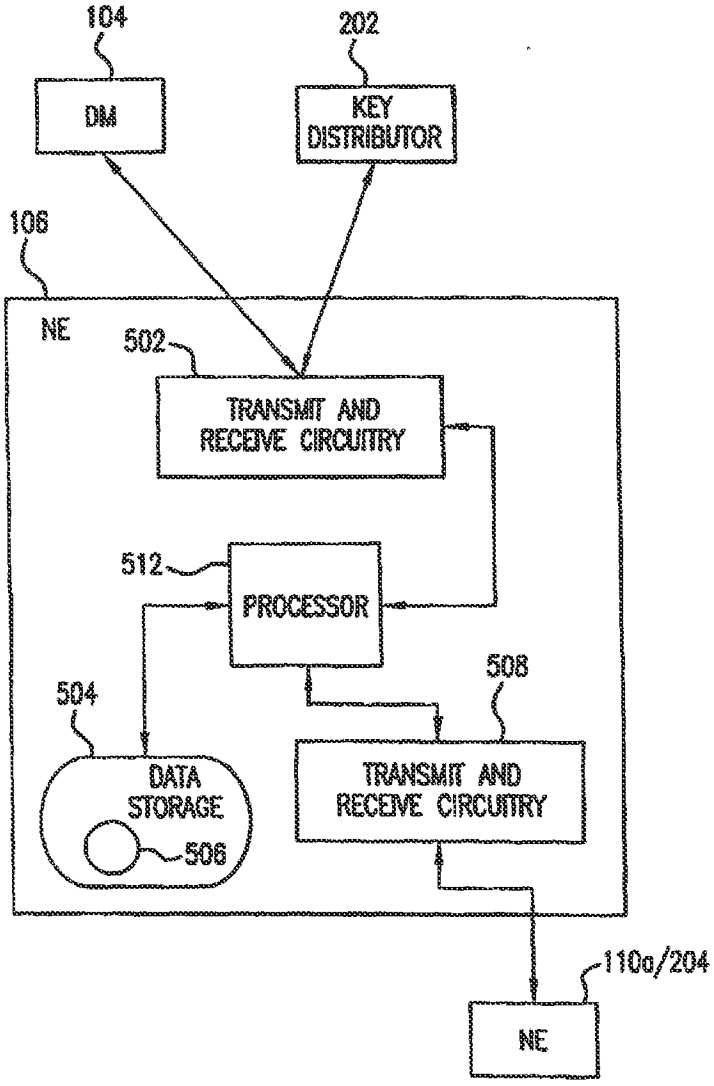


FIG.5

ERICSSON EXHIBIT 1005, Page 30

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 09 16 1710

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	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (3GPP TS 32.422 version 8.1.0 Release 8); ETSI TS 132 422" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, no. V8.1.0, 17 June 2007 (2007-06-17), XP002551240 ISSN: 0000-0001 Section 4.1.2.4 Section 5.6 -----	1-26	INV. H04W24/10
A	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements (3GPP TS 32.421 version 8.2.0 Release 8); ETSI TS 132 421" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, no. V8.2.0, 17 June 2008 (2008-06-17), XP002551239 ISSN: 0000-0001 Section 5.3 ----- -/--	1-26	TECHNICAL FIELDS SEARCHED (IPC) H04W

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	20 October 2009	Bertolissi, Edy

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)

ERICSSON EXHIBIT 1005, Page 31

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 09 16 1710

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	"Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunication management; Subscriber and equipment trace; Trace data definition and management (3GPP TS 32.423 version 7.4.0 Release 7); ETSI TS 132 423" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. 3-SA5, no. V7.4.0, 1 June 2007 (2007-06-01), XP014038358 ISSN: 0000-0001 Section 1 -----	1-26	
			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	20 October 2009	Bertolissi, Edy

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)

ERICSSON EXHIBIT 1005, Page 32

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/00 | A2

(11) International Publication Number: **WO 98/33340**

(43) International Publication Date: 30 July 1998 (30.07.98)

(21) International Application Number: PCT/US98/00441

(22) International Filing Date: 7 January 1998 (07.01.98)

(30) Priority Data:
08/788,151 24 January 1997 (24.01.97) US

(71) Applicant: AT & T WIRELESS SERVICES, INC. [US/US]; 500 Carillon Point, Kirkland, WA 98033 (US).

(72) Inventors: AMIN, Umesh, J.; 10522 180 Court, N.E., Redmond, WA 98052 (US). ROWE, Lorin, B.; 14843 N.E. 14th Place, Bellevue, WA 98007 (US). WAUGHMAN, Russell, John; 13117 N.E. 128th Place, Kirkland, WA 98034 (US).

(74) Agent: DWORETSKY, Samuel, H.; AT & T Corp., P.O. Box 4110, Middletown, NJ 07748 (US).

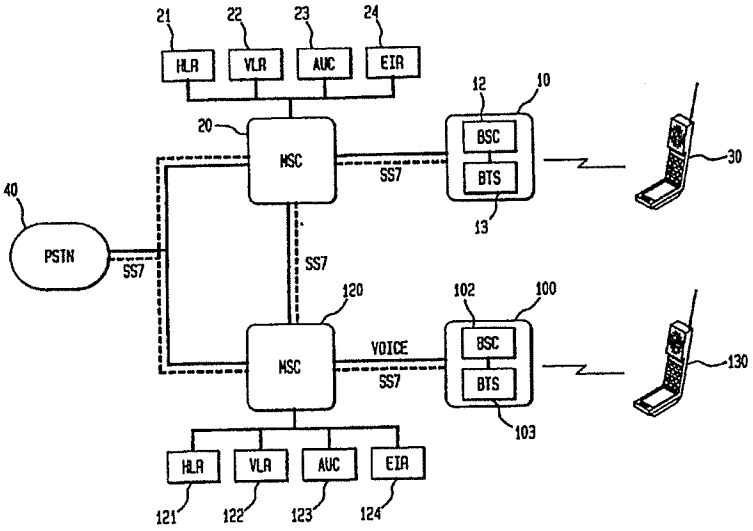
(81) Designated States: BR, CA, JP, MX, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: DETECTION OF FRAUDULENTLY REGISTERED MOBILE PHONES

(57) Abstract

A system and method are provided for detecting fraudulent use of a unique identifier associated with an authorized mobile station in a wireless telecommunications network. A monitoring system passively collects data associated with the registration of one or more mobile stations utilizing the unique identifer. A fraud detection processor analyzes the collected data using a first pattern recognition device. The pattern recognition device determines the periodicity of successive registration messages associated with the unique identifier of the authorized mobile station and a suspected fraudulent event is identified when the time between successive registration messages is non–periodic. A second pattern recognition device may be utilized alone or in combination with the first pattern recognition device to identify suspected fraudulent activity when an apparent velocity of the mobile station utilizing the unique identifier between successive registration messages exceeds a predetermined maximum velocity. The apparent velocity is based upon the approximated geographical distance and time between successive registration messages. Upon the detection of a suspected fraudulent event by the first and/or second pattern recognition devices, an authentication system may be utilized to identify a suspected mobile station as an unauthorized mobile station when a response to an authentication challenge received from the suspected mobile station is not substantially the same as a predicted response calculated by the authentication system based upon at least the unique identifier of the authorized mobile station.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TITLE OF THE INVENTION

DETECTION OF FRAUDULENTLY REGISTERED MOBILE PHONES

BACKGROUND OF THE INVENTION

1. Field Of The Invention

The present invention relates in general to wireless communications systems and, more particularly, to a system and method for detecting unauthorized use of a mobile station in a wireless telecommunications system.

2. Description Of The Related Art

With the increased popularity of wireless telecommunications systems (e.g., wireless cellular telecommunications systems), telecommunication service providers offer many different types of telecommunication services to their respective customers. Such services are generally provided to users on a subscription basis and, therefore, such users are generally referred to as "subscribers."

With the increase in overall usage of such wireless telecommunications systems, the incidence of fraudulent and unauthorized usage has also increased at an alarming rate. For example, it is estimated that fraudulent calls in the U.S. make up as much as 5 percent to 30 percent of all calls completed and account for hundreds of millions of dollars in lost revenue to telecommunication service providers. In addition to lost revenue, the effect of such wireless fraud also includes degraded service to the subscriber base, increased operational costs and reduced network capacity due to excess traffic associated with fraudulent calls.

There are several different methods by which unscrupulous persons attempt to obtain fraudulent access to and initiate unauthorized calls within a wireless telecommunications system. As a result of the mobile nature of mobile stations (e.g., cellular telephones), many of these methods of committing wireless fraud are extremely difficult to detect and prevent.

One such method of committing wireless fraud is known as "cloning fraud." Cloning fraud typically involves the misappropriation of a valid set of subscriber identification numbers (e.g., mobile identification number (MIN) and electronic serial number (ESN)) and programming the misappropriated MIN/ESN into at least one mobile station. When the "cloned" mobile station is fraudulently

used to initiate calls over the wireless telecommunications network, the network, believing the unauthorized user to be the valid subscriber whose MIN/ESN was misappropriated, is deceived into providing such wireless services to the unauthorized user.

To combat wireless fraud, telecommunications service providers have resorted to a number of fraud detection and prevention systems. For instance, one proposed solution to identify cloning fraud involves the collection of call detail records associated with calls completed in the wireless network to identify concurrent call originations or receptions for a single subscriber identification number (MIN). Another proposed solution also includes the collection of call detail records associated with calls actually completed in the wireless network to determine whether the time interval between successive calls for a particular subscriber identification number (MIN) is too short to justify the geographic separation of the subscriber's mobile station for the successive calls. In yet another proposed solution, a subscriber's past calling activity is collected to formulate a historical usage pattern and any calls initiated by the subscriber that deviate from the historical usage pattern are identified as potentially fraudulent. Still another proposed solution performs a velocity check to identify potential cloning fraud by comparing the number of calls initiated by a subscriber within a discrete period of time to a minimum threshold number indicative of fraud.

A shortcoming of these conventional fraud detection systems is that they cannot identify such wireless fraud (e.g., cloning fraud) until after the fraudulent activity has occurred. That is, these conventional fraud detection systems generally require that the unauthorized user have actually placed the fraudulent call before the wireless fraud can be detected.

SUMMARY OF THE INVENTION

The above-described problems and shortcomings of such prior art systems are solved and a technical advance is made over the prior art in accordance with the present invention by providing a system and method for detecting unauthorized use of a mobile station that functions in real time to automatically identify existing fraudulent activity and potentially fraudulent activity.

In accordance with the present invention, a system and method is provided for detecting fraudulent use of a unique identifier associated with an

authorized mobile station in a wireless telecommunications network. A monitoring system collects data associated with the registration of one or more mobile stations utilizing the unique identifier. A fraud detection processor analyzes the collected data using a first pattern recognition device. The pattern recognition device determines the periodicity of successive registration messages associated with the unique identifier of the authorized mobile station and a suspected fraudulent event is identified when the time between successive registration messages is non-periodic.

A second pattern recognition device may be utilized alone or in combination with the first pattern recognition device to identify suspected fraudulent activity when an apparent velocity of the mobile station utilizing the unique identifier between the successive registration messages exceeds a predetermined maximum velocity. The apparent velocity is based upon the approximated geographical distance and time between successive registration messages.

Upon the detection of a suspected fraudulent event by the first and/or second pattern recognition devices, an authentication system may be utilized to identify which of several mobile stations is an unauthorized mobile station. When a response to an authentication challenge received from the suspected mobile station is the same as a predicted response calculated by the authentication system based upon at least the unique identifier of the authorized mobile station, then this mobile station is the authorized mobile station. It follows that the other mobile station(s) must be unauthorized and action may be taken to prevent these unauthorized mobile stations from further calling activity.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing features and other aspects of the invention are explained in the following description taken in connection with the accompanying drawings wherein:

FIG. 1 is a block diagram illustrating the interconnections between a mobile station, a base station system, a mobile switching center and the public switched telephone network;

FIG. 2 is a block diagram illustrating the architectural details of the fraud detection system according to the present invention;

FIG. 3 is a block diagram further illustrating the fraud detection system illustrated in FIG. 2;

FIG. 4 is a flow diagram illustrating a pattern of IS41 Messages according to the present invention;

FIG. 5 is a flow diagram illustrating a representative pattern of messages applicable to the geographic dispersion fraud detection method according to the present invention;

FIG. 6 is a flow diagram illustrating a representative pattern of messages applicable to the periodicity fraud detection method according to the present invention; and

FIG. 7 is diagram illustrating a representative non-periodic pattern of registration (RegNot) messages indicative of cloning fraud in connection with the periodicity fraud detection method according to the present invention.

DETAILED DESCRIPTION

While it is understood that the present invention is not necessarily limited to cellular telecommunications networks, FIG. 1 illustrates a typical cellular telecommunications system in which the present invention may be utilized. In such a system, conventional cellular technology is applied to allow the same frequencies of a common allocated radio bandwidth to be reused in separated local areas or cells of a broader region.

Although it is understood that a typical cellular telecommunications system may have any number of cells, FIG. 1 illustrates two representative cells of the cellular telecommunications system. Generally, each cell of the cellular network is served by a base station system **10** or **100** comprising a group of local transceivers connected to a common antenna.

The base station systems **10**, **100**, each typically comprising a base station controller (BSC) **12**, **102** and at least one base station transceiver (BTS) **13**, **103**, are interconnected via a switching system, commonly referred to as a mobile switching center (MSC) **20**, **120**. The MSC **20**, **120** is used for switching calls involving at least one mobile station **30**, **130** and for much of the system processing. The MSC **20**, **120** is also connected to the public switched telephone network (PSTN) **40** for communicating with land-based stations (not shown).

Base station system **10** and mobile station **30** communicate via radio connections. Base station system **10** is also connected via trunks to carry the voice or data, and control messages between mobile station **30** and MSC **20**. It is

understood that base station system **100** illustrated in FIG. 1 operates in an identical fashion with respect to mobile station **130** and MSC **120**.

Wireless telecommunications networks such as that illustrated in FIG. 1 typically comprise many units that need to communicate signaling information for controlling establishment of connections. Such signalling information is typically communicated over links or channels separate from the channels carrying actual voice or data communications between the customers being connected. Among the units that need to communicate are the mobile stations **30**, **130**, the base station systems **10**, **100** connected by radio to the mobile station **30**, **130**, the MSC **20**, **120** and the various databases that are consulted for the establishment of mobile calls (including the home location register (HLR) **21**, **121**; the visitor location register (VLR) **22**, **122**; the authentication center (AUC) **23**, **123**; and the equipment identity register (EIR) **24**, **124**). These databases are described below.

Although not illustrated, it is understood that HLR, VLR, AUC and EIR databases may be separate nodes from the associated MSC and may be directly accessed from other MSC's within the network.

Assuming that a subscriber is registered in the particular service area of the MSC **20**, HLR **21** contains data associated with that subscriber and is the main user database. MSC **20** is thus referred to as the "home MSC" whose HLR contains permanent data associated with that particular subscriber. The data stored in HLR **21** is the permanent data that is independent of the subscriber's present location within the wireless telecommunications network, plus temporary data such as the addresses of Service Centers that have stored short messages for a mobile station **30**. These addresses are erased after the short messages have been delivered. HLR **21** also indicates the signaling system point code used to find a module that contains the VLR currently associated with the mobile station **30**. HLR **21** may be connected to MSC **20** by a high-speed MAP interface.

The signaling system point code described above could be, for example, the CCITT signaling system 7 protocol (SS7), the ANSI (American standard) SS7 protocol or even the CCITT-defined X.25 protocol. Thus, while the signaling system point code is referred to hereinafter in terms of SS7 messages, it is understood the present invention is not limited to SS7 messaging and is equally applicable to other signalling systems as well (e.g., ANSI, X.25, etc.).

Because it is not expected for a subscriber to be constantly in the

service area of the home MSC **20**, each MSC **20**, **120** generally comprises a VLR **22**, **122** containing current temporary data for those mobile stations **30**, **130** locally registered within the service area of the particular MSC **20**, **120**, including the present or most recently known area of the subscriber's mobile station, the on/off status of the subscriber's mobile station, and various security parameters. The MSC where the subscriber is locally registered is referred to as the "visiting MSC".

The VLR is used for both local and roaming subscribers and has an extensive data exchange with the subscriber's HLR. The VLR is accessed by the MSC for each call setup, and therefore the MSC will always have an associated VLR. Because extensive signalling occurs between the MSC and VLR, they will usually be co-located. Often, the VLR is integral with the switch.

AUC **23**, **123** generally provides authentication and encryption parameters to screen for cloning fraud and provides data (cipher key) for encryption of the voice/data and control signals transmitted between the mobile station **30**, **130** and the base station system **10**, **100**.

EIR **24**, **124** retains a record of ranges of certified equipment identifications and ranges of or individual equipment identifications that are under observation or barred from service. Equipment identification information is received from the mobile station **30**, **130** at the MSC **20**, **120** and EIR **24**, **124** is used to verify that the equipment number of the mobile station **30**, **130** is certified for use in the network and is not on the observation or service barred list.

When a mobile station is first powered up within the cellular network, the mobile station's unique MIN (or International Mobile Subscriber Identification number (IMSI)) and ESN are used by the mobile station in a conventional manner to identify and register itself with the MSC serving the area within the network where the mobile station is located (visiting MSC). Such registration is generally accomplished by determining which base station system and associated MSC provides the greatest signal strength to the mobile station. Thus, the location area of the mobile station within the cellular network is determined by ascertaining which MSC the mobile station is currently registered with.

The mobile station continues to monitor the broadcast control channel (BCCH) for the identity of its location. When changes are noted, the mobile station issues a Location Update Request (LUR) that will register the mobile in the new

location. If the mobile station roams into an area supported by a different MSC and VLR, then the VLR will issue a new Mobile Subscriber Roaming Number (MSRN). The HLR associated with the home MSC is then provided with information about the mobile station's new MSRN. Alternatively, the VLR can inform the HLR of the current MSC location and the MSRN can then be transacted between the MSC and the HLR. At certain time intervals, the mobile station will be requested to provide Periodic Registration (PR) to update the VLR and HLR files on the mobile station's location and status.

FIGS. 2 and 3 illustrate the preferred architecture of the fraud detection system **200** according to the present invention. With reference to FIGS. 2 and 3, a fraud detection system (HLR Visibility System) **200** is provided that may interoperate with several network elements already in place in conventional wireless networks, including the MSC **20**, HLR **21**, Fraud Management System (FMS) **230** and Business Support System **212** (the database of customer account information, such as name, address, services subscribed to, etc.). The FMS **230** is part of the Fraud Mitigation Complex associated with the wireless network.

As illustrated in FIGS. 2 and 3, MSC **20** is communicatively connected to HLR **21** via a signaling data network. A typical network would comprise data links or channels (e.g., SS7 data links) and data switching elements **202**, **203** (e.g., Signalling Transfer Points (STP)). It is over these data links that messages (including mobile station registration signals) are communicated between the MSC **20** and HLR **21**. While it is understood that the present invention is applicable with several different types of signaling systems, SS7 and IS41 will be referred to hereinafter for clarity and illustrative purposes only.

The fraud detection system **200** preferably includes a monitoring system **201** that passively collects SS7 messages going to and from the HLR **21**. Preferably, the monitoring system **201** passively monitors the SS7 messages using a passive monitor tap **204**, such as a commercially available ADC Patchmate panel, which feeds the SS7 messages to the monitoring system **201**. It is understood, however, that the SS7 messages could also be captured and analyzed directly at HLR **21**, or at the data link switching elements **202**, **203**.

The monitoring system **201** should preferably be capable of passively monitoring a plurality of data links without loosing messages. The monitoring system **201** time stamps each message, which time stamp is preferably to an

accuracy of 1 millisecond resolution (plus or minus 1 millisecond) per hour variance from GMT. Furthermore, the monitoring system **201** preferably sends the monitored messages across an ethernet link using TCP/IP protocol.

One commercially available monitoring system **201** that may be utilized in accordance with the present invention is an INET Turbo-7 SS7 Analyzer, which is a packaged DOS-based 486 personal computer that operates on Turbo-7 "SPI NODE" software. Alternatively, a Tecelec STP may be utilized for forwarding the data link messages.

The messages forwarded by the Monitoring System **201** should preferably include a header block and binary data. The header block contains at least a time stamp, the data link number being monitored, the direction the message is going, and the length of the binary data which is the SS7 message.

Because the monitoring system **201** may also monitor a data link that carries several types of signaling protocol that are substantially the same (e.g., IS41, a North American standard, and proprietary mobility management signaling from other vendor's MSCs), the fraud detection system **200** converts any non-IS41B message (MTUP) into IS41 counterparts. The fraud detection system **200** will place messages in standard format. This format will pair SS7 transactions, which, according to IS41 protocol, are typically, but are not limited to, a series of independent transactions. Each transaction comprises an INVOKE message signaling unit (MSU) between two network elements (such as the MSC and HLR), and a RETURN RESULT between the same two network elements. The fraud detection system **200** looks for these INVOKE and RETURN RESULTS MSUs to create a single data element of a transaction. The message will then be placed into the fraud detection system's defined format..

A MSU Standard Interface **205** is preferably connected to the monitoring system **201** via an ethernet connection and collects MSU's from the wireless network and forward the collected MSU's to the fraud detection system **200** in a standardized format. The MSU Standard Interface **205** preferably includes the following capabilities:

- transaction pairing to provide both the INVOKE and RETURN RESULT as a transaction pair
- translation of proprietary mobility management MSUs to IS41 equivalents

- filters unnecessary message types and forwards transactions to pattern recognizers
- forwards all messages to logging function

A transaction log or database **206** is connected to the MSU Standard Interface **205** and stores all SS7 messages coming into the fraud detection system **200** into log files. All MSU's are captured into log files in a manner that data can be retrieved by an authorized fraud analyst at user interface **220** using keyed fields, such as MIN, date, time and message type. In addition, the log file display is configured to select messages in the following manner: date range, start time, stop time, MIN range, ESN or message type.

The messages are stored into a transaction log or database **206** for later retrieval and messages that are not required by the pattern recognizers **208** are also filtered out by data filter **207**. The data filter **207** functions to reduce the record processing load on each pattern recognizer **208**. Filtering may be accomplished based upon message type, MIN, system identification (SID) or point code.

The filtered messages are then forwarded within the fraud detection system **200** to pattern recognizers **208**, which contain user-defined pattern recognition algorithms indicative of fraud and process the filtered SS7 messages as they arrive to identify potentially fraudulent activity. The pattern recognizers **208** run concurrently on each MSU pair of SS7 messages as they arrive at the pattern recognizers.

When one of the pattern recognizers **208** identifies a possible fraud condition, that condition is reported by the pattern recognizer **208** to the fraud event manager **209** as a possible or probable fraudulent event. The fraud event manager **209** logs each such fraudulent event with at least the following information: date, time, event type, MIN, MSCID, priority and level of confidence of fraud. Priority and level of confidence of fraud are defined based on the event type.

Market specific, service provider defined actions based upon the priority and level of confidence of the identified fraudulent event may then be automatically performed by the fraud event manager **209**, which action may be tailored to the market environment, the probability of fraud and current subscriber status. Such actions may range from reporting the fraudulent event to requiring a user of a suspect mobile station to communicate with a fraud analyst of the service

provider before initiating a call. The fraud event manager **209** is preferably capable of generating standard event messages through CCITT X.25 protocol, ethernet, and async ports to drive the network elements it will interface with. A reporting system **210** thereafter marks for reporting each fraud event communicated by the fraud event manager **209**.

The MSU Standard Interface **205**, transaction log **206**, filter **207**, pattern recognizers **208**, fraud event manager **209** and reporting system **210** may be separate units or combined in a single programmable work station, such as a commercially available SUN SPARC 20 or equivalent work station.

The pattern recognition methods or algorithms applied by the pattern recognizers **208** include, but are not limited to, a geographic dispersion algorithm and periodicity algorithm.

The geographic dispersion method or algorithm analyzes the message received by the particular pattern recognizer **208** in which the method or algorithm is stored to identify unrealistic geographic movement between VLR's and authentication messages. The principle message to be monitored may be any message in the mobility management protocol that unambiguously identifies the location of the mobile station and any authentication message that unambiguously identifies a mobile station as successfully authenticating. A typical example of such a message to be monitored is the Registration Notification (IS41) messages (RegNot) and the Security Status Messages. The RegNot messages are generated every time a mobile station sends a registration message to the cell site, or when the mobile station attempts to initiate a call and there is no current VLR. The Security Status Message may be generated each time the mobile station authenticates and a parameter in the message indicates whether such authentication was successful.

A table of minimum travel times between all points in the wireless network is maintained in or is accessible by the pattern recognizer **208** in which the algorithm is stored. The minimum travel times stored in the table take into account the realities of Cellular Radio transmission distances.

The registration signals regularly generated by the mobile stations within the cellular network are utilized in accordance with the present invention to detect potentially fraudulent activity (e.g., cloning fraud). In conventional cellular networks, the mobile stations generate a registration signal approximately every 10 minutes to 20 minutes. Each time the mobile station moves and registers on a

different MSC, the HLR associated with the home MSC receives and sends several SS7 IS 41 messages.

The pattern of Registration Notification (RegNot) messages is analyzed at the HLR and potentially counterfeit or fraudulent mobile stations are identified by searching for unrealistic movements between MSC's (e.g., from New York to Los Angeles in a period of 10 minutes). Detection of such unrealistic movement in a given period of time alerts the telecommunications service provider of a very high probability of the existence of cloning fraud.

FIG. 4 is illustrative of the above-mentioned technique. If, for example, a mobile station located in Seattle, Washington registers with the MSC covering that area (Seattle MSC) at 9:00 a.m., the Seattle MSC will send a RegNot message back to the HLR associated with that mobile station located, for instance, in Santa Barbara, California. If the power of a cloned mobile station located in Miami, Florida is thereafter turned on at 9:10 a.m., the MSC covering that area (Miami MSC) will also send a RegNot message to the Santa Barbara HLR. By comparing the time of the registrations with the known distances between cellular coverage areas (e.g., the distance between Seattle and Miami), a high probability of cloning fraud is identified.

Referring now to FIG. 5, there is illustrated a representative pattern of RegNot and Security Status Messages applicable to the geographic dispersion method or algorithm. At step **1** in FIG. 5, a first mobile station in the coverage area of VLR 1 registers autonomously on VLR 1 (authentication is not available on VLR 1). At step **2**, VLR 1 identifies the MIN associated with the first mobile station, decodes the MIN to identify an HLR destination associated with the authorized subscriber, and sends a RegNot message to the HLR. The HLR looks up the MIN/ESN stored in its database and compares the stored MIN/ESN to the MIN/ESN contained in the received RegNot message. If the received MIN/ESN and stored MIN/ESN are the same, then the HLR sends a return result with the authorized subscriber's profile to VLR 1.

In step **3** illustrated in FIG. 5, VLR 1 constructs the subscriber's profile and sends a registration acknowledgement to the first mobile station. The first mobile station now initiates an internal timer and will re-register when the registration clock in the overhead messages reaches the re-registration time interval defined by VLR 1. This re-registration time interval is constant and is preferably

between 10 and 30 minutes depending upon the particular VLR and MSC settings.

In step **4** illustrated in FIG. 5, a second mobile station (having the same MIN and ESN as the first mobile station in the coverage area of VLR 1) is turned on in the coverage area of VLR 2, which is geographically remote from the coverage area of VLR 1. If the second mobile station is equipped and set for autonomous registration and, if it is time to register, then the second mobile station will generate a registration attempt to VLR 2.

In step **5**, VLR 2 identifies the MIN of the second mobile station, decodes the MIN to the HLR destination associated with the authorized subscriber and sends a RegNot message to the HLR. Once again, the HLR looks up the MIN/ESN stored in its database and compares the stored MIN/ESN to the MIN/ESN contained in the RegNot message received in step **5**. If the received MIN/ESN and stored MIN/ESN are the same, then the HLR sends a return result with the subscriber's profile to VLR 2.

At this time, it is possible to detect that there is a possible cloned mobile station by analyzing the time intervals between steps **2** and **5**. The distance between VLR 1 and VLR 2 is obtained from the table of distances preferably stored in the pattern recognizer **208**. If the elapsed time interval is too short for the physical distance between VLR 1 and VLR 2, then a likelihood of cloning fraud is identified.

In step **6** of FIG. 5, VLR 2 constructs the subscriber's profile and sends a registration acknowledgement to the second mobile station in the coverage area of VLR 2. The second mobile station now initiates an internal timer and will re-register when the registration clock in the overhead messages reaches the re-registration time period or interval defined by the VLR 2. This re-registration time interval is also constant and is preferably between 10 and 30 minutes depending upon the particular VLR and MSC settings.

In step **7**, the HLR cancels the old VLR record in VLR 1 by sending a Registration Cancellation (RegCanc) message to VLR 1. In step **8**, VLR 1 deletes the VLR record in response to the RegCanc message and sends a return result message to the HLR indicating a successful cancellation.

Having identified a possible fraudulent event, VLR 2 is equipped and capable of making authentication (as discussed further below) when a call is initiated on the second mobile station in step **9**. At this time, an authentication

challenge is performed in a conventional manner at VLR 2 as illustrated in step **10**. If the result to the authentication challenge is successful, the second mobile station is identified as the authorized mobile station and a report is sent back to the HLR Authentication Center (AC).

Thus, if the time between registrations (velocity) at VLR 1 and VLR 2 for a single MIN/ESN is unreasonably short for the geographic distance between VLR 1 and VLR 2, then there is a high probability that the first mobile station originally registered at VLR 1 is the cloned or fraudulent mobile station. Alternatively, if the result of the authentication challenge was unsuccessful, then there is a high probability that the second mobile station is the cloned mobile station.

It is understood that the above-mentioned scenario is illustrative of the manner in which the fraud detection system identifies potentially fraudulent activity and that the cloned mobile station may also be detected by several other combinations of registration and call events. For example, the fraud detection system would also have detected a cloned mobile station if the authorized subscriber had registered first on VLR 2 and placed a call, and then the unauthorized user on the cloned mobile station had registered on VLR 1 in an unrealistic time frame.

In addition to the geographic dispersion fraud detection method described above, the pattern recognizers **208** also detect cloning fraud within the cellular network using a periodicity method or algorithm to analyze the message received by the particular pattern recognizer **208**. This periodicity method or algorithm utilizes the regular registration patterns of mobile stations within the cellular network that are in the service area of different MSC's (rather than necessarily being geographically dispersed as in the geographic dispersion fraud detection method described above).

The periodicity fraud detection method or algorithm is illustrated in FIGS. 6 and 7 and is described below. Each subscriber's mobile station registers every time the overhead message "alarm clock" goes off or the system identification (SID) changes. When crossing a border from the coverage area of a first MSC into the coverage area of a second MSC, a registration is usually triggered as the clocks in each MSC are offset.

In addition, a significant number of subscribers' mobile stations may register several times on a single MSC. In general, these mobile stations are

relatively immobile and situated deep within the coverage area of the serving MSC. Typically, if one were to view the data links associated with these mobile stations, there would be one registration back to the HLR and then nothing for several registration periods.

Furthermore, there is another group of subscribers that move on the coverage area border of more than one MSC. The mobile stations of these subscribers tend to generate random registrations depending upon the speed and location of the mobile station. Typically, every change between MSC's is identifiable on the HLR data links.

Thus, as is illustrated in FIGS. 6 and 7, should a cloned mobile station register at the same time as an authorized mobile station, then several detectable patterns of registration (RegNot) messages emerge that are indicative of cloning fraud.

Referring to step **1** illustrated in FIG. 6, a first mobile station in the coverage area of VLR 1 registers autonomously on the VLR 1 (authentication is not available on VLR 1). At step **2**, VLR 1 identifies the MIN associated with the first mobile station, decodes the MIN to identify an HLR destination associated with the subscriber, and sends a RegNot message to the HLR. The HLR looks up the MIN/ESN stored in its database and compares the stored MIN/ESN to the MIN/ESN contained in the received RegNot message. If the received MIN/ESN and stored MIN/ESN are the same, then the HLR sends a return result with the authorized subscriber's profile to VLR 1.

In step **3** illustrated in FIG. 6, VLR 1 constructs the subscriber's profile and sends a registration acknowledgement to the first mobile station. The first mobile station initiates an internal timer and will re-register when the registration clock in the overhead messages reaches the re-registration time interval defined by VLR 1 (e.g., the registration period set in VLR 1). This re-registration time period or interval is a constant and is preferably between 10 and 30 minutes depending upon the particular VLR and MSC settings.

In step **4** illustrated in FIG. 6, a second mobile station (having the same MIN and ESN as the mobile station in the coverage area of VLR 1) is turned on in the coverage area of VLR 2, which is geographically remote from the coverage area of VLR 1. If the second mobile station is equipped and set for autonomous registration and, if it is time to register, then the second mobile station

generates a registration attempt to VLR 2.

In step **5** illustrated in FIG. 6, VLR 2 identifies the MIN of the second mobile station, decodes the MIN to the HLR destination associated with the authorized subscriber, and sends a RegNot message to the HLR. Once again, the HLR looks up the MIN/ESN stored in its database and compares the stored MIN/ESN to the MIN/ESN contained in the RegNot message received in step **5**. If the received MIN/ESN and stored MIN/ESN are the same, then the HLR sends a return result with the subscriber's profile to VLR 2.

In step **6** illustrated in FIG. 6, VLR 2 constructs the subscriber's profile and sends a registration acknowledgement to the second mobile station in the coverage area of VLR 2. The second mobile station now initiates an internal timer and will re-register when the registration clock in the overhead messages reaches the re-registration time interval defined by VLR 2 (e.g., the registration period set in VLR 2). This re-registration time interval or period is a constant and is preferably between 10 and 30 minutes depending upon the particular VLR and MSC settings.

In step **7**, the HLR cancels the old VLR record in VLR 1 by sending a Registration Cancellation (RegCanc) message to VLR 1. In step **8**, VLR 1 deletes the VLR record in response to the RegCanc message and sends a return result message to the HLR indicating a successful cancellation.

In step **9** illustrated in FIG. 6, the first mobile station then re-registers with VLR 1 when the registration clock in the overhead messages reaches the re-registration time period set in and defined by VLR 1. In step **10**, VLR 1 will once again identify the MIN associated with the first mobile station, decode the MIN to identify the HLR destination associated with the authorized subscriber, and send another RegNot message to the HLR. In response to the RegNot message, the HLR looks up the MIN/ESN stored in its database and compares the stored MIN/ESN to the MIN/ESN contained in the received RegNot message. If the received MIN/ESN and stored MIN/ESN are the same, then the HLR sends a return result with the authorized subscriber's profile to the VLR 1.

In step **11** illustrated in FIG. 6, VLR 1 again constructs the subscriber's profile and sends a registration acknowledgement to the first mobile station. The first mobile station initiates the internal timer and will re-register when the registration clock in the overhead messages reaches the re-registration time

period defined by the VLR 1.

In step **12** illustrated in FIG. 6, the second mobile station (having the same MIN and ESN as the mobile station in the coverage area of VLR 1) then re-registers with VLR 2 when the registration clock in the overhead messages reaches the re-registration time period set in and defined by the VLR 2. At step **13**, VLR 2 will once again identify the MIN associated with the second mobile station, decode the MIN to identify the HLR destination associated with the authorized subscriber, and send another RegNot message to the HLR. In response to this RegNot message, the HLR looks up the MIN/ESN stored in its database and compares the stored MIN/ESN to the MIN/ESN contained in the received RegNot message. If the received MIN/ESN and stored MIN/ESN are the same, then the HLR sends a return result with the authorized subscriber's profile to VLR 2.

In step **14** illustrated in FIG. 6, VLR 2 again constructs the authorized subscriber's profile and sends a registration acknowledgement to the second mobile station. The second mobile station initiates the internal timer and will re-register when the registration clock in the overhead messages reaches the re-registration time period defined by the VLR 2.

In step **15** of FIG. 6, the HLR cancels the old VLR record in VLR 1 by sending a Registration Cancellation (RegCanc) message to VLR 1. In step **16**, VLR 1 deletes the VLR record in response to the RegCanc message and sends a return result message to the HLR indicating a successful cancellation.

This re-registration process between the first and second mobile stations may repeat itself in the manner described above depending upon the location and status of the mobile stations.

The time interval between steps **2** and **10** illustrated in FIG. 6 is substantially equivalent to the registration period for VLR 1 if the first mobile station: (1) does not move out of the coverage area of the MSC associated with VLR 1; (2) is not powered down; (3) does not re-scan onto another MSC; and (4) does not initiate a call. Similarly, the time interval between steps **5** and **13** is substantially equivalent to the registration period for VLR 2 if the second mobile station meets conditions similar to those discussed above with respect to the first mobile station.

Thus, cloning fraud may be identified by analyzing the SS7 RegNot messages for the first and second mobile stations at the HLR and/or pattern

recognizers **208** and comparing the total number of RegNot messages associated with the MIN/ESN to the registration period of the MSC/VLR in which the mobile station is currently registered. This switch registration period may be determined by storing the registration periods for all of the MSC/VLR's in the network in a table and looking up the registration period for a desired MSC/VLR in which the mobile station is currently registered.

For example, assuming that the registration period for a first MSC (VLR 1) is set for 19 minutes and the registration period for a second MSC (VLR 2) is set for 21 minutes, then an authorized mobile station registered on the first MSC (VLR 1) and a cloned mobile station (having the same MIN and ESN as the authorized mobile station) registered on the second MSC (VLR 2) will cause SS7 RegNot messages to be generated in a pattern indicative of cloning fraud, such as that illustrated in FIG. 7.

In FIG. 7, each arrow represents an SS7 RegNot message associated with a particular MIN/ESN. Since the registration period for a particular MSC/VLR is constant, the first mobile station registered on the first MSC (VLR 1) in the above example generates a RegNot message every 19 minutes (the registration period set for the first MSC) to form a pattern of RegNot messages at 19 minute intervals. In the above example the second mobile station registered at the second MSC (VLR 2) generates a RegNot message every 21 minutes (the registration period set for the second MSC) to form a pattern of RegNot messages at 21 minute intervals. Because both mobile stations have the same MIN and ESN (e.g., one mobile station is a clone of an authorized mobile station), the combined RegNot messages for both the authorized and cloned mobile stations are forwarded as SS7 messages to the HLR where the permanent records associated with the subscriber's MIN are located.

Because the registration period for a particular MSC (VLR) is a constant, it is expected that the pattern of RegNot messages of an authorized subscriber's mobile station would be at discrete periodic intervals. Therefore, as illustrated in FIG. 7, when the pattern of RegNot messages for a particular subscriber is non-periodic (e.g., spaced apart at uneven intervals), then a cloned mobile station may be detected at the HLR and/or pattern recognizer **208**.

Having identified a possible cloned mobile station, the MSC/VLR responsible for the coverage area in which the mobile station is located is equipped

and capable of making authentication (as discussed further below) when a call is initiated on that mobile station. At this time, an authentication challenge may be performed in a conventional manner at the VLR. If the result to the authentication challenge is successful, the mobile station is identified as the authorized mobile station and a report is sent back to the HLR Authentication Center (AC). Alternatively, if the authentication result is unsuccessful, then the mobile station is identified as a clone and a report of the fraudulent event is generated.

While the above examples of the periodicity fraud detection method discuss analysis of the pattern of RegNot messages across two MSC/VLR's, it is understood that the present invention may be utilized to detect cloning fraud by analyzing a pattern of RegNot messages across more than two MSC/VLR's and/or where more than one cloned mobile station exists (each programmed to have the same MIN and ESN).

As discussed above, the geographic dispersion and/or periodicity fraud detection methods may be utilized to identify the existence of cloning fraud. To facilitate identification of the authorized subscriber's mobile station and the cloned mobile station, conventional authentication and encryption techniques may thereafter be utilized. As discussed below, conventional authentication and encryption techniques may include use of a challenge/response and encrypted data to identify the authorized mobile station.

One such authentication technique that may be utilized in accordance with the present invention to identify which of at least two mobile stations are authorized mobile station is described in European cellular communication system recommendations generated by Groupe Special Mobile (GSM). In general, this technique requires the subscriber to openly transmit a temporary mobile subscriber identification number (TMSI) to the base station system and/or MSC serving the mobile station, which in turn generates and transmits a random number (RAND) to the mobile station. The enciphering technique generally requires the mobile station to autonomously retrieve at least three enciphering elements from the memory of the mobile station (a predefined ciphering key, MIN and ESN). The mobile station then uses the ciphering key to encipher the MIN and ESN assigned to the mobile station to construct the RAND into a signed response (SRes), which is transmitted back to the base station system and/or MSC serving the mobile station.

The serving base station system and/or MSC thereafter looks up the

mobile station's ciphering key, MIN and ESN stored in a database using the subscriber's TMSI. The serving base station system and/or MSC generates a predicted response to the same RAND using the information retrieved from the database and compares the SRes received from the mobile station to the predicted response generated by the base station system/MSC. If the responses are substantially equivalent, then the mobile station is considered to be authorized and authentication of the mobile station is granted.

Another known authentication technique that may be utilized with the present invention to identify which of at least two mobile stations is authorized is described in the United States Digital Cellular (USDC) standard known as IS-54 and IS-95. Like the above-described GSM authentication technique, the USDC technique utilizes a series of specialized messages communicated between the mobile station and the serving base station system/MSC before authentication is granted. However, the USDC authentication method utilizes a so-called "challenge-response" authentication between the mobile station and the serving base station system/MSC using a shared secret key (S-Key) that is not communicated over the wireless network. The S-Key is a key that is known only by the parties involved in the authentication.

The global challenge of the IS-54/95 protocols is preferably 32 bits in length (as compared to the 128 bit RAND used in the GSM authentication method). When the global challenge is mixed or encrypted with the S-Key, the result is an 18 bit SRes. Further processing using the same algorithm and additional shared secret data (or using a different algorithm) generates a message encryption algorithm key and voice privacy mask. A mobile station that fails to successfully complete the challenge-response authentication is considered to be an unauthorized or cloned mobile station.

Once the cloned mobile station is identified using the above-described fraud detection methods, the fraud detection system according to the present invention may take any of a variety of pre-defined actions to prevent further fraudulent activity, including generating a counterfeit alert to other processes and network elements within the cellular network to shut down or monitor the cloned mobile station.

The FMS **230** of the Fraud Mitigation Complex may be responsible for taking such action once the fraudulent event is identified. The FMS **230** should

preferably have a flexible response for each detected type of fraud. The action to be taken by the FMS **230** may be defined by the telecommunications service provider based upon any of at least the following factors: the type of fraud detected, MIN, the MIN's current calling profile and/or the severity of the problem. It is understood that other factors may also be considered in determining the appropriate action to be taken in response to fraudulent activity.

Among the type of automatic actions that may be initiated by the FMS **230** are:

- Placing an indicator against the subscriber's MIN to prevent further incoming or outgoing calls. If the subscriber attempts to place a call, the subscriber will be connected to a fraud analyst for further processing.
- Placing an indicator against the subscriber's MIN to deny outgoing service (e.g., prevent initiation of calls), while not affecting incoming service.
- Setting up a roam authorization on a per MSC or point code basis to deny service within the geographic coverage area of that MSC or point code for a predetermined period of time.
- Command the serving MSC to tear down a call in progress on that MSC.

The FMS **230** should preferably be programmed with the intelligence to prevent repeat actions when the suspected counterfeiter (e.g., cloned mobile station) repeats the action that caused identification of the suspected cloning fraud in the first instance. In addition, FMS **230** may also contain a list of subscribers that should have no action taken against them. This may permit an operator to identify subscribers who have already been handled by other fraud mitigation techniques in the network.

It is also desirable to record such automatic actions taken by the FMS **230** in a log for audit and reconciliation purposes. This may be accomplished by sending a message in the Macrocell or AXYS customers record. Such log should preferably record all detected events, all actions taken, and be organized to allow a fraud analyst or other operator to analyze the data in at least the following ways:

- All detected data for a given period of time.
- All actions taken for a given period of time.

- All actions taken with respect to a given MIN or set of MINs.
- All detected events with respect to a given MIN or set of MINs.
- All detected events with respect to a particular event detector.
- All actions taken with respect to a particular event detector.
- All actions prevented by repeat action.
- All actions prevented because the subscriber is on a "no action" list.

Although illustrative preferred embodiments have been described herein in detail, it should be noted and will be appreciated by those skilled in the art that numerous variations may be made within the scope of this invention without departing from the principle of this invention and without sacrificing its chief advantages. The terms and expressions have been used herein as terms of description and not terms of limitation. There is no intention to use the terms or expressions to exclude any equivalents of features shown and described or portions thereof and this invention should be defined in accordance with the claims which follow.

CLAIMS

We claim:

1. A method of detecting fraudulent use of a mobile station in a wireless telecommunications network, the mobile station having a unique identifier associated therewith, the method comprising the steps of:

determining the actual elapsed time period between successive registrations associated with the unique identifier of the mobile station; and

detecting a suspected fraudulent event when the actual elapsed time period between successive registrations is substantially non-periodic.

2. The method according to claim 1, further comprising the steps of:

identifying a switch in the wireless network where the mobile station is registered;

determining the constant registration period associated with the switch, the constant registration period defining the expected time period between successive registrations by the mobile station to the switch; and

comparing the actual elapsed time period between successive registrations associated with the unique identifier of the mobile station to the constant registration period associated with the switch to determine whether the actual elapsed time period is substantially non-periodic.

3. The method according to claim 2, wherein the actual elapsed time period between successive registrations is substantially non-periodic when the actual elapsed time period corresponds to at least two different constant registration periods.

4. The method according to claim 1, further comprising the step of monitoring registration messages associated with the unique identifier to determine the actual elapsed time period between successive registrations.

5. The method according to claim 4, wherein the registration messages are passively monitored at the Home Location Register associated with the unique identifier of an authorized mobile station.

6. The method according to claim 1, further comprising the steps of:

receiving a response to an authentication challenge from the mobile station;

determining a predicted response based upon at least the unique identifier of the mobile station;

comparing the received response to the predicted response; and

identifying the mobile station as an unauthorized mobile station when the received response is not substantially the same as the predicted response.

7. The method according to claim 6, further comprising the step of providing an indication of a fraudulent event when the mobile station is identified as being unauthorized.

8. The method according to claim 6, further comprising the step of instructing the wireless telecommunications network to take a predefined action in response to identification of the mobile station as being unauthorized.

9. The method according to claim 1, further comprising the steps of:

determining the location of the mobile station within the wireless network at each registration associated with unique identifier;

determining the approximate distance between the determined locations for successive registrations associated with the unique identifier;

calculating an apparent velocity of the mobile station between successive registrations based upon the approximated distance and the actual elapsed time period between successive registrations;

comparing the apparent velocity with a predetermined maximum velocity; and

detecting a suspected fraudulent event when the apparent velocity exceeds the predetermined maximum velocity for successive registrations associated with the unique identifier of the mobile station.

10. The method according to claim 9, further comprising the steps of:

receiving a response to an authentication challenge from the mobile station;

determining a predicted response based upon at least the unique identifier of the mobile station;

comparing the received response to the predicted response; and

identifying the mobile station as an unauthorized mobile station when the received response is not substantially the same as the predicted response.

11. The method according to claim 10, further comprising the step of providing an indication of a fraudulent event when the mobile station is identified as being unauthorized.

12. The method according to claim 8, further comprising the step of instructing the wireless telecommunications network to take a predefined action in response to identification of the mobile station as being unauthorized.

13. A method of detecting fraudulent use of a unique identifier associated with an authorized mobile station in a wireless telecommunications network, comprising the steps of:

monitoring registration messages associated with the unique identifier;

determining a first elapsed time between successive first and second registration messages associated with the unique identifier;

determining a second elapsed time between the second registration and a successive third registration associated with the unique identifier;

detecting a suspected fraudulent event when the first and second elapsed times are not substantially the same.

14. The method according to claim 13, further comprising the steps of:

identifying at least one switch in the wireless network where a mobile station utilizing the unique identifier is registered;

determining the constant registration period associated with the switch, the constant registration period defining the expected time period between successive registrations by the mobile station;

comparing the elapsed time between successive registrations to the constant registration period associated with the switch; and

detecting a suspected fraudulent event when the first or second elapsed time is not substantially the same as the constant registration period.

15. The method according to claim 13, wherein the registration messages are passively monitored at the Home Location Register (HLR) associated with the unique identifier of the authorized mobile station.

16. The method according to claim 13, wherein the unique identifier is the unique mobile identification number (MIN) and equipment serial number (ESN) of the authorized mobile station.

17. The method according to claim 13, further comprising the steps of:

receiving a response to an authentication challenge from a suspected mobile station utilizing the unique identifier;

determining a predicted response based upon at least the unique identifier of the authorized mobile station;

comparing the received response to the predicted response; and

identifying the suspected mobile station as an unauthorized mobile station when the received response is not substantially the same as the predicted response.

18. The method according to claim 17, further comprising the step of providing an indication of a fraudulent event when the suspected mobile station is identified as being unauthorized.

19. The method according to claim 17, further comprising the step of instructing the wireless telecommunications network to take a predefined action in response to identification of the suspected mobile station as being

unauthorized.

20. The method according to claim 13, further comprising the steps of:

monitoring the successive first and second registration messages associated with the unique identifier to determine the respective location of the mobile station within the wireless network at the time of each of the registration messages;

determining the approximate geographic distance between the respective locations of the mobile station at the time of the first and second registration messages;

calculating an apparent velocity of the mobile station between the first and second successive registration messages based upon the approximated geographical distance and the first elapsed time between the first and second successive registration messages;

comparing the apparent velocity with a predetermined maximum velocity; and

detecting a suspected fraudulent event when the apparent velocity exceeds the predetermined maximum velocity.

21. The method according to claim 20, further comprising the steps of:

receiving a response to an authentication challenge from a suspected mobile station utilizing the unique identifier;

determining a predicted response based upon at least the unique identifier of the authorized mobile station;

comparing the received response to the predicted response; and

identifying the suspected mobile station as an unauthorized mobile station when the received response is not substantially the same as the predicted response.

22. The method according to claim 21, further comprising the step of providing an indication of a fraudulent event when the suspected mobile station is identified as being unauthorized.

23. The method according to claim 21, further comprising the step of instructing the wireless telecommunications network to take a predefined action in response to identification of the suspected mobile station as being unauthorized.

24. A system for detecting fraudulent use of a unique identifier associated with an authorized mobile station in a wireless telecommunications network, comprising:

a monitoring system for collecting data associated with the registration of one or more mobile stations utilizing the unique identifier; and

a fraud detection processor in communication with the monitoring system for analyzing the data collected by the monitoring system, the processor comprising a first pattern recognition device for determining the periodicity of successive registration messages associated with the unique identifier, wherein a suspected fraudulent event is identified when the time between successive registration messages is non-periodic.

25. The system according to claim 24, further comprising a passive monitor tap for passively monitoring data at the Home Location Register (HLR) associated with the unique identifier of the authorized mobile station, the passively monitored data being transmitted from the tap to the monitoring system.

26. The system according to claim 25, wherein the tap passively monitors data on at least one data link connected to the HLR.

27. The system according to claim 24, wherein the unique identifier is the unique mobile identification number (MIN) and equipment serial number (ESN) of the authorized mobile station.

28. The system according to claim 24, wherein the fraud detection processor further comprises a second pattern recognition device for identifying suspected fraudulent activity when an apparent velocity of the mobile station utilizing the unique identifier between successive registration messages exceeds a

predetermined maximum velocity, the apparent velocity being based upon the approximated geographical distance and time between the successive registration messages.

29. The system according to claim 24, further comprising an authentication system for identifying a suspected mobile station as an unauthorized mobile station when a response to an authentication challenge received from the suspected mobile station is not substantially the same as a predicted response calculated by the authentication system based upon at least the unique identifier of the authorized mobile station.

FIG. 1

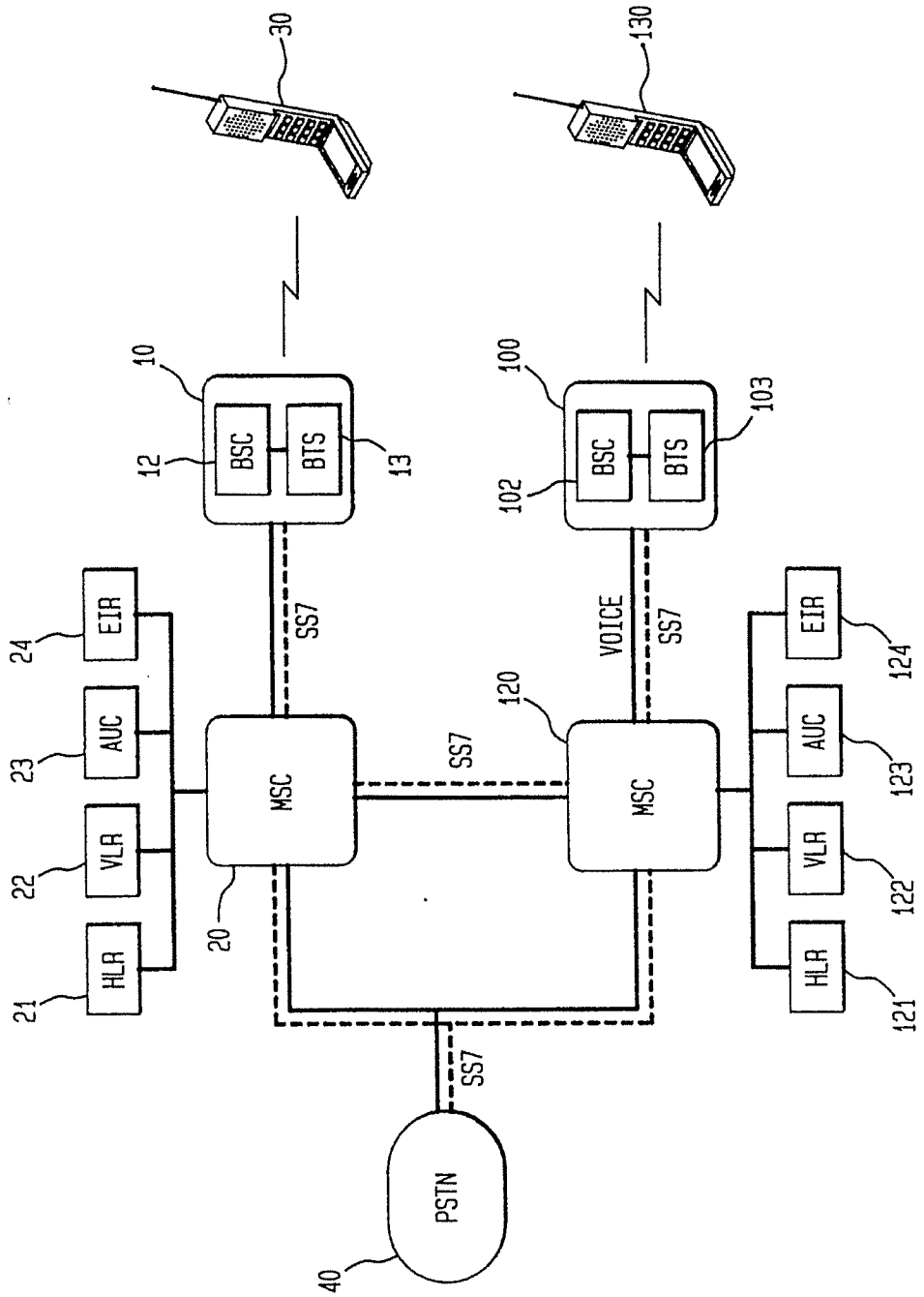

30
130
10
100
BSC
BTS
12
13
102
103
SS7
VOICE
EIR
AUC
VLR
HLR
24
23
22
21
124
123
122
121
MSC
20
120
PSTN
40

FIG. 2

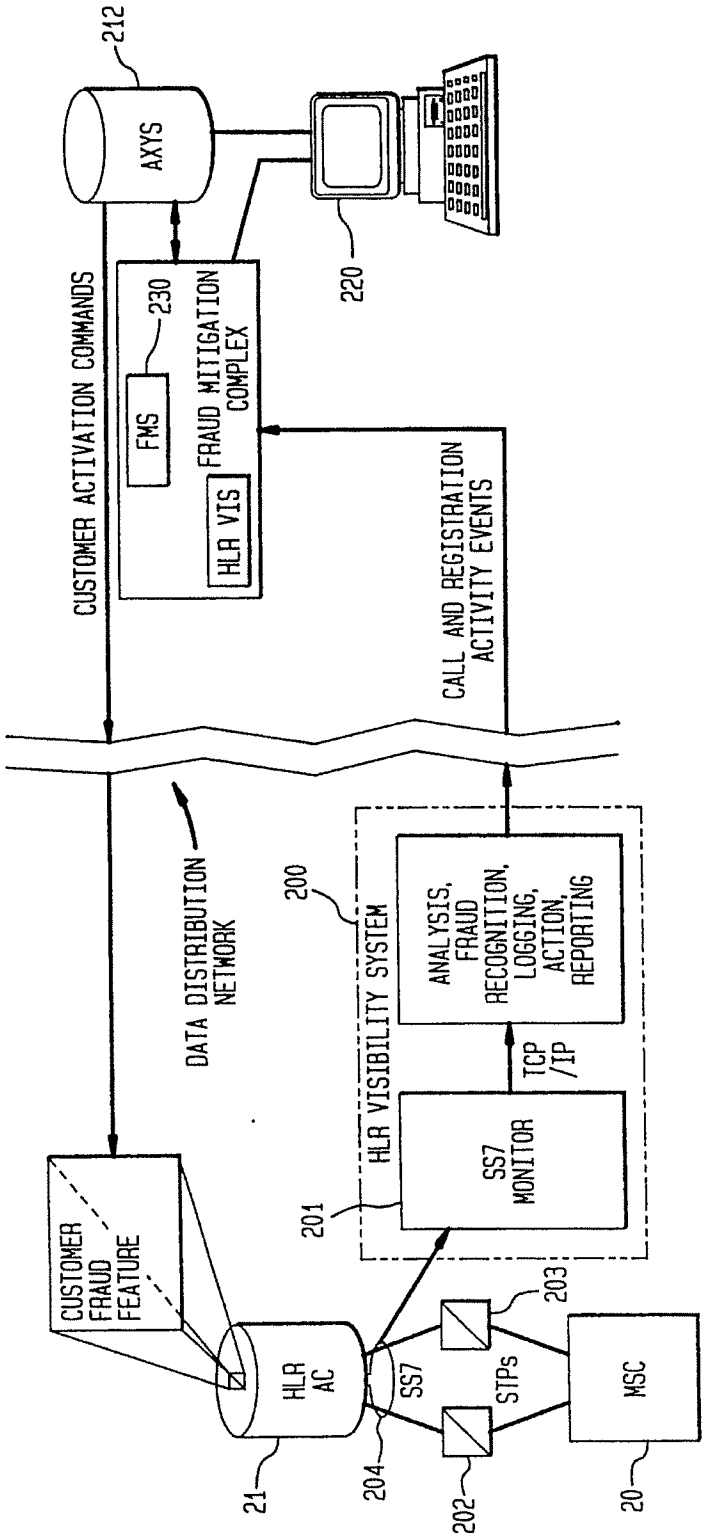

212
AXYS
220
230
FMS
HLR VIS
FRAUD MITIGATION COMPLEX
CUSTOMER ACTIVATION COMMANDS
CALL AND REGISTRATION ACTIVITY EVENTS
DATA DISTRIBUTION NETWORK
200
HLR VISIBILITY SYSTEM
ANALYSIS, FRAUD RECOGNITION, LOGGING, ACTION, REPORTING
TCP /IP
SS7 MONITOR
201
CUSTOMER FRAUD FEATURE
HLR AC
SS7
STPs
203
MSC
21
204
202
20

FIG. 3

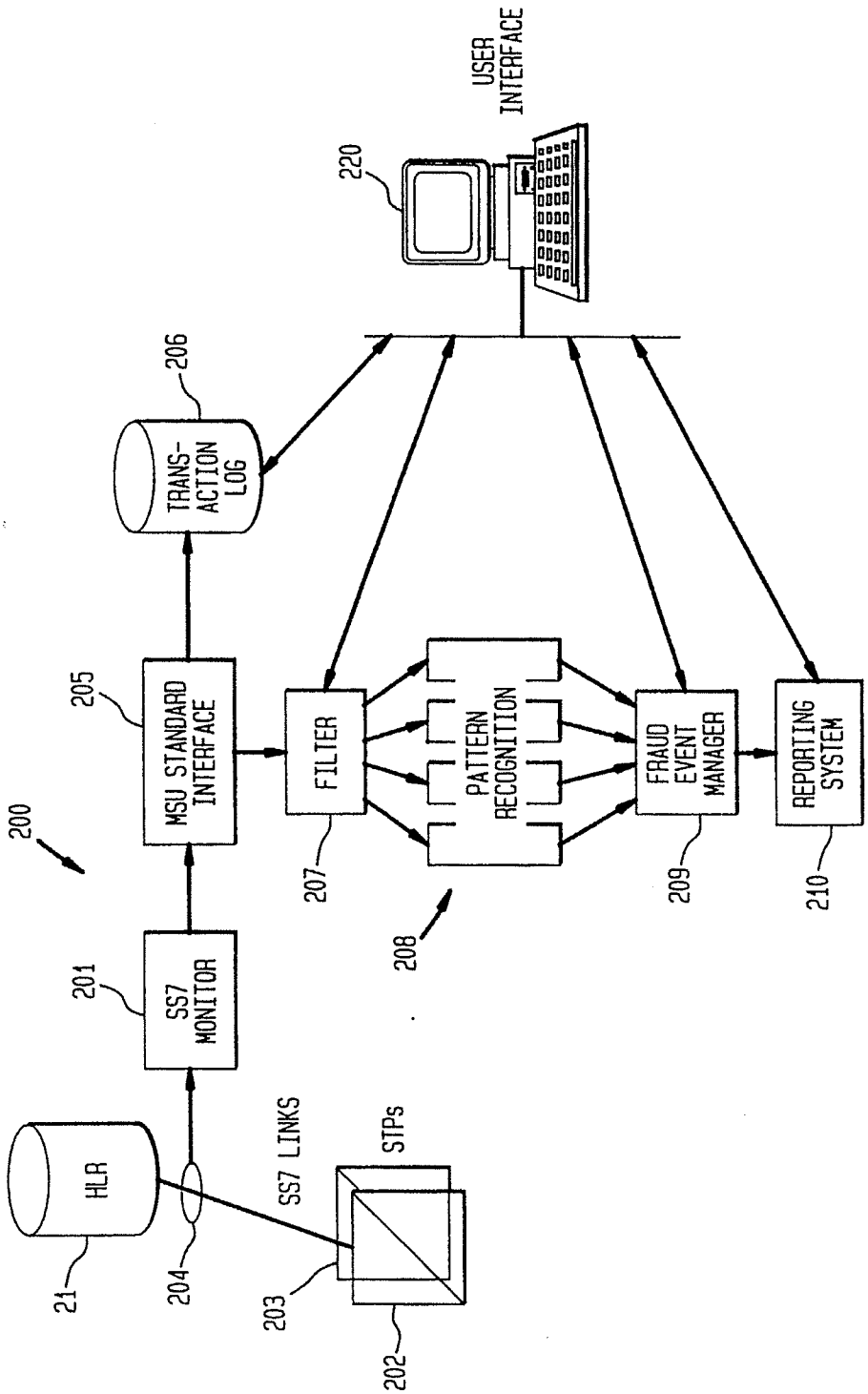

USER INTERFACE
220
206
TRANS-ACTION LOG
205
MSU STANDARD INTERFACE
200
FILTER
PATTERN RECOGNITION
FRAUD EVENT MANAGER
REPORTING SYSTEM
207
208
209
210
201
SS7 MONITOR
HLR
SS7 LINKS
STPs
21
204
203
202

FIG. 4

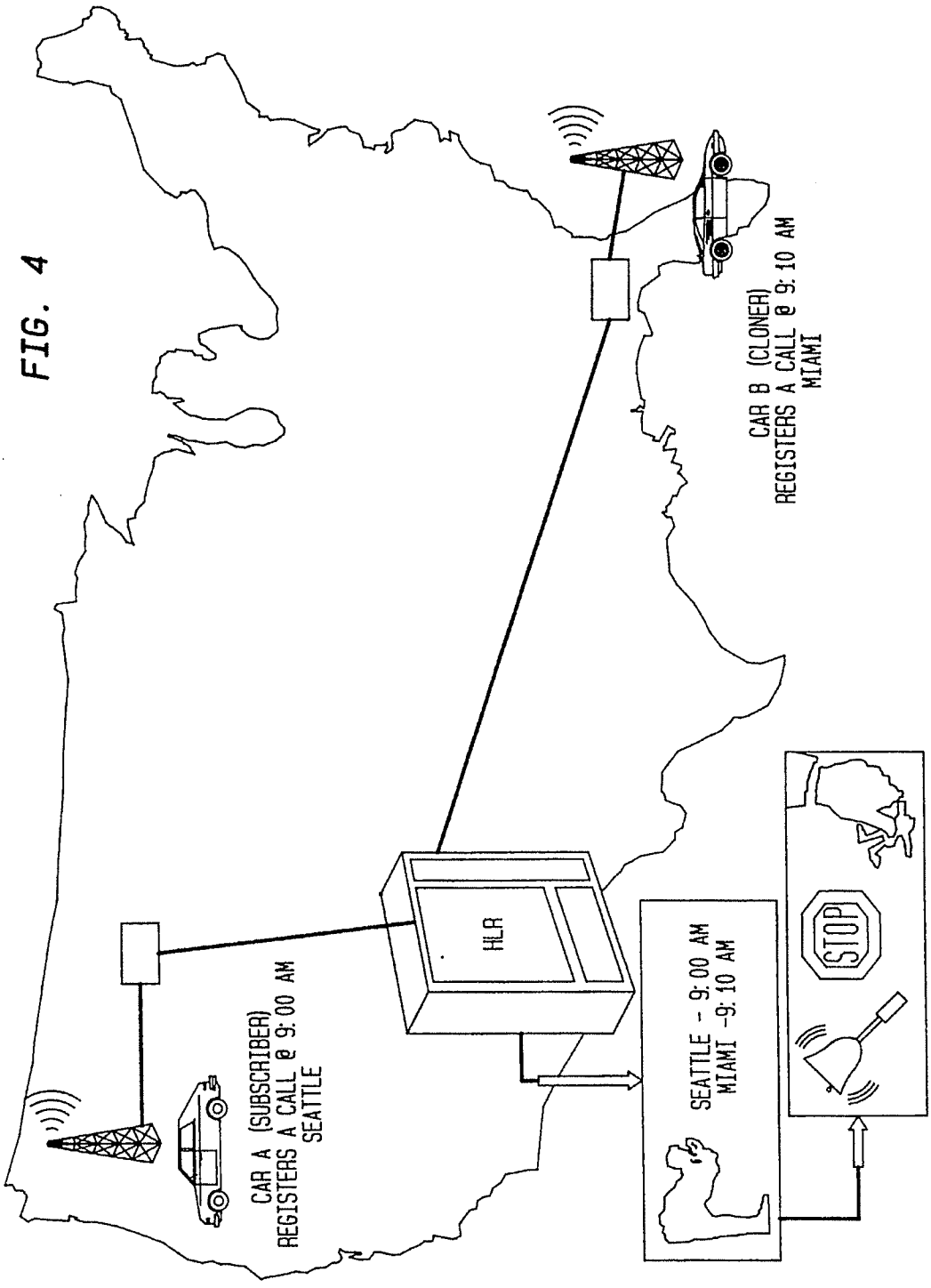

CAR A (SUBSCRIBER)
REGISTERS A CALL @ 9:00 AM
SEATTLE
HLR
SEATTLE - 9:00 AM
MIAMI -9:10 AM
STOP
CAR B (CLONER)
REGISTERS A CALL @ 9:10 AM
MIAMI

FIG. 5

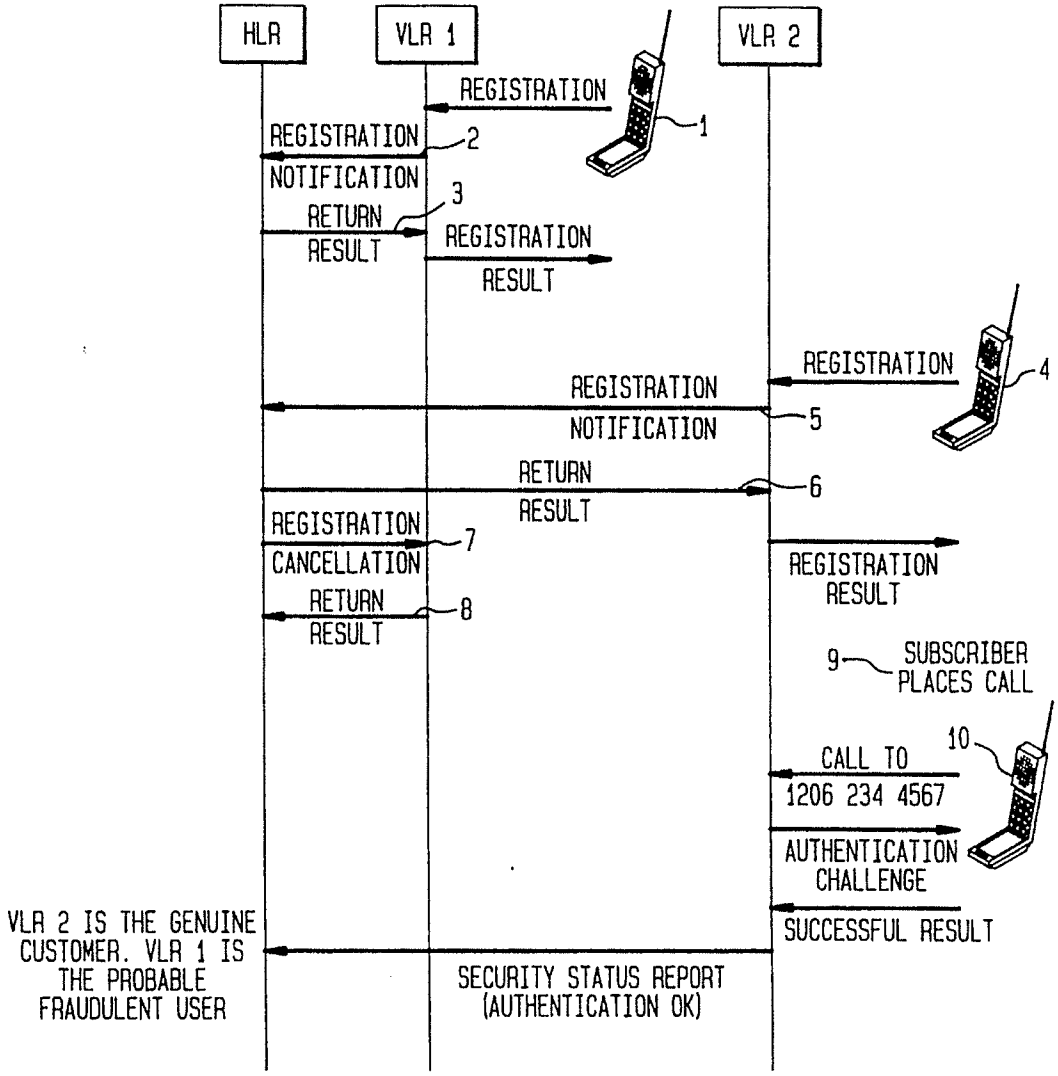

HLR
VLR 1
VLR 2
REGISTRATION
1
REGISTRATION
2
NOTIFICATION
3
RETURN
RESULT
REGISTRATION
RESULT
REGISTRATION
4
REGISTRATION
NOTIFICATION
5
RETURN
RESULT
6
REGISTRATION
7
CANCELLATION
RETURN
8
RESULT
REGISTRATION
RESULT
9
SUBSCRIBER
PLACES CALL
10
CALL TO
1206 234 4567
AUTHENTICATION
CHALLENGE
SUCCESSFUL RESULT
VLR 2 IS THE GENUINE
CUSTOMER. VLR 1 IS
THE PROBABLE
FRAUDULENT USER
SECURITY STATUS REPORT
(AUTHENTICATION OK)

FIG. 6

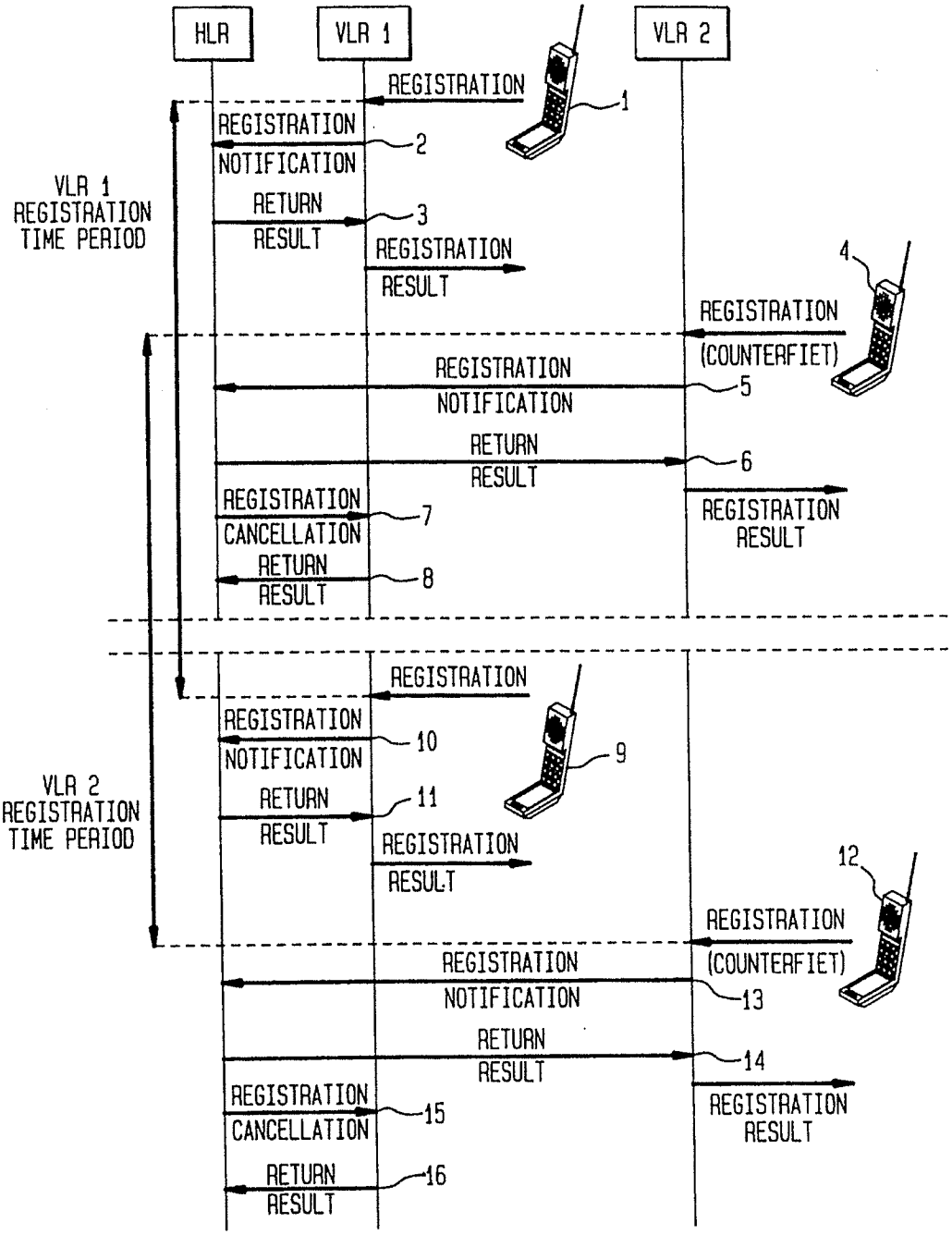
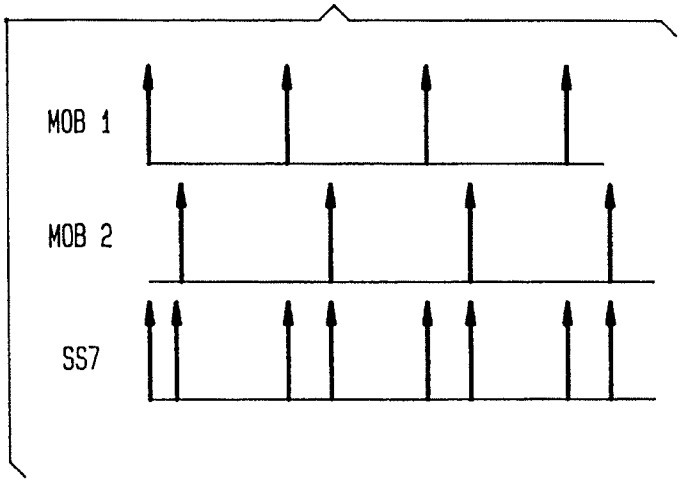

HLR
VLR 1
VLR 2
REGISTRATION
1
REGISTRATION
2
NOTIFICATION
VLR 1
REGISTRATION
TIME PERIOD
RETURN
RESULT
3
REGISTRATION
RESULT
4
REGISTRATION
(COUNTERFIET)
REGISTRATION
NOTIFICATION
5
RETURN
RESULT
6
REGISTRATION
RESULT
REGISTRATION
CANCELLATION
7
RETURN
RESULT
8
REGISTRATION
9
REGISTRATION
10
NOTIFICATION
VLR 2
REGISTRATION
TIME PERIOD
RETURN
RESULT
11
REGISTRATION
RESULT
12
REGISTRATION
(COUNTERFIET)
REGISTRATION
NOTIFICATION
13
RETURN
RESULT
14
REGISTRATION
RESULT
REGISTRATION
CANCELLATION
15
RETURN
RESULT
16

FIG. 7



PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/38

A3

(11) International Publication Number: WO 98/33340

(43) International Publication Date: 30 July 1998 (30.07.98)

(21) International Application Number: PCT/US98/00441

(22) International Filing Date: 7 January 1998 (07.01.98)

(30) Priority Data:
08/788,151 24 January 1997 (24.01.97) US

(71) Applicant: AT & T WIRELESS SERVICES, INC. [US/US]; 500 Carillon Point, Kirkland, WA 98033 (US).

(72) Inventors: AMIN, Umesh, J.; 10522 180 Court, N.E., Redmond, WA 98052 (US). ROWE, Lorin, B.; 14843 N.E. 14th Place, Bellevue, WA 98007 (US). WAUGHMAN, Russell, John; 13117 N.E. 128th Place, Kirkland, WA 98034 (US).

(74) Agent: DWORETSKY, Samuel, H.; AT & T Corp., P.O. Box 4110, Middletown, NJ 07748 (US).

(81) Designated States: BR, CA, JP, MX, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

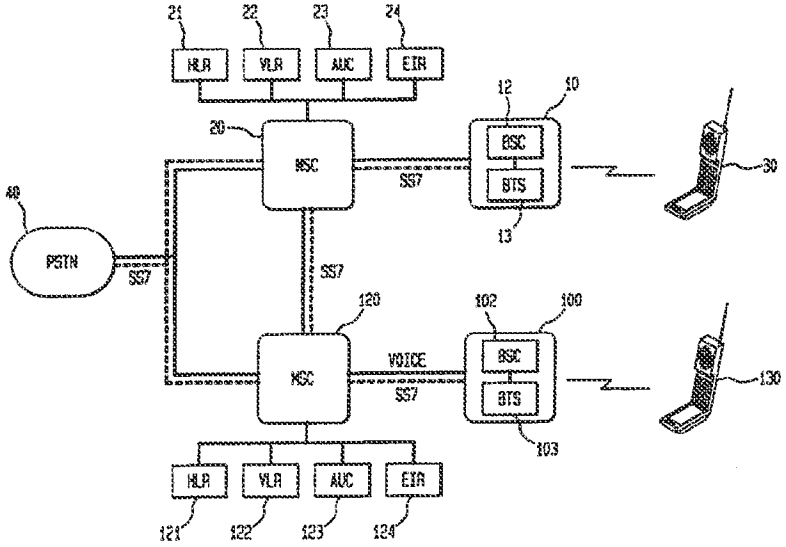
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
12 November 1998 (12.11.98)

(54) Title: DETECTION OF FRAUDULENTLY REGISTERED MOBILE PHONES

(57) Abstract

A system and method are provided for detecting fraudulent use of a unique identifier associated with an authorized mobile station in a wireless telecommunications network. A monitoring system passively collects data associated with the registration of one or more mobile stations utilizing the unique identifer. A fraud detection processor analyzes the collected data using a first pattern recognition device. The pattern recognition device determines the periodicity of successive registration messages associated with the unique identifier of the authorized mobile station and a suspected fraudulent event is identified when the time between successive registration messages is non-periodic. A second pattern recognition device may be utilized alone or in combination with the first pattern recognition device to identify suspected fraudulent activity when an apparent velocity of the mobile station utilizing the unique identifier between successive registration messages exceeds a predetermined maximum velocity. The apparent velocity is based upon the approximated geographical distance and time between successive registration messages. Upon the detection of a suspected fraudulent event by the first and/or second pattern recognition devices, an authentication system may be utilized to identify a suspected mobile station as an unauthorized mobile station when a response to an authentication challenge received from the suspected mobile station is not substantially the same as a predicted response calculated by the authentication system based upon at least the unique identifier of the authorized mobile station.



ERICSSON EXHIBIT 1005, Page 70

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/00441

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38

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 6 H04Q

Documentation searched other than minimumdocumentation 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 15643 A (TELEFONAKTIEBOLAGET LM ERICSSON) 23 May 1996 see figure 98 see page 35, line 35 - page 36, line 23 see page 37, line 9 - line 18 see page 45, line 2 - line 11	1
A	*Idem*	2,4,5,9, 13,14, 20,24,28
A	US 5 481 611 A (OWENS ET AL.) 2 January 1996 see abstract; figure 1 see column 3, line 51 - column 4, line 5	6,10,17, 21
A	EP 0 336 079 A (MOTOROLA INC.) 11 October 1989 see claim 1	6

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate 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 theinternational search	Date of mailing of the international search report
16 September 1998	28/09/1998

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	Danielidis, S

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/00441

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9615643 A	23-05-1996	US 5734977 A	31-03-1998
		AU 3942395 A	06-06-1996
		BR 9509723 A	21-10-1997
		CA 2204992 A	23-05-1996
		SE 9701723 A	08-07-1997
US 5481611 A	02-01-1996	NONE	
EP 336079 A	11-10-1989	US 4992783 A	12-02-1991
		CA 1314956 A	23-03-1993
		JP 2013035 A	17-01-1990

ERICSSON EXHIBIT 1005, Page 73

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2006 (05.10.2006)

PCT

(10) International Publication Number
WO 2006/104752 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2006/010108

(22) International Filing Date: 21 March 2006 (21.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/094,416 31 March 2005 (31.03.2005) US

(71) Applicant *(for all designated States except US)*: **LUCENT TECHNOLOGIES INC.** [US/US]; 600 Mountain Avenue, Murray Hill, New Jersey 07974-0636 (US).

(72) Inventors: **BU, Tian**; 57 J Reading Road, Edison, New Jersey 08817 (US). **NORDEN, Samphel**; 5621 DELMAR BOULEVARD, Apt. 811, St. Louis, Missouri 63112 (US). **WOO, Thomas, Y.**; 2 Exeter Road, Short Hills, New Jersey 07078 (US).

(74) Agent: **CURTIN, John, E.**; LUCENT TECHNOLOGIES INC., DOCKET ADMINISTRATOR - ROOM 3J-219, 101 Crawfords Corner Road, Holmdel, New Jersey 07733 (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.

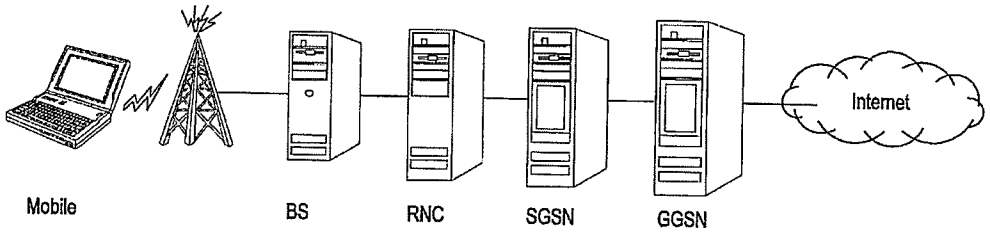
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, 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.

WO 2006/104752 A1

(54) Title: METHODS AND DEVICES FOR DEFENDING A 3G WIRELESS NETWORK AGAINST A SIGNALING ATTACK



(57) Abstract: Wireless state information and user/network profiling are used to detect and prevent Denial of Service attacks.

METHODS AND DEVICES FOR DEFENDING A 3G WIRELESS NETWORK AGAINST A SIGNALING ATTACK

BACKGROUND OF THE INVENTION

[0001] Denial of Service (DoS) attacks continue to present a significant challenge. In fact, the frequency and magnitude of attacks in the Internet have been steadily increasing. There have been a number of well-publicized attacks such as the February, 2000 attack on popular Web sites that included Yahoo, CNN, EBay, etc., and the recent attacks on root DNS servers.

[0002] DoS attacks typically involve sending a large volume of traffic to a node that exceeds its processing capability, in effect knocking the afflicted node out of the network for the duration of the attack. A more sophisticated attack is a Distributed DoS attack (DDoS).

[0003] An attacker intending to launch a DDoS attack begins by subverting a number of nodes, using well-known security loopholes. These compromised nodes essentially become slaves of the attacker and act as launch points to inject traffic into the network. By summoning a reasonable number of compromised nodes, an attacker can potentially launch a large-scale, network wide attack by cascading the traffic from multiple launch points.

[0004] A large variety of solutions have been proposed to counter DoS attacks. The current state-of-the-art in defending against DoS attacks include firewalls (Cisco's PIX router, Netscreen, Checkpoint's Firewall-1 are some examples), router modifications to support pushback, traceback mechanisms that attempt to detect the source of the attack, and related intrusion detection mechanisms that look for anomalies or signatures in arriving traffic. Some of these approaches require significant changes to existing network elements, and are costly to deploy, while others require collaboration across ISPs, and thus may be impractical. Nonetheless, these schemes do reduce the threat of wireline DoS attacks. For example, most firewalls do not

ERICSSON EXHIBIT 1005, Page 75

allow connections to be initiated from outside, thus preventing DoS flooding attacks.

[0005] Wireless networks on the other hand are significantly more fragile than wireline networks. There are several vulnerabilities in wireless networks that can be exploited by novel DoS attacks:

- **Limited wireless link bandwidth:** The scarcity of resources combined with the low capacity of a wireless link makes it an easy target of a DoS attack. In fact, the attacker's job is made even easier than in the wireline case because it takes significantly less traffic (i.e., relatively low volume) to overload a wireless link. In addition, the relatively low volume of traffic makes it difficult to detect a wireless DoS attack.

- **Processing Overhead:** A typical 3G1x or UMTS network has several infrastructure elements that perform a host of functions such as power control, resource allocation, paging, etc. A radio network controller (RNC) and base stations are involved in these activities for each mobile. With fast handoff, the overhead required by these devices is tremendous. Furthermore, such devices are typically engineered to handle a load with a certain number of users being simultaneously active. Overload, therefore, is a significant concern for any wireless infrastructure.

- **Limited Power supply:** Another constraining factor is that mobile devices ("mobile") in a wireless network are usually powered by batteries whose limited lifetimes make them targets of a class of attacks that simply drain their power by making the mobile perform redundant power consuming activities. This by itself can render the mobile inoperable.

ERICSSON EXHIBIT 1005, Page 76

- **Multi-targeted:** In a wireless DoS attack, the attacker has more flexibility because both the infrastructure as well as mobiles can be easily attacked. The same attack can now target multiple mobiles, either by attacking each mobile individually, or by targeting the wireless infrastructure for a more widespread effect. Furthermore, new architectures such as 1xEV-DO with its always-on capability increases the probability of an attack.

[0006] An attacker launching a wireless-specific DoS attack can easily exploit these vulnerabilities.

[0007] Another by-product of a wireless attack is that once the attack reaches a mobile it is too late. In a wireline DoS attack, it takes a certain amount of time for a server to be disabled because such machines have a larger processing capacity than a wireless endpoint (mobile). In contrast, a mobile has limited processing and battery lifetime. In addition, a wireless link is severely bandwidth-constrained when compared to a wireline network. If the traffic from an attack reaches a mobile, the attack has already succeeded in wasting critical resources of the wireless link, the wireless infrastructure, and the battery power of the mobile. This is in contrast to typical wireline DoS attacks that must overload processing resources at a server in order to succeed.

[0008] It is desirable, therefore, to provide methods and devices for detecting, preventing and defending against 3G wireless network DoS-like attacks. More particularly, it is desirable to provide methods and devices for detecting, preventing and defending against wireless DoS-like attacks launched against UMTS, CDMA2000 and other 3G wireless networks.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 depicts an example of a UMTS wireless network architecture.

ERICSSON EXHIBIT 1005, Page 77

[0010] FIG. 2 depicts an example of a message flow associated with the UMTS wireless network of FIG. 1.

[0011] FIGs. 3a and 3b depict exemplary simulations of a possible impact of a signaling attack.

[0012] FIG. 4 depicts exemplary steps in setting up a fundamental channel in a 3G1x wireless network.

[0013] FIG. 5 depicts an example of a 3G1x wireless network architecture.

[0014] FIG. 6 depicts an example of an architecture for detecting and preventing signaling attacks according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION, WITH EXAMPLES

[0015] A 3G wireless network requires the establishment (i.e., set-up) of a dedicated channel between a mobile and the associated wireless infrastructure for data to be transmitted. In order to set up the channel, signaling messages need to be transmitted between the mobile and elements of the wireless infrastructure. Signaling attacks seek to exploit the nature of this signaling to overload the wireless infrastructure.

Signaling attacks in UMTS networks

[0016] First, we begin with a brief introduction of the UMTS architecture. Then, we present an overview of the signaling required to set up a data channel and the vulnerability of a UMTS network to signaling attacks.

[0017] FIG. 1 shows the typical architecture of a UMTS wireless network. There are several components, beginning with the Gateway GPRS Support Node (GGSN) which is a GPRS network entity that serves as a wireless gateway between a Serving GPRS Support Node (SGSN) and the Internet. Additionally, the GGSN interfaces with authentication servers on external networks as well as DHCP servers

ERICSSON EXHIBIT 1005, Page 78

for dynamic address allocation. When a mobile or user successfully authenticates and registers with the network, a Point-to-Point (PPP) link is set up between the GGSN and the mobile.

[0018] The SGSN is responsible for sending data to and from mobile stations, in addition to maintaining information about the location and authentication of a mobile. Typically, there are multiple SGSNs, each of which serves the GPRS users physically located in their serving area.

[0019] A Radio Network Controller (RNC), also known as a Base Station Controller (BSC) is the point where wireless link layer protocols terminate. The RNC provides an interface between wireless devices communicating through Base Stations (BS) and the network edge. This includes controlling and managing the radio transceivers in BS equipment, including radio resource control, admission control, channel allocation, as well as management tasks like handoff between BS's and deciding power control parameters. The BS functionality includes wireless link transmission/reception, modulation/demodulation, physical channel coding, error handling, and power control. In this hierarchical architecture, multiple mobiles communicate with a BS, multiple BS's communicate with an RNC, and multiple RNC's talk to the GGSN/SGSN.

[0020] The UMTS signaling control flow for setting up channels for resource allocation is now described. Essentially, when data arrives for a subscriber, a UMTS RNC needs to establish a radio access bearer (RAB) with the base station of the subscriber. The RAB is a channel for data transfer and is released after a timeout period for inactivity. For establishing and releasing an RAB, a significant number of messages are exchanged between an RNC, mobile and base station. This is a significant amount of overhead for the RNC and causes severe processing overhead during signaling time intervals.

[0021] An example of a message flow between an RNC, base station(s) and a mobile is shown in FIG. 2. Essentially, for every data

ERICSSON EXHIBIT 1005, Page 79

call, a number of messages are exchanged between a mobile and an RNC. While the RNC is not the termination point for some of these messages (designated as Non Access Stratum or NAS messages), the RNC is required to forward these messages to the final destination in the core network (e.g., PDSN).

Radio Resource Control (RRC) Messages

[0022] RRC-like messages are used to establish/release radio channels for mobile power measurements, to transport paging messages and to broadcast information. An RRC setup leads to the creation of a dedicated signaling channel, which is the first step in enabling data transmission to/from a mobile. This requires 6 messages exchanged between the RNC and the mobile. Following this, there is a series of messages exchanged between the mobile and the core network for the purposes of authentication, and establishment of context, including a PPP connection with a PDSN, and assignment of an IP address. A further 4 messages are exchanged between the RNC, the core network and the mobile for a control security mode which results in the exchange of ciphers to secure the context for a given subscriber. Finally, an RAB is set up requiring an additional 8 messages exchanged at the RNC (2 with a core network, 3 with a mobile and 3 with a base station), resulting in a total of 24 messages to establish a single RAB with the RNC (not including messages exchanged between different elements within the RNC). It should be noted that subsequent RAB establishments do not need to perform an RRC signaling channel setup, though use of a control security mode may be required to re-authenticate a mobile.

[0023] Depending on the location of a mobile, a so-called soft handoff requires adding "legs" or base stations to the primary node with which the mobile has the strongest signal. This requires an additional 4 messages exchanged at the RNC (2 with the mobile and 2 with the primary base station). Finally, after a transfer, a mobile can initiate a teardown of RAB and RRC connections. This is initiated by

ERICSSON EXHIBIT 1005, Page 80

an IU release function. This requires a total of 11 messages exchanged at the RNC (2 with the core network, 4 with the mobile and 5 with the base station). This number again does not include intra-RNC processing messages that contribute to the overall load at the RNC.

[0024] If there is no data exchanged between a mobile and its core network, the mobile is placed in a suspended state. In such a state, air link resources are released and assigned to other active mobiles, which requires 4 messages (2 with its core network and 2 with a base station). However, the context is still maintained at the RNC, and the mobile retains its IP address obtained during RRC/RAB establishment. A mobile can be reactivated (2 messages exchanged with RNC) using a packet call context resumption message (additional 2 messages with its core network) as long as an idle timeout period of 5 seconds has not occurred.

Vulnerability and Nature of the Attack

[0025] An attacker exploits the heavy-duty signaling overhead required for setup of RABs by essentially triggering an excessive signaling message exchange between the RNC and BS. This may be achieved by sending a low volume burst at appropriately timed periods so that immediately after an RAB is torn down due to inactivity, a burst arrives from an attacker to trigger an establishment of a new RAB. This frequent setup/release can easily overload the RNC by requiring an excessive amount of signaling messages.

[0026] It should be noted that it is relatively easy for an attacker to obtain the IP addresses of mobiles. Wireless service providers typically assign chunks of contiguous IP addresses making it easy for an attacker to guess a valid range of addresses simply by posing as a valid subscriber.

[0027] Two salient features of an attack are worthy of note. First, as noted before, the low average transmission rate of the attack

(small bursts are sent periodically), make it hard for any existing detection mechanism to classify the traffic as malicious. The low volume also makes it easier for an attacker to launch an attack as opposed to conventional DDoS attacks requiring the attacker to compromise thousands of hosts in order to even launch an attack. Furthermore, only one packet needs to be sent per mobile allowing the attacker to have a widespread, diffused impact further complicating detection.

Damage Due to the Attack

[0028] The damage due to such an attack may be so severe that valid traffic may not receive an allocation of resources causing it to be dropped by an RNC. The RNC can also become overloaded, effectively denying service to a significant number of subscribers. In addition, RNC's are engineered to handle a certain amount of simultaneously active mobiles/users (in practice, 10%). It is easy for an attacker to exceed this number due to the low-volume nature of an attack.

[0029] Another side effect of a signaling attack is the potential for draining a mobile's battery. Normally, to conserve power, a mobile switches to a low-power idle or dormant state when there are no packets being sent or received. Because low volume bursts are sent periodically, mobiles would be forced to stay active longer than necessary. In a worst case scenario, a mobile may never be allowed to enter a dormant state causing rapid draining of its battery.

[0030] The present inventors performed simulations of the impact of an attack; some of the results are given by the graphs in FIGs. 3a and 3b. FIG. 3a plots a Base Station Controller's load versus time of day for a series of attacks, while FIG. 3b plots call set-up delay time (i.e., delay experienced after a call arrives until the time resources are allocated) versus time of day.

[0031] The results from FIGs. 3a and 3b demonstrate the drastic effect of an attack. Simply by sending 6% attack traffic, the load at an

RNC may be increased by a factor of 5 from a utilization of 15% to 75%. This also translates into a 5-fold increase in call setup delay, which further erodes consumer confidence, especially for providers touting real-time services. It is relatively easy to overload an RNC simply by sending around 10% attack traffic.

[0032] Changing gears, the following is a brief description of the 3G1x architecture (e.g., CDMA2000) and signaling.

3G1x Architecture

[0033] FIG. 5 depicts a typical architecture for a 3G1x wireless network. The PDSN may be a router, which functions as a gateway for data flow to and from all user mobiles/terminals in the entire wireless network. When a mobile or user successfully authenticates and registers with the network, a PPP link is set up between the GGSN and the user/mobile. On the path to the PDSN, there are three devices that are typically part of a wireless infrastructure. The RNC and the BS have functionality identical to their counterparts in UMTS. In this hierarchical architecture, multiple mobiles communicate with a base station, multiple base stations communicate with an RNC, and multiple RNCs talk to the PDSN.

3G1x Signaling

[0034] In a 3G1x network, there is an analogous problem for resource allocation. The equivalent of an RAB in UMTS networks is the fundamental channel (FCH) that needs to be setup to transfer data. Typical steps used to set-up an FCH are shown in FIG. 4.

[0035] When a PDSN receives data for a mobile, it pages the mobile. Once a successful response to a paging message has been received (3 messages exchanged), a base station initiates the setup of a FCH or Traffic Channel with the mobile (exchanging 8 messages). In parallel, a service request is made between the base station and an RNC requiring 4 messages. The RNC is also expected to forward messages to the core network, which in this case is required to

authenticate the user. This results in an additional 6 messages. Finally, 2 additional messages are exchanged between the RNC and the PDSN for accounting purposes. Once this is done, an active channel exists for transmitting data to and from the mobile.

[0036] Call release(s) follow the reverse procedure and require 7 messages from the RNC to the PDSN and base station, 8 messages between the base station and the RNC, PDSN and mobile. Overall, 29 messages are generated or received by the BS and 13 messages by the RNC in addition to 9 more messages that the RNC is responsible for forwarding to the core network.

[0037] Every subscriber typically has an primary leg assigned, which originally acts as the forwarding base station when a call is first setup. In certain cases, an additional base-station, called an anchor leg, is established for long-lived connections. This leg could be distinct from the primary leg and is defined as the base station with the strongest signal to the mobile. The anchor leg takes charge of deciding when to allocate supplemental channels (SCH), which are used when there is insufficient capacity on a 9.6Kbps FCH.

[0038] If there is excess data in the form of bursts that exceed the capacity of the FCH, then resources are allocated on demand to create a SCH for each user. There are an additional 16 messages exchanged between the anchor leg, the RNC and other base stations (for soft handoffs) leading to a similar vulnerability of the anchor leg for supplemental channel allocation and release.

[0039] While an attack on the anchor leg potentially has less widespread damage than an attack on the RNC, the impact is still severe enough to lead to a significant loss of revenue to a wireless service provider. If an attacker can impact multiple anchor legs, then the damage is magnified even more. An attacker may even be able to target the subscribers that belong to a particular anchor leg.

ERICSSON EXHIBIT 1005, Page 84

[0040] It should be noted that if an attacker simply sends randomly addressed bursts the damage could still be severe. Even if a single anchor leg is not in charge of the subscribers that are receiving the bursts, the RNC can still be overloaded due to its interaction with multiple anchor legs.

[0041] To prevent and defend against an attack, the present inventors recognized that knowledge of so-called wireless states, in particular the signaling cost(s) as traffic traverses through a wireless network was needed. This allows malicious traffic to be identified as soon as it begins to introduce excessive signaling cost. Signaling cost can be obtained in various ways depending on the wireless infrastructure involved. Ideally, an exact signaling cost can be obtained by querying wireless elements, such as an RNC and base station, when these elements provide an interface for such queries. However, current 3G wireless networks do not have such an interface, thus requiring modifications in order to support such queries. Changing an existing infrastructure, however, is not a viable solution given the amount of investment already expended by network owners/operators.

[0042] The present inventors discovered a simple, yet novel mechanism of estimating the signaling cost from traffic arrival patterns assuming knowledge of signaling call(s). The present inventions provide for methods and devices for detecting an attack using the so estimated signaling cost.

[0043] As mentioned above, if a wireless element provides an interface for querying, the signaling cost can be obtained by a simple query. Absent that, the challenge is to obtain the cost without the assistance of such wireless elements. In one embodiment of the present invention, the signaling cost is estimated from traffic arrival patterns. This requires knowledge of the signaling protocols inside wireless elements. Table 1 shows an example of a technique for estimating signaling cost (due to RAB establish/release) in a UMTS

ERICSSON EXHIBIT 1005, Page 85

network according to one embodiment of the present invention. Similar techniques within the scope of the present invention can be used to estimate other types of signaling costs for CDMA2000 networks according to alternative embodiments of the present invention.

TABLE 1

```
1. LastArrival(i) = 0
2. while true do
      a. Packet arrives for user i OR user i sends a packet
      b. IF (CurrentTime – LastArrival(i) > IdleTimeout) THEN
            i. Cost(i) += cost of RAB establishment
            ii. Cost(i) += cost of RAB release
3. LastArrival(i) = CurrentTime
```

[0044] The present invention makes use of the fact that, upon arrival of a packet, if the destination's RAB has been released, the destination mobile has to reestablish the RAB. This reestablishment creates an added cost to establish a new RAB and release the previous RAB due to the expiration of an idle timer; a cost which can be detected by techniques provided by the present invention.

[0045] A reliable sign of an ongoing signaling attack is the detection of excessive or additional signaling costs even though the volume of actual, transmitted data is low. Before continuing, it should be noted that an attacker can flood a network using huge amounts of traffic that would also introduce excessive signaling costs. However, this can be, relatively speaking, easily detected by existing firewall or intrusion detection mechanisms. With a low-volume attack, there needs to be a more accurate metric for detection. In accordance with the present invention, a statistical measure referred to as a signaling cost to data ratio is used as a metric. If the ratio exceeds a certain profiled threshold, a signaling attack is detected and malicious traffic/packets from the source of the attack are blocked. In a further embodiment of the present invention, if multiple attacks from the same source are detected, malicious traffic/packets, etc. from the source of the attack is blocked while allowing traffic from

ERICSSON EXHIBIT 1005, Page 86

other sources through, for example. Other intrusion detection mechanisms may also be used to reduce the chance of false alarms.

[0046] In accordance with an exemplary method of the present invention, the first step in determining if traffic is part of an attack is to define a threshold for later comparison. This should be user/application specific. The value of this threshold may be chosen by profiling user/applications during a pre-processing time period.

[0047] During such a time period, a profile for each user may be created based on a statistical signaling cost to data ratio. Information used in building the profile includes packet arrival times, IP addresses and port numbers of source(s) and destination(s).

[0048] One novel aspect of the profiling mechanism provided by the present invention is the ability to aggregate (user, application, as well as server) related profiles. By user profile, we refer to the statistics for an individual user. This division can be further categorized by individual application. For instance, web surfing is the most frequently used service by most users. Similarly, a video-on-demand server may use RTP packets to broadcast video to users. Statistics on an individual web server basis can also be compiled by logging the arrival of HTTP/RTP packets.

[0049] To enable scalability, the profiles can be aggregated across users with similar behaviors. Current traffic can then be compared to the aggregated profile to detect inconsistencies. Aggregated profiles can analogously be maintained for popular servers and also for popular applications. The flexibility of using different classification approaches allows a more comprehensive and accurate characterization of what is considered as normal traffic. This profile is key to detecting abnormal and malicious traffic, while also minimizing the probability of false positives (incorrect classification of valid traffic as malicious traffic).

ERICSSON EXHIBIT 1005, Page 87

TABLE 2

1. Collect the signaling cost to data ratio
    a. Query: Actual number of signaling messages exchanged per user from wireless elements
    b. Estimate: Infer signaling cost from packet arrivals
2. Detection: For packet(j) from sender s to user i:
    Metric: Signaling Cost to Data Ratio (S/D)
    IF (S/D) > $S/D_{THRESH}(i)$ for user i, THEN
        - $FLAG_J^S$++;
        - Start $INVALID_{TIMER}(s)$
3. Verification: IF ($FLAG_J^S$ > $VOTE_{THRESH}(s)$ OR $INVALID_{TIMER}$ = 0) THEN
        - Install filter at firewall to block data to s

[0050] Table 2 above sets forth an example of a method or algorithm for defending against a DoS Signaling attack. This method may be executed by a device or devices capable of either estimating or collecting user state statistical information (e.g., actual traffic flow) from the wireless infrastructure. In general this method operates as follows.

[0051] In an initial step, a current measure, such as a signaling cost to data ratio is generated or derived. This ratio can be obtained through either directly querying the infrastructure or by using an estimation technique.

[0052] Next, the signaling cost to data ratio is compared against a threshold, reference ratio. If the derived ratio exceeds the threshold for a user, i.e., S/D_{THRESH}, determined from a pre-processing step that builds a profile for the user, subsequent traffic from a sender "s" is flagged.

[0053] Lastly, if a sufficient number of packets (when compared to a threshold, $VOTE_{THRESH}$) have been flagged as suspicious from the sender s, OR the suspicious behavior lasts for an extended period of time ($INVALID_{TIMER}$), then a filter may be applied at a firewall to block future traffic from that sender.

ERICSSON EXHIBIT 1005, Page 88

[0054] It should be noted that the user profile generated during the pre-processing step is adaptable to user behavior in order to minimize false positives and accurately detect when a violation occurs. More specifically, after the initial profile is created during pre-processing, it may be updated regularly based on changes to a user's behavior.

[0055] The method utilized in Table 2 may be implemented in a number of different ways, one of which may be referred to as an Architecture for Wireless Attack REsistance (AWARE). AWARE-enabled devices may be modular and can support upgrades in order to counter future attacks.

[0056] In one embodiment of the present invention, an AWARE architecture (e.g., enabled device) may comprise two components: a *learning database* and *profiler*, and/or a *detection engine* or *detector*. The learning database is operable to capture and store information about a user during the pre-processing step. The profiler is operable to generate a traffic profile for a given user under normal (i.e., non-attack) conditions. The database and profiler may be one and the same and may be correlated with other user databases and profilers for cross-mobile correlation. The information in these databases is fed to a detector/detection engine. In one embodiment of the present invention, the detection engine is operable to maintain a threshold for each user and verify if current traffic for a user or set of users violates the corresponding threshold. Depending on the wireless elements that are capable of communicating with an AWARE-enabled device (one that contains a database, profiler and/or a detector), the location of the AWARE-enabled device may be varied:

- *Co-located with a Firewall:* An AWARE-enabled device can be co-located with a firewall of a wireless service provider. If such a design is chosen, then it is not necessarily assumed that any other part of the wireless infrastructure is aware of the presence

ERICSSON EXHIBIT 1005, Page 89

of an AWARE-enabled device or interacts with the AWARE-enabled device.

In an embodiment of the present invention, an AWARE-enabled device uses IP layer information such as packet arrivals and information from IP/TCP and application layer headers to build profiles. This assumes that the AWARE-enabled device can look inside a packet. If *IPsec* (tunnel mode) has been enabled, an AWARE-enabled device can be co-located with an IPsec gateway in the domain so as to be able to decrypt and inspect packet headers and payloads.

- *Between the PDSN and an RNC:* In an alternative embodiment of the present invention, an AWARE-enabled device may be placed between a PDSN and an RNC. In such a design, the device may interact with the PDSN, and obtain information as to how packets are distributed to different RNC's. An RNC provides finer grain information, such as: the number of signaling events for a FCH & SCH setup/release, the timestamp(s) of signaling messages, and power control information via a base station that estimates mobile power consumption. It should be understood that, in the event that an AWARE-enabled device is a stand-alone device, an AWARE-compatible interface may be needed to allow the device to operate with a wireless infrastructure (e.g., firewall).

[0058] In a "least-invasive" design, an AWARE-enabled device simply looks at IP packets that are passed on from a firewall before they reach the PDSN. All of the necessary information is contained in the application, TCP and IP headers and the payload itself. Information needed to build a profile can be extracted from the above headers and payload.

[0059] An AWARE-enabled device should be able to communicate with existing firewalls or IPsec gateways. Ideally, an AWARE-enabled

ERICSSON EXHIBIT 1005, Page 90

device may be co-located at these entities acting as a filter to block suspected traffic. If a AWARE-enabled device is not co-located with the IPsec gateway, there needs to be a so-called security association with the gateway so it can decrypt and process ESP-encapsulated packets in a tunnel mode. Even if an AWARE-enabled device is not co-located with the firewall, there typically is an interface with most commercial firewalls such as Checkpoint's Firewall-1 that allows the configuration of filters.

[0060] If an AWARE-enabled device is placed between the PDSN and an RNC, more user-specific state information may be gathered (i.e., which RNC a user belongs to, and potentially other information that can be obtained from an RLP frame). Also, an AWARE-enabled device may obtain mobility related information because a mobile may cross over from one RNC to another. The impact of mobility information on the detection heuristic is worth analyzing, because highly mobile end-users can contribute significantly to the load of an infrastructure. Launching a wireless DoS attack against highly mobile users requires additional tasks, such as more frequent paging, that can add substantially to processing overhead. Also, a mobile may initiate a PPP connection with the PDSN before initiating a transfer. An AWARE-enabled device may also query the PDSN to obtain a PPP state history.

[0061] In addition to AWARE-enabled devices, the present inventors also recognized that an AWARE related architecture may also require additional devices.

[0062] For example, an AWARE-compatible interface is provided by the present invention. In one embodiment of the present invention, such an interface is operable to query wireless user/mobile state(s). Such an interface also allows an AWARE-enabled device (or devices) to communicate in a secure manner with the wireless infrastructure in order to obtain mobile/user-specific information. It should be noted that such an interface may be included as an option in infrastructures

ERICSSON EXHIBIT 1005, Page 91

other than a PDSN, because at a minimum, packet arrivals need to be known in order to estimate state information.

[0063] In addition to an interface, the present invention provides for a plug-in detector.

[0064] *Snort* is an open-source IDS mechanism that emulates the functionality of an AWARE-enabled device. Snort is modular and allows new plug-ins to be installed, thus allowing the detection mechanism to be customized and enhanced for defense against current and future attacks. By "plug-in" is meant a generic term that refers to modules that can be added dynamically to alter the behavior of Snort.

[0065] In an additional embodiment of the present invention, a Snort compatible plug-in incorporating the detection heuristic functions of the present invention is provided.

[0066] Other plug-ins are also provided by the present invention. Again, during their experiments the present inventors utilized *Snortsam* to interface with a firewall and react to attacks.

[0067] In an additional embodiment of the present invention, a *Snortsam* compatible plug-in that allows such interfacing is provided by the present invention. Such a plug-in may be operable to act as filter(s) to block malicious traffic.

[0068] Alternatively, this plug-in may be interfaced with a wireless packet scheduler to reduce the priority of malicious traffic.

[0069] It should be understood that the methods of the present invention, the AWARE-enabled devices, interfaces, and any subcomponents (e.g., learning database, profiler, detector, etc.) may be realized in hardware, software, firmware or some combination of the three. For example, one or more programmable or programmed controllers, processors, etc. may be operable to store one or more programs or code (and data) that, in turn, is operable to carry out the

ERICSSON EXHIBIT 1005, Page 92

features and functions of the present invention described above and in the claims that follow.

ERICSSON EXHIBIT 1005, Page 93

We claim:

1. A method for detecting a signaling attack against a 3G wireless network comprising:

measuring a traffic level associated with a mobile device;

generating a cost-to-data ratio associated with the measured traffic level and a signaling cost; and

comparing the generated ratio to a profiled, reference cost-to-data threshold ratio to determine whether a Denial-of-Service signaling attack is directed at the device.

2. The method as in claim 1 further comprising preventing malicious traffic intended for the mobile device from reaching the device when the generated ratio equals or exceeds the threshold reference ratio.

3. The method as in claim 1 wherein the network is selected from the group comprising a UMTS or CDMA2000 network.

4. The method as in claim 1 further comprising generating the signaling cost from traffic arrival patterns.

5. The method as in claim 1 wherein the traffic level is a relatively low volume of data.

6. A method for detecting a denial-of-service (DoS) attack in a wireless network, comprising:

(a) generating a statistical measure characterizing a relationship between signaling cost and actual data transmitted to or from at least one mobile during normal operation of the wireless network;

(b) comparing the statistical measure to a current measure; and

ERICSSON EXHIBIT 1005, Page 94

(c) detecting a DoS attack if the current measure differs from the statistical measure by more than a threshold.

7. The method as in claim 6, wherein the statistical measure is based on a ratio of the signaling cost within a specified time interval to an amount of actual data transmitted to or from the at least one mobile within a specified time interval.

8. The method as in claim 7 further comprising estimating the ratio based on a traffic arrival pattern.

9. A 3G wireless network comprising:

one or more access nodes adapted to provide access between the wireless network and an Internet;

one or more radio network controllers (RNCs) adapted to communicate with the access node;

one or more base stations for each RNC adapted to communicate with an RNC and with one or more mobile units; and

an architecture adapted to:

(a) generate a statistical measure characterizing a relationship between signaling cost and actual data transmitted to or from at least one mobile during normal operations of the wireless network;

(b) compare the statistical measure to a current measure; and

(c) detect a DoS attack if the current measure differs from the statistical measure by more than a threshold.

10. A device for detecting a Denial-of-Service signaling attack against a 3G wireless network comprising:

a database operable to store mobile information;

ERICSSON EXHIBIT 1005, Page 95

a profiler operable to generate a traffic profile for the mobile associated with non-attack conditions, based on the stored information; and

a detector operable to detect an attack by comparing a traffic arrival rate associated with the mobile with a threshold associated with the at least the generated mobile profile.

ERICSSON EXHIBIT 1005, Page 96

FIG. 1

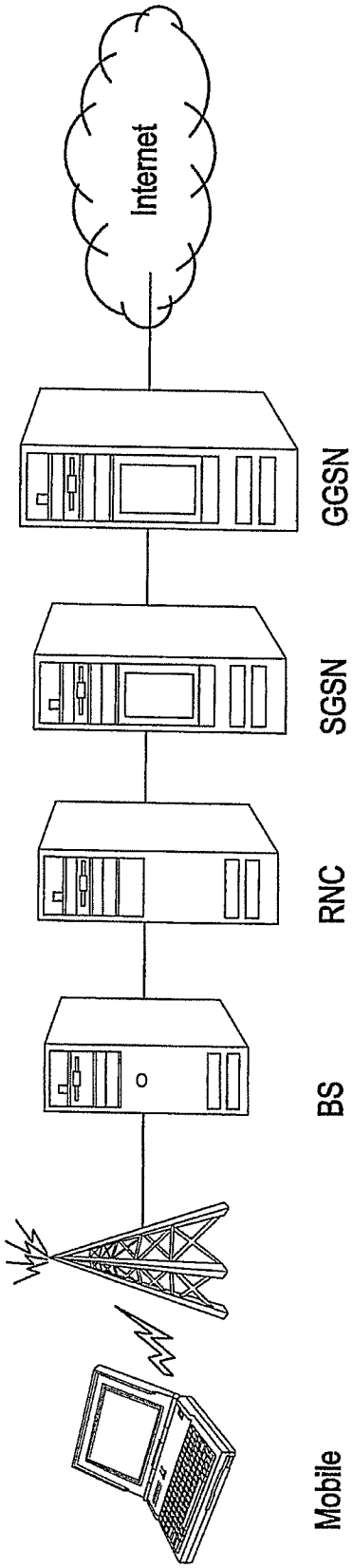


FIG. 2

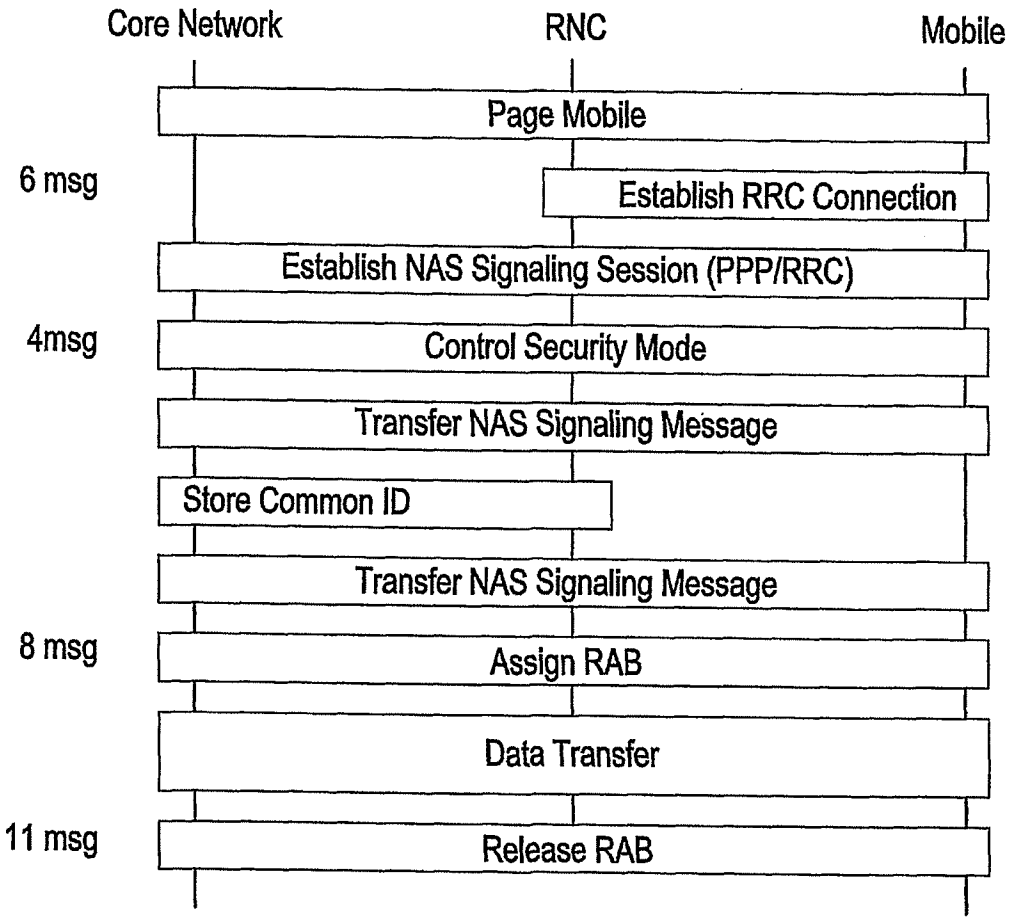

Core Network
RNC
Mobile
Page Mobile
6 msg
Establish RRC Connection
Establish NAS Signaling Session (PPP/RRC)
4msg
Control Security Mode
Transfer NAS Signaling Message
Store Common ID
Transfer NAS Signaling Message
8 msg
Assign RAB
Data Transfer
11 msg
Release RAB

FIG. 3A

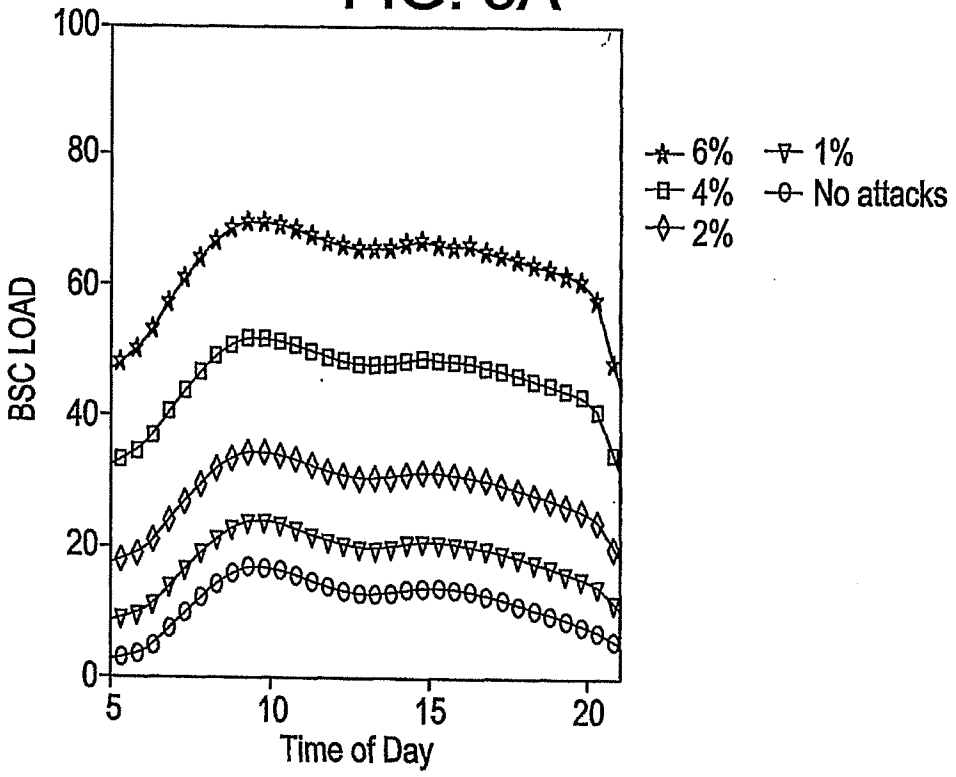

100
80
60
40
20
0
BSC LOAD
5
10
15
20
Time of Day
6%
1%
4%
No attacks
2%

FIG. 3B

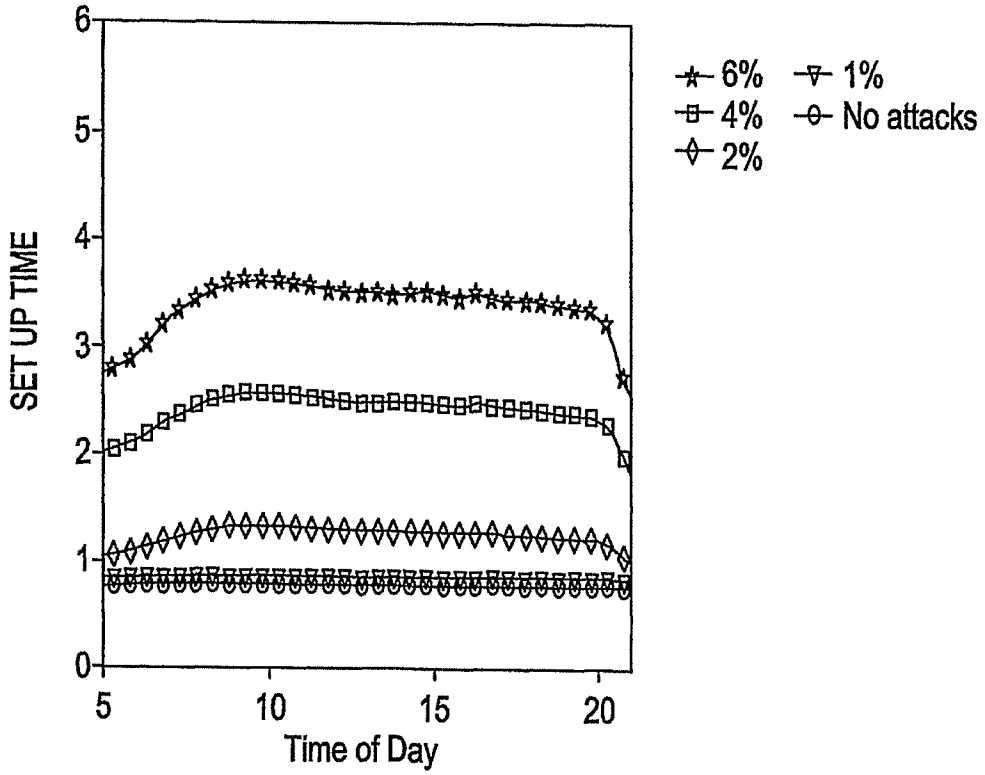

6
5
4
3
2
1
0
SET UP TIME
5
10
15
20
Time of Day
6%
1%
4%
No attacks
2%

FIG. 4

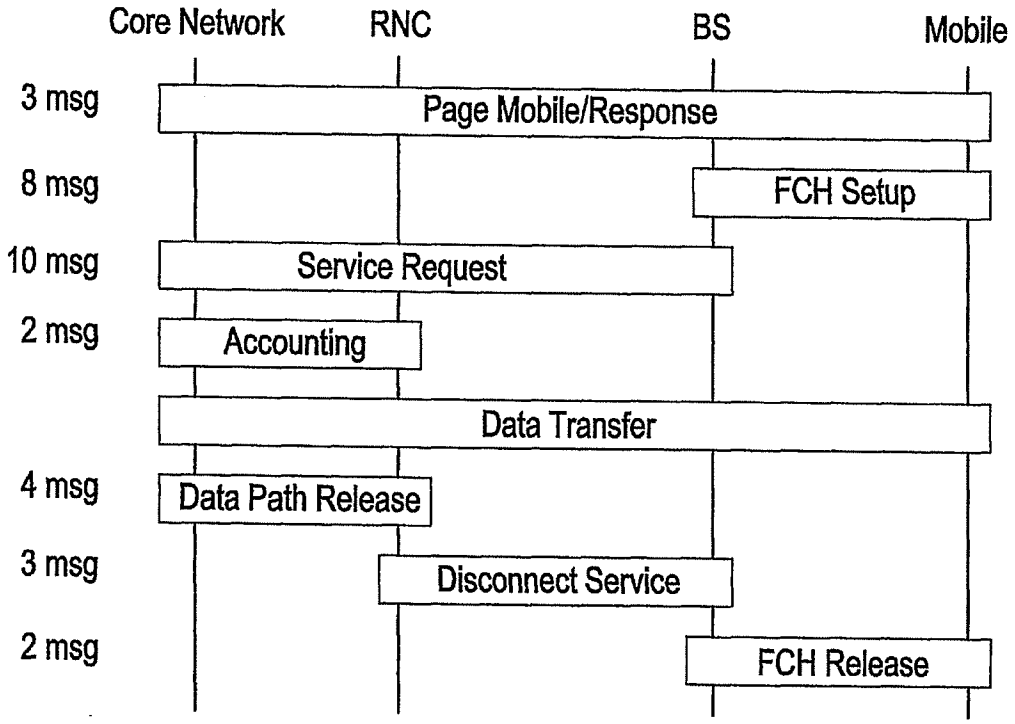

Core Network
RNC
BS
Mobile
3 msg
Page Mobile/Response
8 msg
FCH Setup
10 msg
Service Request
2 msg
Accounting
Data Transfer
4 msg
Data Path Release
3 msg
Disconnect Service
2 msg
FCH Release

FIG. 5

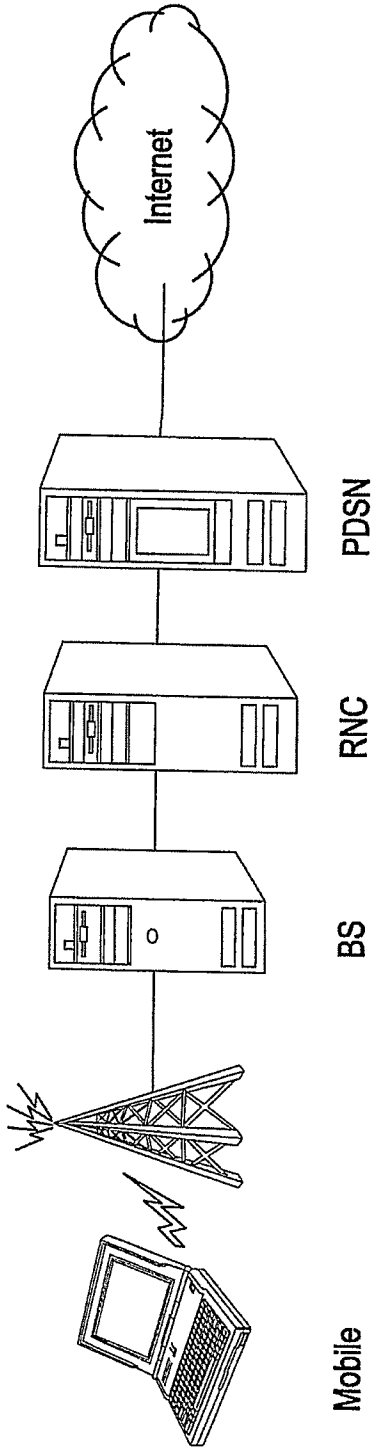
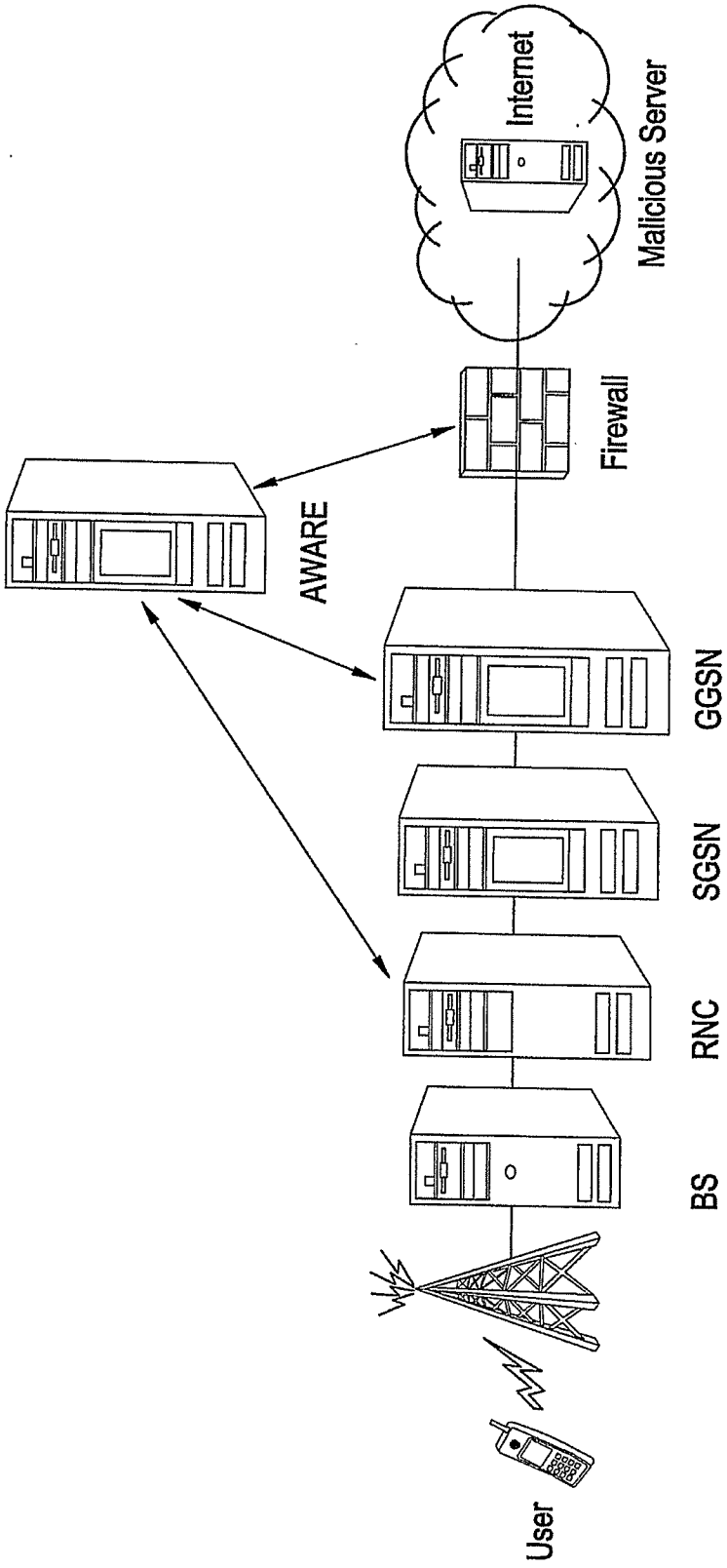


FIG. 6


Internet
Malicious Server
Firewall
AWARE
GGSN
SGSN
RNC
BS
User

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/010108

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, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	YIH HUANG ET AL: "Countering denial-of-service attacks using congestion triggered packet sampling and filtering" COMPUTER COMMUNICATIONS AND NETWORKS, 2001. PROCEEDINGS. TENTH INTERNATIONAL CONFERENCE ON 15-17 OCT. 2001, PISCATAWAY, NJ, USA,IEEE, 15 October 2001 (2001-10-15), pages 490-494, XP010562136 ISBN: 0-7803-7128-3 page 491, left-hand column, last paragraph - page 492, left-hand column, last paragraph figure 2	1-9

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 July 2006	23. 08. 06

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	Bengi-Akyuerek, K

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/010108

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 2003/217283 A1 (HRASTAR SCOTT ET AL) 20 November 2003 (2003-11-20) paragraphs [0068], [0069] paragraphs [0076] - [0090] figures 3,4 -----	1-9

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2006/010108

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-9

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9

Methods and system for cost-ratio based intrusion detection in wireless networks.

---

2. claim: 10

Apparatus for generic threshold-based intrusion detection in wireless networks.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/010108

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003217283 A1	20-11-2003	NONE	

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: TBA**
Serial No.: TBA	)	**Art Unit: TBA**
Filed: May 21, 2015	)	**Confirmation No.: TBA**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

PRELIMINARY AMENDMENT

Please enter the following amendment prior to examination on the merits. The Patent Office is authorized and requested to charge all fees to deposit account 13-2490.

Amendments to the Specification begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendment to the Specification

Please insert the following at page 1, line 1 of the specification:

CROSS REFERENCE TO RELATED APPLICATIONS

The present application is a national stage entry of, and claims priority to, PCT/EP2013/074440, filed on November 22, 2013, which claims priority to European Patent Application EP 12193884.9, filed in the European Patent Office on November 22, 2012, both of which are hereby incorporated in their entirety herein by reference.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

No new matter has been introduced into the present application as a result of the above amendment.

Prompt consideration and entry of this amendment prior to examination is respectfully requested. If there are any questions or comments regarding this amendment or application, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,

McDonnell Boehnen
Hulbert & Berghoff LLP

Date: May 21, 2015

By: / David A. Grabelsky /
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	System to Detect Behaviour in a Telecommunication Network
First Named Inventor/Applicant Name:	David A. Grabelsky
Filer:	David A. Grabelsky/Holly Mueller
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
National Stage Fee	1631	1	280	280
Natl Stage Search Fee - Report provided	1642	1	480	480
National Stage Exam - all other cases	1633	1	720	720
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1480**

Electronic Acknowledgement Receipt

EFS ID:	22412153
Application Number:	14646554
International Application Number:	PCT/EP2013/074440
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunication Network
First Named Inventor/Applicant Name:	David A. Grabelsky
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	21-MAY-2015
Filing Date:	
Time Stamp:	15:24:57
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1480
RAM confirmation Number	1731
Deposit Account	132490
Authorized User	GRABELSKY, DAVID ANDREW

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	15_686_WO_US_Transmittal.pdf	218475 85bccb83214d074ac51c14a0fe47147b81c17307	no	4
Warnings:					
Information:					
2	Application Data Sheet	15_686_WO_US_ADS.pdf	1819281 f6bfa088a195855af282324aad233ec6e58e99d1	no	8
Warnings:					
Information:					
3	Documents submitted with 371 Applications	PCTEP2013074440.pdf	836641 82bf896b92aac1e39043231c8a5ab168bcbb5eef	no	21
Warnings:					
Information:					
4	Documents submitted with 371 Applications	15_686_WO_US_SearchReport.pdf	117477 fdb661e7b8b9cdc0e4ee59c2e43c0d11e5c615d7	no	4
Warnings:					
Information:					
5	Documents submitted with 371 Applications	PCTIB304.pdf	69290 75fe0aa31dd76d8f9da344317c5e900d1c5a1a89	no	1
Warnings:					
Information:					
6	Documents submitted with 371 Applications	PCTIB308.pdf	66259 8914d36fa051c74e2eed3d56e933615656179253	no	1
Warnings:					
Information:					
7	Documents submitted with 371 Applications	PCTIB306.pdf	61914 d4835ac769d9792d8b9ec514af27b4178f58e90b	no	1
Warnings:					
Information:					

8	Oath or Declaration filed	15_686_WO_US_Declaration.pdf	149503 7cac6cf102302660202aa8f364f5b6e3bb287b88	no	2
Warnings:					
Information:					
9	Information Disclosure Statement (IDS) Form (SB08)	15_686_WO_US_IDS.pdf	612801 83c4f8db5c1b8d0cd9e37d83ef8f78b1c8b2fa2f	no	4
Warnings:					
Information:					
10	Foreign Reference	EP2139279A1.pdf	15157551 cb6ddd90f87fe2f55a70d2490934c98ab2d5e05f	no	14
Warnings:					
Information:					
11	Foreign Reference	WO9833340A2.pdf	1616535 a89d9bd3ef1e9c96c6c5c302e1663f151df9ccda	no	37
Warnings:					
Information:					
12	Foreign Reference	WO9833340A3.pdf	3537914 6d32166cdfbbd54c288a9a85c97babd1f69ad439	no	4
Warnings:					
Information:					
13	Foreign Reference	WO2006104752.pdf	1429970 ddd65094bec8f15d751029393a4c2e1c40c0cfb4	no	34
Warnings:					
Information:					
14	Non Patent Literature	NPL_1.pdf	274482 8fbce101bbd015f68283a69fd036215c77f1008e	no	7
Warnings:					
Information:					
15	Non Patent Literature	NPL_2.pdf	638442 6fdb3c3fd2da4f2e3cde7da94d1a43b0483d1a07	no	12
Warnings:					
Information:					
16	Non Patent Literature	NPL_3.pdf	117477 3a3f11331e86ef67ba609de65c68c4b6ebbd9285	no	4
Warnings:					
Information:					

17		15_686_WO_US_PreliminaryAmendment.pdf	110071 9fdbfeb4e1e70777eeb7e989bf82572ab0e52733	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	3

Warnings:

Information:

18	Fee Worksheet (SB06)	fee-info.pdf	35499 fc1f25098fa8bae309339cf148bd1deae7b69811	no	2

Warnings:

Information:

Total Files Size (in bytes):	26869582

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung	Certificate	Attestation
Die angehefteten Unterlagen stimmen mit der als ursprünglich eingereicht geltenden Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	The attached documents are exact copies of the text in which the European patent application described on the following page is deemed to have been filed.	Les documents joints à la présente attestation sont conformes au texte, considéré comme initialement déposé, de la demande de brevet européen qui est spécifiée à la page suivante.

Patentanmeldung Nr.	**Patent application No.**	**Demande de brevet n°**
	12193884.9 / EP12193884	

The organization code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP12193884.

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le President de l'Office européen des brevets
p.o.

U. Ingmann

Anmeldung Nr:
Application no.: 12193884.9
Demande no :

Anmeldetag:
Date of filing: 22.11.12
Date de dépôt :

Anmelder / Applicant(s) / Demandeur(s):

Koninklijke KPN N.V.
Maanplein 55
2516 CK The Hague/NL

Nederlandse Organisatie voor Toegepast
-Natuurwetenschappelijk Onderzoek TNO
Schoemakerstraat 97
2628 VK Delft/NL

Bezeichnung der Erfindung / Title of the invention / Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, oder falls die Anmeldung in einer Nicht-Amtssprache des EPA eingereicht wurde, siehe Beschreibung bezüglich ursprünglicher Bezeichnung.
If no title is shown, or if the application has been filed in a non-EPO language, please refer to the description for the original title.
Si aucun titre n'est indiqué, ou si la demande a été déposée dans une langue autre qu'une langue officielle de l'OEB, se référer à la description pour le titre original.)

System to detect behaviour in a telecommunications network

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Am Anmeldetag benannte Vertragstaaten / Contracting States designated at date of filing / Etats contractants désignées lors du dépôt:

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

System to detect behaviour in a telecommunications network

FIELD OF INVENTION

The invention relates to a system for detecting behaviour of a mobile telecommunications device in a telecommunications network, and further relates to a device for detecting behaviour of a mobile telecommunications device within a telecommunications network.

Telecommunications networks provide radio telecommunication to users of mobile devices, typically according to agreed and standardised radio protocols, for example GSM, UTMS and LTE as would be known by the skilled person.

Mobile telecommunications devices are common and include mobile phones and in particular smartphones, tablet devices and other handheld computer devices, handheld personal assistants, and even communication devices situated in vehicles. All can provide users with telecommunication with each other and with access to the internet while moving around.

Access to the internet exposes devices to malware and malicious applications that may be downloaded, accidentally or otherwise, onto the mobile device from the internet. Typically, and often because of their smaller size and memory capacity, mobile telecommunications devices do not contain security features which are as stringent as those available for desk computers and other large devices with internet access. As such, these smaller mobile telecommunications devices are vulnerable to infection and attack by malware and malicious applications, which will typically infect the application processor of a mobile device. But because mobile telecommunications devices are also typically in direct contact with a radio telecommunications network the telecommunications network itself is vulnerable to attack from any malware or malicious applications residing on the mobile devices.

Existing methods to detect malicious mobile device behaviour are applied entirely within the mobile handset itself. For example, “Taming Mr Hayes: Mitigating signaling based attacks on smartphones”, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), 2012, dsn, pp. 1-12, Collin Mulliner, Steffen Liebergeld, Matthias Lange, Jean-Pierre Seifert, describes a method of detecting malicious behaviour within the application processor of a mobile phone and proposes a virtual partition of the application processor as part of the solution.

However a disadvantage of this method is that if the mobile device has been infected with malware there can be no real certainty that the detection method itself can be trusted.

Similarly, US 2006/0288407 describes a method to perform detection on a mobile handset and therefore also results in a similar disadvantage.

Nevertheless, it is a problem to correctly identify the existence of malware or malicious software on a mobile device because only once an infected device has been correctly identified can appropriate action be taken.

DESCRIPTION OF THE INVENTION

The problem is solved according to the invention as described in the claims.

The claims describe a system for detecting behaviour of a mobile telecommunications device in a telecommunications network. The system includes a telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and further to process the signals into data streams. The data streams include data of a first type arranged to cause an event of a first type within the telecommunications network. The network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

The system as claimed solves the problem by identifying malicious behaviour in a mobile device, but identifying it from within the telecommunications network itself. This is done according to the arrangement of the invention by monitoring the data streams, or transfers of data, which occur in the network due to the interaction between the network and the mobile. This data is monitored for excessive occurrences of particular signals.

Malware resident on a mobile device may cause that device to indulge in malicious behaviour, which is typically anything that uses up network resources without being for an express user intention. Typically it is anything which uses up network resources but without resulting in a benefit for the user or for the device. For example, a user of a mobile device may wish to download a video to watch on the device. This will use up resources but the use of resources in this case is time limited and in any event, once the video is downloaded the user spends time watching the video and while doing so is unlikely to download other videos or perform other tasks. Malware, however, may be programmed to download videos continuously, and this uses excessive network resources.

In an alternative example, malware may be programmed to continuously perform attach and detach of the mobile device onto the network. This will use excessive network resources because the network will try to authenticate the mobile device every time the device attaches. The continuous attach and detach however does not result in an advantage for either the user or the mobile device.

In an alternative example, malware may be programmed to manipulate signal level reports used by the network for handover decisions. The mobile device continuously measures the signal levels from base stations in the surrounding cells and reports the signal levels to the network. The network uses this, and other information, to device whether or not to handover the communication with the mobile

device to a different base station than the one that is currently serving the mobile device. Malware could be programmed to manipulate the measurement reports in such a way that a very large number of handovers takes place, which uses excessive network resources.

In an alternative example the malware may be programmed to force the mobile device which carries the malware to continuously request call forwarding. When a request for call forwarding is made the device requests the network to forward incoming calls to a second number. The continuous making of this request will use up network resources.

In an alternative example the malware may constantly request the setting up of bearers, and in particular new bearers, between the device and the network. Again, this uses up network resources.

In an alternative example the malware may force the mobile device which carries the malware to continuously make requests for service without using the proffered services. These requests may be for any kind of service typically provided by the telecommunications network but it wastes network resources when the continuous requests for service do not result in a provided service which benefits either the user or the mobile device making the request.

In all these examples an exchange of data occurs between the mobile device and the telecommunications network but also further within the telecommunications network itself. As is known by the skilled person, when the mobile device transmits signals to the telecommunications network they are received in a base station and processed into data streams internal to the telecommunications network. For example, if an attach request is made by a mobile device then the telecommunication network which receives the attach request makes an attempt to authenticate the mobile device. This results in data streams, or signals, being sent between, for example in the case of a UMTS network, the radio network controller RNC, the mobile switching centre MSC, the Home Location Register HLR, and the Authentication Centre AuC, as would be known by the skilled person. As would also be known by the skilled person, other malicious behaviours described would also result in signalling, or data streams, transmitted not just between the device and the network but also within the network itself.

The network can therefore detect malicious behaviour by monitoring the occurrence in the data streams in the network of data of a first type, typically a predetermined type which represents some interaction in the network between network devices for the normal processing of signals. Further the network registers when this occurrence exceeds a level which indicates acceptable behaviour of the mobile telecommunications device in the telecommunications network. In other words, the network detects malicious behaviour by monitoring for, and detecting, the incidence of various types of data steams within the network itself and registering when the occurrence is too high.

For example, in order to detect the malicious behaviour in which a device continuously attempts to attach and detach the network may count the number of times the Mobile Switching Centre, MSC, is caused to request authentication of the device at the Authentication Centre AuC, or alternatively count the number of times the Authentication Centre AuC signals back a reply.

In a particularly advantageous embodiment the detection of data steams is performed in the core network, and in particular in the Mobility Management Entity MME if the network is an LTE network, in the MSC if it is a UMTS or GSM network or the Serving Gateway Support Node SGSN in a GPRS network. In this embodiment the incidence of particular, or predetermined, data streams can be identified in a central location within each respective network. This has the advantage that it reduces the time it takes for the telecommunications network to identify mobile devices which may be infected by malware.

However the occurrence of specific data streams may be detected further back in the network. In an example of this, excessive attach requests may be detected at the AuC by detecting authentication attempts per mobile device. Alternatively, excessive attach requests may be detected by counting at the HLR the number of times the network requests data regarding a particular mobile device.

In certain embodiments detection could be performed in the eNodeB or base station. This has the advantage that detection of malicious behaviour uses fewer network resources. For example, excessive numbers of attach and detach could be detected in the receiving base station. However, a particular disadvantage of performing detection at the base station, for example, occurs when signals from the mobile device arrive in the network through different base stations, and one example of this is when a device is physically moving quickly across base station cells. In such a case no one particular base station, or eNodeB, will necessarily receive the full signalling from the device and therefore no one base station will be able to unambiguously perform detection.

In a particularly advantageous embodiment the network counts the occurrence of particular data signals when their rate of occurrence exceeds a predetermined temporal rate. For example, if the network is monitoring for the sending of an authentication request to the AuC, the network is arranged to detect when the rate of transmission of authentication requests for a particular mobile exceeds a predetermined threshold and also to count the number of times authentication is then requested, while the rate of authentication requests exceeds the predetermined rate.

In other words the network monitors for, and detects when the frequency of a certain predetermined signal or data occurrence in the data streams becomes too high. The network then proceeds to count the number of occurrences while the rate remains above the predetermined temporal rate.

This particular embodiment is even more advantageous if the network is further arranged to register when the number of detected occurrences itself exceeds a predetermined threshold. In our example

this would mean that the network registers when the number of authentication requests exceeds a certain number, with each authentication request having been received at a rate which is greater than the predetermined temporal rate.

In a further advantageous embodiment, the network can detect if the rate of occurrence of a signal or data event, for example a request for authentication transmitted to the AuC, occurs at or above a predetermined temporal rate by measuring the time elapsed between successive occurrences. In this embodiment the network is arranged to detect the time elapsed between two consecutive authentication requests to the AuC, in our example, and calculate when this elapsed time is less than a predetermined time interval. The data occurrences are deemed to occur at a rate which exceeds the predetermined rate when they occur within the respective predetermined time interval.

In a particularly advantageous example the network includes a counter, C, and is arranged to detect a detectable event, X, which occurs within the network, for example the first instance of an attach, or, the transmission of a request for authentication to the AuC, or, the arrival of signaling in the MME indicating that a handover has taken place, and starts the counter.

The counter then becomes: C=1

At the same time the network starts a timer. The counter is stored and associated with the mobile device.

If the next detection of X in the network takes place within a predetermined time interval then the counter becomes: C=2

In an embodiment the timer measures a time t from the first detection of X and in this case the counter is incremented by 1 if the next detection occurs at a time, $t < \Delta$, where Δ is the predetermined time interval. In an alternative embodiment the time at each detection of the event X is registered, the time of the first event, ST, being stored and associated with the mobile device. A timer, T, is started at ST and the counter is incremented if the time of the next detected event X is t where:

$$t<ST + \Delta$$

Within this embodiment the value of ST is then replaced by the new time NT at which the second event X was detected.

In both embodiments the counter is incremented again if the following detection of X occurs within the same time interval. In such a case the counter would now register:

C=3

If the counter reaches a predetermined threshold, say C_n, in which case the counter becomes:

$$C=C_n$$

the telecommunications network registers the fact. This may be done by setting a flag, but the skilled person knows that there are alternative methods of registering.

In an alternative embodiment the network registers if the counter exceeds a predetermined threshold.

If X is not detected again within the predetermined time interval, the counter goes back to zero.

In an alternative embodiment the network could monitor and count the number of detachments of a particular mobile device.

In an embodiment in which handover is detected, the following further embodiment is particularly advantageous. The network maintains a record of the tracking area of the mobile device and also an indication of when the tracking area changes. This allows the network to know when the device is moving. If the network registers an excessive number of handovers the tracking area information can be used to discount excessive handovers when the device is actually in physically rapid movement.

In a further embodiment the network registers when a device switches frequently between neighbouring bases stations. This is an indication of genuine mala fide behaviour as normally such switches are suppressed by existing handover algorithms to avoid excessive handover of a mobile device that is actually physically situated on the border between two cells.

In an alternative, and particularly advantageous embodiment, the network monitors improbable service request combinations. For example, it is unlikely that a user would request the streaming of five movie downloads in parallel. Equally unlikely is that the user would genuinely attempt to listen to his own voice mail while making a telephone call. Such examples of unlikely behaviour can be determined and monitored for by the network.

Following detection of malicious behaviour the network can perform several actions. These include: detaching the mobile device; sending a signal to the device to permanently block access to the network; starting a back off timer to stop the mobile device from making another connection request within a certain time period; send a warning message to the owner of the device. In the last example the warning could be transmitted to the mobile device itself, via sms for example, however if the device is infected by malware and cannot be trusted then the network cannot assume any warning message transmitted to the device itself will be seen or heard by the user. Therefore a warning could

be transmitted to the user via other channels relying on other data stored for the user, for example by email to a known email address.

In a further advantageous embodiment the network tracks the behaviour of several devices and aggregates the results. In this way malware behaviour can be tracked and monitored across an entire network.

In a further advantageous embodiment the network monitors for the occurrence of data of a second type in the data streams. Typically the data streams that are passed around the network include more than one type of data and in addition to including data of a first type arranged to cause an event of a first type within the telecommunications network, may include data of a second type arranged to cause an event of a second type with the telecommunications network. In a particularly advantageous embodiment the network may monitor for malicious behaviour of a mobile device by monitoring for the occurrence of both data of the first and second type, determining when each exceeds some predetermined threshold. In this case each can exceed a predetermined threshold individually, and the predetermined thresholds can be different or be the same, or, both occurrences can be aggregated and can be compared to a single predetermined threshold together. In an example the network could monitor for data occurrences in the network indicating device attach, as has already been described, but additionally monitor for data occurrences indicating device detach, and only if both occurrences exceed independent predetermined thresholds does the network register that malicious behaviour is occurring. This double measurement, although using extra network resources by effectively counting device behaviour twice, provides the network with a failsafe against accidental registers of malicious continuous attachment due to extraneous other factors within the network, such as error.

In an alternative embodiment, the network could count the occurrence of data of a first type indicating handover, and also count the occurrence of data of a second type indicating change of tracking area.

Further embodiments of the invention are described in the Figures.

Figure 1 shows a telecommunication network in which the invention can be advantageously used.

Figure 2 shows a flow diagram of an embodiment of the invention.

Figure 3 shows a flow diagram of an embodiment of the invention.

Fig. 1 shows a telecommunications network in which the invention can be used. As is known by the skilled person there are multiple technologies described by various telecommunication standards that define telecommunications systems. Typically they include the following layout though the skilled person knows and appreciates that there may be small variations and differences in the way systems work.

A telecommunications network includes a transmitter 101. This is usually called a base station, cell tower, or, in an LTE network an eNodeB. The transmitter is controlled by a base station controller 102, though in, for example, a UMTS network this would be a Radio Network Controller 102 and in, for example, an LTE network the control functions of the base station controller 102 may be subsumed into the eNodeB. Radio signals from hand held mobile devices are received at the transmitter 101, processed into signals and transmitted to the core network.

In the case of a GSM or 2G network the signals are passed to a Mobile Switching Centre, MSC, 103, which routes calls. Upon first receiving signal from a mobile it will query the Home Location Register, HLR, 104, which holds data on mobile subscribers to verify if the signal received is from a mobile device which is subscribed to the network. In order to authenticate the mobile device it will use keys held in the Authentication Centre, AuC, 105.

In the case of a UTMS or 3G network the verified and authenticated signals may be routed through a Gateway Support Node106.

In the case of an LTE or 4G network the signals are passed to a Mobility Management Entity, MME, 103 and the mobile is verified and authenticated at the Home Subscriber Server, HSS, 104/105. Calls are then further routed through a Serving Gateway 106 to a further network 107 which may be the internet.

Fig. 2 shows a flow diagram of an embodiment of the invention suitable for detecting excessive attaches of a mobile device to a telecommunications network. In an advantageous embodiment a device attaches 201 to the network at time t_1 through a base station and the network registers the attach, identifies the mobile device and begins authentication procedures. In parallel with the normal processing of the attach request the network performs the following steps. A counter NA, a start time STA and a timer are initiated 202. Typically the counter will be set to zero and in an advantageous embodiment the timer set to time t_1 registered by the network. The counter value and start time are stored 203 for future reference. The next time an attach is registered for the same device, say at time t_2 the elapsed time T, equal to : $t_2 - STA$

is compared with a predetermined time interval ΔA 204.

If : $T = \Delta A$, or, $T > \Delta A$,

the counter NA and the timer are cleared, 202.

If : $T < \Delta A$,

the counter NA is increased by a value of 1 and the value of STA is replaced by the time t_2, 205. NA and STA are again stored 208. In this case the counter value is further compared with a predetermined threshold, LimitA, 206.

If : NA = LimitA,

an alert is set. If not, the method returns to step 204.

The skilled person will understand there are minor variations which can be made to the embodiment which will still work. For example, the counter could be increased if T is less than or equal to ΔA and only cleared if T is greater than ΔA. Also for example, LimitA could be a value which must be exceeded, in which case an alert flag would be set if NA > LimitA. In another advantageous embodiment a counter could be decremented instead of clearing the counter NA in step 202 if the value of the counter is larger than 0.

As the skilled person will understand, appropriate values for LimitA and the predetermined time interval ΔA will vary depending on the network and the customer base. However, suitable values are ΔA = 500ms and LimitA = 10.

The method as described allows a network to detect malicious behaviour in the form of excessive attach requests from an infected mobile and in an advantageous embodiment would be performed in the MSC, Serving Gateway or MME of the network, as appropriate.

Fig. 3 shows a flow diagram of an embodiment of the invention suitable for detecting excessive handovers of a mobile device in a telecommunications network and in a particularly advantageous embodiment would be performed in the MME of the network, which is informed of handovers before the handover takes place, referred to as an S1-handover, or after the handover has occurred, referred to as an X2-handover.

In order to carry out the method the MME performs the following steps for a group of mobile devices in its area. The group of devices monitored could be the group consisting of all mobile devices in its area, but could also be a sub-group of this group or some other further defined group. For example, the group of mobiles which are monitored could consist, say, of all new mobiles, or of mobiles whose previous activity suggests they might be at risk of infection, for example if they make frequent download requests, or of mobiles which are registered to particular users, says users who frequently change mobiles.

In this advantageous embodiment a device attaches 301 to the network at time t_1 through a base station and the network registers the attach, identifies the mobile device and begins authentication procedures. In parallel with the normal processing of the attach request the network performs the

following steps. A counter NH, a start time STH and a timer are initiated 302. Typically the counter will be set to zero and in an advantageous embodiment the timer set to time t_1 registered by the network. The counter value and start time are stored 303 for future reference. The next time an attach is registered by the same device, say at time t_2 the elapsed time T, equal to :

$$t_2 - STH$$

is compared to a predetermined time interval ΔH 304.

If : $T = \Delta H$, or, $T > \Delta H$,

the counter NH and the timer are cleared, 305.

If : $T < \Delta H$,

the counter NH is increased by a value of 1 and the value of STH is replaced by the time t_2, 305. NH and STH are again stored 308. In this case the counter value is further compared with a predetermined threshold, LimitH, 306.

If : $NH = LimitH$,

an alert is set. If not, the method returns to step 304.

Again, the skilled person will understand there are minor variations which can be made to the embodiment which will still work. For example, the counter could be increased if T is less than or equal to ΔA and only cleared if T is greater than ΔA. Also for example, LimitH could be a value which must be exceeded, in which case an alert flag would be set if NH > LimitH.

The particular advantages of the invention are that a telecommunications network can monitor for malicious activity in mobile devices and identify when a particular device is potentially infected by malware. Although use of the invention requires network resources that would otherwise not be expended, it allows the easy identification of devices which may use up far greater network resources if left unidentified.

As the skilled person will understand, appropriate values for LimitH and the predetermined time interval ΔH will vary depending on the network and the customer base. However, suitable values are ΔH = 2s and LimitH = 20.

Claims

1 A system for detecting behaviour of a mobile telecommunications device in a telecommunications network,

the system comprising:

a telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and further to process the signals into data streams,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,

characterised in that,

the network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

2 The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence of data of the first type by counting the number of times data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3 The system according to claim 2 wherein the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4 The system according to claim 3 wherein the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if the following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

5 The system according to claim 1 wherein the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate.

6 The system according to claim 5 wherein the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate the rate as the ratio of the counted detection of occurrence of data of the first type to the time as measured by the timer.

7 The system according to claim 1 wherein the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer.

8 The system according to claim 1 wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9 The system according to claim 1 wherein the data of the first type indicates the setting up of a bearer by the mobile telecommunications device.

10 The system according to claim 1 wherein the data of the first signal type indicate handover of the mobile telecommunications device.

11 The system according to claim 10 wherein the telecommunications network is further arranged to monitor the tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12 The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the MME or SGSN or MSC of the telecommunications network.

13 The system according to claim 1 wherein the a telecommunications network is further configured to

- identify at least one additional mobile telecommunications device,

- to receive signals from the at least one additional device and to process these signals into additional data streams,

- to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14 Device for detecting behaviour of a mobile telecommunications device arranged to transmit signals to a telecommunications network and wherein the signals are processed into data streams within the telecommunications network, and further wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,

wherein the device is:

arranged to be coupled to the telecommunications network and arranged to receive the data streams and further wherein the device is arranged to monitor an occurrence in the data streams of the data of the first type and arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network.

15 A device according to claim 14 wherein the device is further arranged to operate within a MME or SGSN or MSC.

Abstract

A system is provided for detecting behaviour of a mobile telecommunications device in a telecommunications network. Malware in mobile devices can cause malicious behaviour in the device, for example sequential attaching and detaching of an infected device relative to a telecommunications network. A telecommunications network is provided which is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and process the signals into data streams. The data streams include data of a first type arranged to cause an event of a first type within the telecommunications network. The network is arranged to monitor an occurrence in the data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network. A device for detection of mobile device behaviour is also described.

Fig. 1

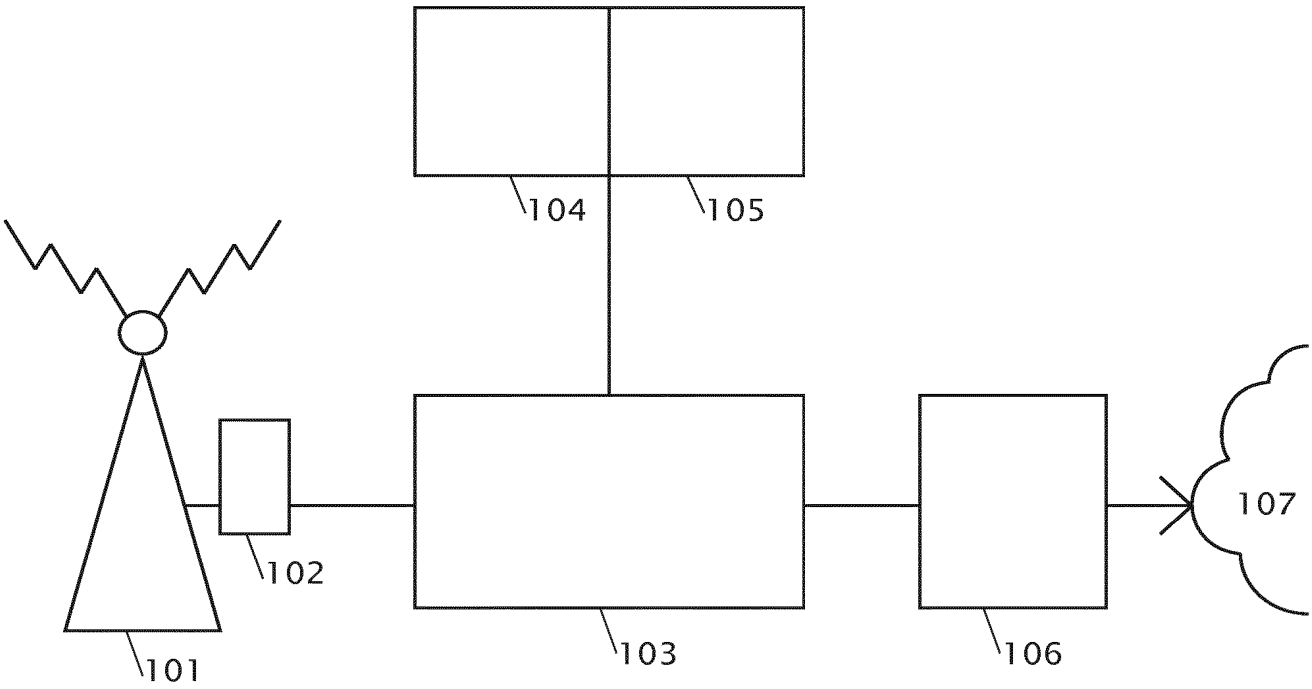


Figure 1

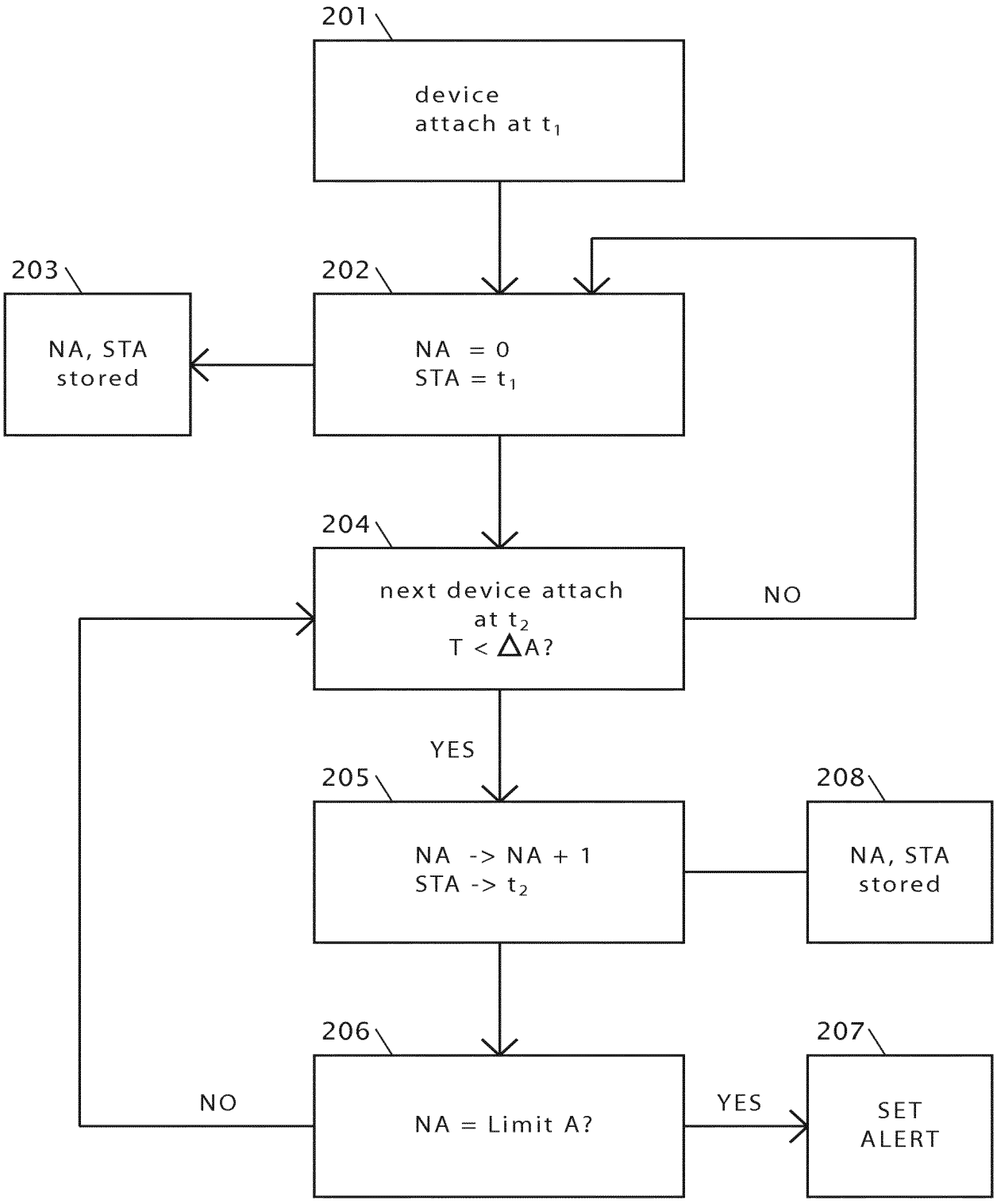

201
device
attach at t_1
202
NA = 0
STA = t_1
203
NA, STA
stored
204
next device attach
at t_2
$T < \Delta A$?
NO
YES
205
NA -> NA + 1
STA -> t_2
208
NA, STA
stored
206
NA = Limit A?
NO
YES
207
SET
ALERT

Figure 2

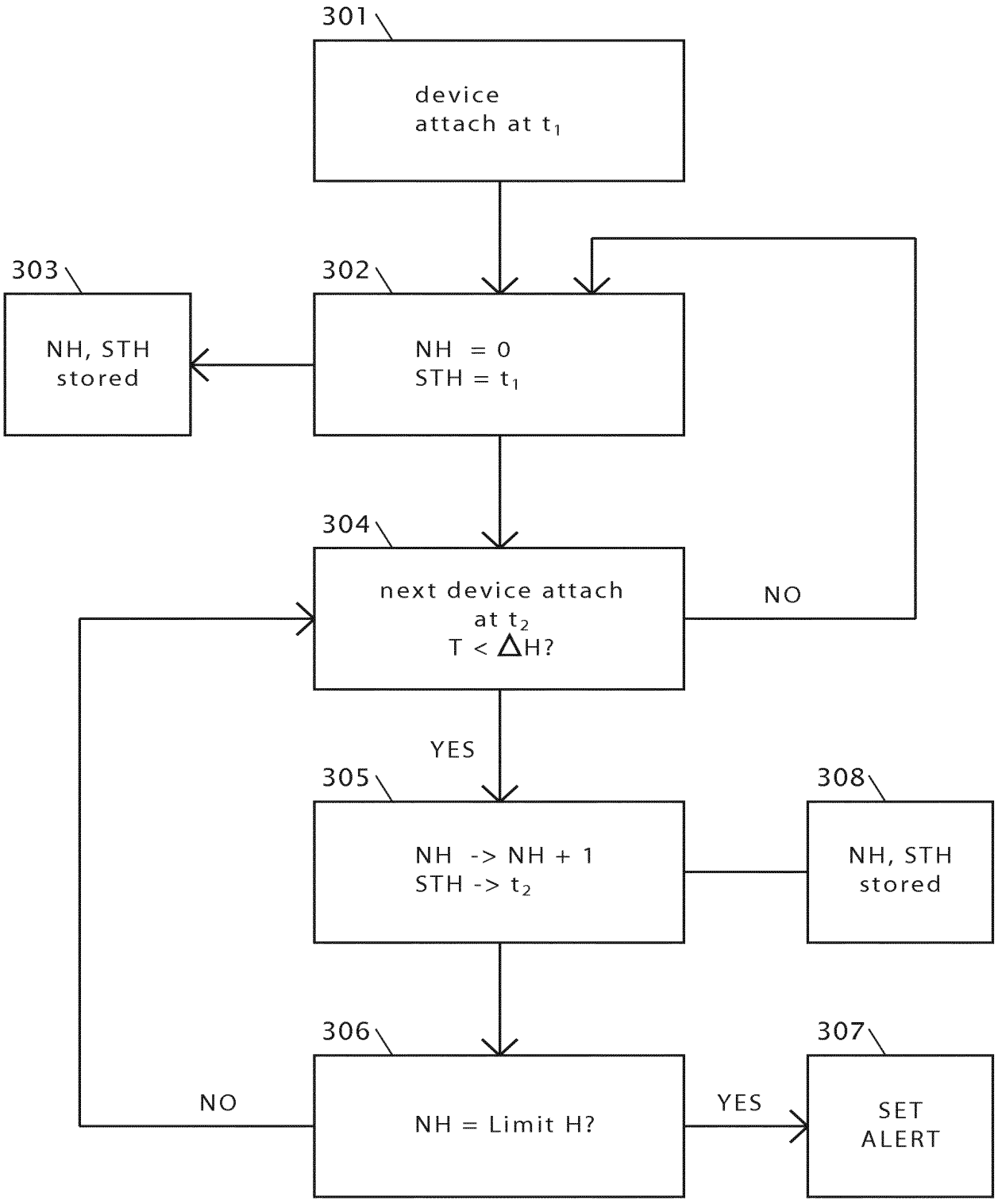

301
device
attach at t_1
303
NH, STH
stored
302
NH = 0
STH = t_1
304
next device attach
at t_2
$T < \Delta H$?
NO
YES
305
NH -> NH + 1
STH -> t_2
308
NH, STH
stored
306
NH = Limit H?
NO
YES
307
SET
ALERT

Figure 3

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/EP2013/074440**
International filing date:		**22 November 2013 (22.11.2013)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**EP**
	Number:	**12193884.9**
	Filing date:	**22 November 2012 (22.11.2012)**
Date of receipt at the International Bureau:		**06 January 2014 (06.01.2014)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

PCT REQUEST

Print Out (Original in Electronic Form)

0	**For receiving Office use only**	
0-1	International Application No.	**PCT/EP2013/074440**
0-2	International Filing Date	**22 NOV 2013 (22.11.2013)**
0-3	Name of receiving Office and "PCT International Application"	**RO/EP**

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT Online Filing Version 3.5.000.235 MT/FOP 20020701/0.20.5.20
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	European Patent Office (EPO) (RO/EP)
0-7	**Applicant's or agent's file reference**	403693WO
I	**Title of Invention**	SYSTEM TO DETECT BEHAVIOUR IN A TELECOM-MUNICATIONS NETWORK
II	**Applicant**	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	KONINKLIJKE KPN N.V.
II-5	Address	Maanplein 55 2516 CK The Hague Netherlands
II-6	State of nationality	NL
II-7	State of residence	NL
II-8	Telephone No.	+31 70 343 39 55
II-9	Facsimile No.	+31 70 385 54 37
II-10	e-mail	dieneke.vandertoorn-dejager@kpn.com
III-1	**Applicant and/or inventor**	
III-1-1	This person is	Applicant only
III-1-2	Applicant for	All designated States
III-1-4	Name	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO
III-1-5	Address	Schoemakerstraat 97 2628 VK Delft Netherlands
III-1-6	State of nationality	NL
III-1-7	State of residence	NL

PCT REQUEST

Print Out (Original in Electronic Form)

III-2	**Applicant and/or inventor**	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	
III-2-4	Name (LAST, First)	MULLER, Frank
III-2-5	Address	Hopstraat 59 2611 TB Delft Netherlands
IV-1	**Agent or common representative; or address for correspondence**	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name (LAST, First)	WUYTS, Koenraad
IV-1-2	Address	P.O. Box 95321 2509 CH The Hague Netherlands
IV-1-3	Telephone No.	+31 70 343 39 55
IV-1-4	Facsimile No.	+31 70 385 54 37
IV-1-5	e-mail	dieneke.vandertoorn-dejager@kpn.com
V	**DESIGNATIONS**	
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**	
VI-1	**Priority claim of earlier regional application**	
VI-1-1	Filing date	22 November 2012 (22.11.2012)
VI-1-2	Number	12193884.9
VI-1-3	Regional Office	EP
VI-2	**Priority document request**	
	The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1

PCT REQUEST

Print Out (Original in Electronic Form)

VI-3	**Incorporation by reference :** where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.		
VII-1	**International Searching Authority Chosen**	European Patent Office (EPO) (ISA/EP)	
VII-2	**Request to use results of earlier search; reference to that search**		
VII-2-1	Filing date	22 November 2012 (22.11.2012)	
VII-2-2	Application Number	12193884.9	
VII-2-3	Country (or regional Office)	EP	
VII-2-4	Statement (Rule 4.12(ii)):	This international application is the same, or substantially the same, as the application in respect of which the earlier search was carried out except, where applicable, that it is filed in a different language.	
VII-2-5	Documents are available to the ISA in a form and manner acceptable to it and therefore do not need to be submitted by the applicant to the ISA (Rule 12bis.1(f)):	A copy of the results of the earlier search A copy of the earlier application A copy of any document cited in the results of the earlier search	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	–	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	–	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	–	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	1	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	–	

VIII-4-1	**Declaration: Inventorship (only for the purposes of the designation of the United States of America)** Declaration of Inventorship (Rules 4.17(iv) and 51bis.1(a)(iv)) for the purposes of the designation of the United States of America:	**I hereby declare that I believe I am the original inventor or an original joint inventor of a claimed invention in the application.** **This declaration is directed to the international application of which it forms a part.** **I hereby declare that the above-identified international application was made or authorized to be made by me.** **I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.**
VIII-4-1-1-1	Name (LAST, First)	**MULLER, Frank**
VIII-4-1-1-2	Residence: (city and either US state, if applicable, or country)	**Delft, Netherlands**
VIII-4-1-1-3	Mailing Address:	**Hopstraat 59 2611 TB Delft**
VIII-4-1-1-4	Inventor's Signature: (The signature must be that of the inventor, not that of the agent)	**/Frank Muller/**
VIII-4-1-1-5	Date:	**22 November 2013 (22.11.2013)**

PCT REQUEST

Print Out (Original in Electronic Form)

IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	5	✓
IX-2	Description	10	✓
IX-3	Claims	3	✓
IX-4	Abstract	1	✓
IX-5	Drawings	3	✓
IX-7	TOTAL	22	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	–	✓
IX-18	PCT-SAFE physical media	–	–
IX-20	**Figure of the drawings which should accompany the abstract**	1	
IX-21	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	(PKCS7 Digital Signature)	
X-1-1	Name (LAST, First)	WUYTS, Koenraad	
X-1-2	Name of signatory	NL, Koninklijke KPN N.V., K. Wuyts 16870	
X-1-3	Capacity (if such capacity is not obvious from reading the request)	(Representative)	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	22 NOV 2013 (22.11.2013)
10-2	**Drawings:**	✓
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/EP
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92*bis*.1 and Administrative Instructions, Section 422)

To:

WUYTS, Koenraad
Koninklijke KPN N.V.
P.O. Box 95321
NL-2509 CH The Hague
PAYS-BAS

Date of mailing *(day/month/year)*
17 April 2015 (17.04.2015)

Applicant's or agent's file reference
403693WO

IMPORTANT NOTIFICATION

International application No.
PCT/EP2013/074440

International filing date *(day/month/year)*
22 November 2013 (22.11.2013)

1. The following indications appeared on record concerning:

☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative

Name and Address
NEDERLANDSE ORGANISATIE VOOR
TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO
Schoemakerstraat 97
NL-2628 VK Delft
Netherlands

State of Nationality: NL
State of Residence: NL
Telephone No.
Facsimile No.
E-mail address

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address
NEDERLANDSE ORGANISATIE VOOR
TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO
Anna van Buerenplein 1
NL-2595 DA 's-Gravenhage
Netherlands

State of Nationality: NL
State of Residence: NL
Telephone No.
Facsimile No.
E-mail address
☐ Notifications by e-mail authorized

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☐ the Authority(ies) specified for supplementary search
☐ the International Preliminary Examining Authority
☒ the designated Offices concerned
☐ the elected Offices concerned
☐ other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Blanc Veronique
e-mail pt06.pct@wipo.int
Telephone No. +41 22 338 74 06

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2014 (30.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/079960 A1

(51) International Patent Classification:
H04W 24/08 (2009.01) *H04L 29/06* (2006.01)
H04W 28/02 (2009.01)

(21) International Application Number:
PCT/EP2013/074440

(22) International Filing Date:
22 November 2013 (22.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12193884.9 22 November 2012 (22.11.2012) EP

(71) Applicants: **KONINKLIJKE KPN N.V.** [NL/NL]; Maanplein 55, NL-2516 CK The Hague (NL). **NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO** [NL/NL]; Schoemakerstraat 97, NL-2628 VK Delft (NL).

(72) Inventor: **MULLER, Frank**; Hopstraat 59, NL-2611 TB Delft (NL).

(74) Agent: **WUYTS, Koenraad**; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

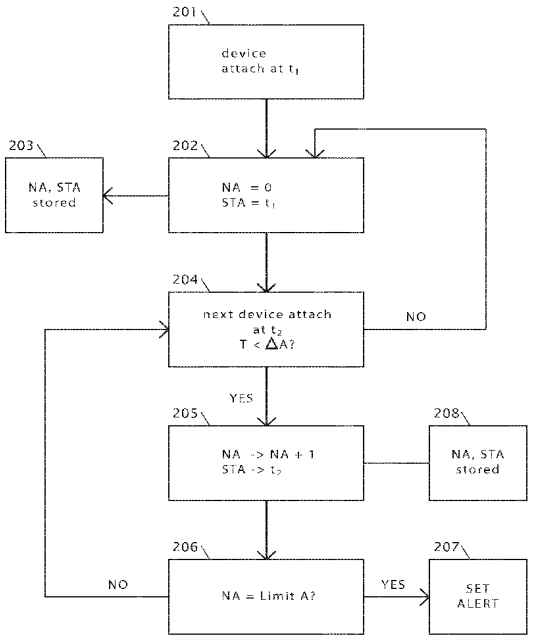


Figure 2

(57) Abstract: A system is provided for detecting behaviour of a mobile telecommunications device in a telecommunications network. Malware in mobile devices can cause malicious behaviour in the device, for example sequential attaching and detaching of an infected device relative to a telecommunications network. A telecommunications network is provided which is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and process the signals into data streams. The data streams include data of a first type arranged to cause an event of a first type within the telecommunications network. The network is arranged to monitor an occurrence in the data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.A device for detection of mobile device behaviour is also described.

WO 2014/079960 A1

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

System to detect behaviour in a telecommunications network

FIELD OF INVENTION

The invention relates to a system for detecting behaviour of a mobile telecommunications device in a telecommunications network, and further relates to a device for detecting behaviour of a mobile telecommunications device within a telecommunications network.

Telecommunications networks provide radio telecommunication to users of mobile devices, typically according to agreed and standardised radio protocols, for example GSM, UTMS and LTE as would be known by the skilled person.

Mobile telecommunications devices are common and include mobile phones and in particular smartphones, tablet devices and other handheld computer devices, handheld personal assistants, and even communication devices situated in vehicles. All can provide users with telecommunication with each other and with access to the internet while moving around.

Access to the internet exposes devices to malware and malicious applications that may be downloaded, accidentally or otherwise, onto the mobile device from the internet. Typically, and often because of their smaller size and memory capacity, mobile telecommunications devices do not contain security features which are as stringent as those available for desk computers and other large devices with internet access. As such, these smaller mobile telecommunications devices are vulnerable to infection and attack by malware and malicious applications, which will typically infect the application processor of a mobile device. But because mobile telecommunications devices are also typically in direct contact with a radio telecommunications network the telecommunications network itself is vulnerable to attack from any malware or malicious applications residing on the mobile devices.

Existing methods to detect malicious mobile device behaviour are applied entirely within the mobile handset itself. For example, “Taming Mr Hayes: Mitigating signaling based attacks on smartphones”, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), 2012, dsn, pp. 1-12, Collin Mulliner, Steffen Liebergeld, Matthias Lange, Jean-Pierre Seifert, describes a method of detecting malicious behaviour within the application processor of a mobile phone and proposes a virtual partition of the application processor as part of the solution.

However a disadvantage of this method is that if the mobile device has been infected with malware there can be no real certainty that the detection method itself can be trusted.

Similarly, US 2006/0288407 describes a method to perform detection on a mobile handset and therefore also results in a similar disadvantage.

Nevertheless, it is a problem to correctly identify the existence of malware or malicious software on a mobile device because only once an infected device has been correctly identified can appropriate action be taken.

DESCRIPTION OF THE INVENTION

The problem is solved according to the invention as described in the claims.

The claims describe a system for detecting behaviour of a mobile telecommunications device in a telecommunications network. The system includes a telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and further to process the signals into data streams. The data streams include data of a first type arranged to cause an event of a first type within the telecommunications network. The network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

The system as claimed solves the problem by identifying malicious behaviour in a mobile device, but identifying it from within the telecommunications network itself. This is done according to the arrangement of the invention by monitoring the data streams, or transfers of data, which occur in the network due to the interaction between the network and the mobile. This data is monitored for excessive occurrences of particular signals.

Malware resident on a mobile device may cause that device to indulge in malicious behaviour, which is typically anything that uses up network resources without being for an express user intention. Typically it is anything which uses up network resources but without resulting in a benefit for the user or for the device. For example, a user of a mobile device may wish to download a video to watch on the device. This will use up resources but the use of resources in this case is time limited and in any event, once the video is downloaded the user spends time watching the video and while doing so is unlikely to download other videos or perform other tasks. Malware, however, may be programmed to download videos continuously, and this uses excessive network resources.

In an alternative example, malware may be programmed to continuously perform attach and detach of the mobile device onto the network. This will use excessive network resources because the network will try to authenticate the mobile device every time the device attaches. The continuous attach and detach however does not result in an advantage for either the user or the mobile device.

In an alternative example, malware may be programmed to manipulate signal level reports used by the network for handover decisions. The mobile device continuously measures the signal levels from base stations in the surrounding cells and reports the signal levels to the network. The network uses this, and other information, to device whether or not to handover the communication with the mobile

device to a different base station than the one that is currently serving the mobile device. Malware could be programmed to manipulate the measurement reports in such a way that a very large number of handovers takes place, which uses excessive network resources.

In an alternative example the malware may be programmed to force the mobile device which carries the malware to continuously request call forwarding. When a request for call forwarding is made the device requests the network to forward incoming calls to a second number. The continuous making of this request will use up network resources.

In an alternative example the malware may constantly request the setting up of bearers, and in particular new bearers, between the device and the network. Again, this uses up network resources.

In an alternative example the malware may force the mobile device which carries the malware to continuously make requests for service without using the proffered services. These requests may be for any kind of service typically provided by the telecommunications network but it wastes network resources when the continuous requests for service do not result in a provided service which benefits either the user or the mobile device making the request.

In all these examples an exchange of data occurs between the mobile device and the telecommunications network but also further within the telecommunications network itself. As is known by the skilled person, when the mobile device transmits signals to the telecommunications network they are received in a base station and processed into data streams internal to the telecommunications network. For example, if an attach request is made by a mobile device then the telecommunication network which receives the attach request makes an attempt to authenticate the mobile device. This results in data streams, or signals, being sent between, for example in the case of a UMTS network, the radio network controller RNC, the mobile switching centre MSC, the Home Location Register HLR, and the Authentication Centre AuC, as would be known by the skilled person. As would also be known by the skilled person, other malicious behaviours described would also result in signalling, or data streams, transmitted not just between the device and the network but also within the network itself.

The network can therefore detect malicious behaviour by monitoring the occurrence in the data streams in the network of data of a first type, typically a predetermined type which represents some interaction in the network between network devices for the normal processing of signals. Further the network registers when this occurrence exceeds a level which indicates acceptable behaviour of the mobile telecommunications device in the telecommunications network. In other words, the network detects malicious behaviour by monitoring for, and detecting, the incidence of various types of data steams within the network itself and registering when the occurrence is too high.

For example, in order to detect the malicious behaviour in which a device continuously attempts to attach and detach the network may count the number of times the Mobile Switching Centre, MSC, is caused to request authentication of the device at the Authentication Centre AuC, or alternatively count the number of times the Authentication Centre AuC signals back a reply.

In a particularly advantageous embodiment the detection of data steams is performed in the core network, and in particular in the Mobility Management Entity MME if the network is an LTE network, in the MSC if it is a UMTS or GSM network or the Serving Gateway Support Node SGSN in a GPRS network. In this embodiment the incidence of particular, or predetermined, data streams can be identified in a central location within each respective network. This has the advantage that it reduces the time it takes for the telecommunications network to identify mobile devices which may be infected by malware.

However the occurrence of specific data streams may be detected further back in the network. In an example of this, excessive attach requests may be detected at the AuC by detecting authentication attempts per mobile device. Alternatively, excessive attach requests may be detected by counting at the HLR the number of times the network requests data regarding a particular mobile device.

In certain embodiments detection could be performed in the eNodeB or base station. This has the advantage that detection of malicious behaviour uses fewer network resources. For example, excessive numbers of attach and detach could be detected in the receiving base station. However, a particular disadvantage of performing detection at the base station, for example, occurs when signals from the mobile device arrive in the network through different base stations, and one example of this is when a device is physically moving quickly across base station cells. In such a case no one particular base station, or eNodeB, will necessarily receive the full signalling from the device and therefore no one base station will be able to unambiguously perform detection.

In a particularly advantageous embodiment the network counts the occurrence of particular data signals when their rate of occurrence exceeds a predetermined temporal rate. For example, if the network is monitoring for the sending of an authentication request to the AuC, the network is arranged to detect when the rate of transmission of authentication requests for a particular mobile exceeds a predetermined threshold and also to count the number of times authentication is then requested, while the rate of authentication requests exceeds the predetermined rate.

In other words the network monitors for, and detects when the frequency of a certain predetermined signal or data occurrence in the data streams becomes too high. The network then proceeds to count the number of occurrences while the rate remains above the predetermined temporal rate.

This particular embodiment is even more advantageous if the network is further arranged to register when the number of detected occurrences itself exceeds a predetermined threshold. In our example

this would mean that the network registers when the number of authentication requests exceeds a certain number, with each authentication request having been received at a rate which is greater than the predetermined temporal rate.

In a further advantageous embodiment, the network can detect if the rate of occurrence of a signal or data event, for example a request for authentication transmitted to the AuC, occurs at or above a predetermined temporal rate by measuring the time elapsed between successive occurrences. In this embodiment the network is arranged to detect the time elapsed between two consecutive authentication requests to the AuC, in our example, and calculate when this elapsed time is less than a predetermined time interval. The data occurrences are deemed to occur at a rate which exceeds the predetermined rate when they occur within the respective predetermined time interval.

In a particularly advantageous example the network includes a counter, C, and is arranged to detect a detectable event, X, which occurs within the network, for example the first instance of an attach, or, the transmission of a request for authentication to the AuC, or, the arrival of signaling in the MME indicating that a handover has taken place, and starts the counter.

The counter then becomes: C=1

At the same time the network starts a timer. The counter is stored and associated with the mobile device.

If the next detection of X in the network takes place within a predetermined time interval then the counter becomes: C=2

In an embodiment the timer measures a time t from the first detection of X and in this case the counter is incremented by 1 if the next detection occurs at a time, $t < \Delta$, where Δ is the predetermined time interval. In an alternative embodiment the time at each detection of the event X is registered, the time of the first event, ST, being stored and associated with the mobile device. A timer, T, is started at ST and the counter is incremented if the time of the next detected event X is t where:

$$t<ST + \Delta$$

Within this embodiment the value of ST is then replaced by the new time NT at which the second event X was detected.

In both embodiments the counter is incremented again if the following detection of X occurs within the same time interval. In such a case the counter would now register:

C=3

If the counter reaches a predetermined threshold, say C_n, in which case the counter becomes:

$$C=C_n$$

the telecommunications network registers the fact. This may be done by setting a flag, but the skilled person knows that there are alternative methods of registering.

In an alternative embodiment the network registers if the counter exceeds a predetermined threshold.

If X is not detected again within the predetermined time interval, the counter goes back to zero.

In an alternative embodiment the network could monitor and count the number of detachments of a particular mobile device.

In an embodiment in which handover is detected, the following further embodiment is particularly advantageous. The network maintains a record of the tracking area of the mobile device and also an indication of when the tracking area changes. This allows the network to know when the device is moving. If the network registers an excessive number of handovers the tracking area information can be used to discount excessive handovers when the device is actually in physically rapid movement.

In a further embodiment the network registers when a device switches frequently between neighbouring bases stations. This is an indication of genuine mala fide behaviour as normally such switches are suppressed by existing handover algorithms to avoid excessive handover of a mobile device that is actually physically situated on the border between two cells.

In an alternative, and particularly advantageous embodiment, the network monitors improbable service request combinations. For example, it is unlikely that a user would request the streaming of five movie downloads in parallel. Equally unlikely is that the user would genuinely attempt to listen to his own voice mail while making a telephone call. Such examples of unlikely behaviour can be determined and monitored for by the network.

Following detection of malicious behaviour the network can perform several actions. These include: detaching the mobile device; sending a signal to the device to permanently block access to the network; starting a back off timer to stop the mobile device from making another connection request within a certain time period; send a warning message to the owner of the device. In the last example the warning could be transmitted to the mobile device itself, via sms for example, however if the device is infected by malware and cannot be trusted then the network cannot assume any warning message transmitted to the device itself will be seen or heard by the user. Therefore a warning could

be transmitted to the user via other channels relying on other data stored for the user, for example by email to a known email address.

In a further advantageous embodiment the network tracks the behaviour of several devices and aggregates the results. In this way malware behaviour can be tracked and monitored across an entire network.

In a further advantageous embodiment the network monitors for the occurrence of data of a second type in the data streams. Typically the data streams that are passed around the network include more than one type of data and in addition to including data of a first type arranged to cause an event of a first type within the telecommunications network, may include data of a second type arranged to cause an event of a second type with the telecommunications network. In a particularly advantageous embodiment the network may monitor for malicious behaviour of a mobile device by monitoring for the occurrence of both data of the first and second type, determining when each exceeds some predetermined threshold. In this case each can exceed a predetermined threshold individually, and the predetermined thresholds can be different or be the same, or, both occurrences can be aggregated and can be compared to a single predetermined threshold together. In an example the network could monitor for data occurrences in the network indicating device attach, as has already been described, but additionally monitor for data occurrences indicating device detach, and only if both occurrences exceed independent predetermined thresholds does the network register that malicious behaviour is occurring. This double measurement, although using extra network resources by effectively counting device behaviour twice, provides the network with a failsafe against accidental registers of malicious continuous attachment due to extraneous other factors within the network, such as error.

In an alternative embodiment, the network could count the occurrence of data of a first type indicating handover, and also count the occurrence of data of a second type indicating change of tracking area.

Further embodiments of the invention are described in the Figures.

Figure 1 shows a telecommunication network in which the invention can be advantageously used.

Figure 2 shows a flow diagram of an embodiment of the invention.

Figure 3 shows a flow diagram of an embodiment of the invention.

Fig. 1 shows a telecommunications network in which the invention can be used. As is known by the skilled person there are multiple technologies described by various telecommunication standards that define telecommunications systems. Typically they include the following layout though the skilled person knows and appreciates that there may be small variations and differences in the way systems work.

A telecommunications network includes a transmitter 101. This is usually called a base station, cell tower, or, in an LTE network an eNodeB. The transmitter is controlled by a base station controller 102, though in, for example, a UMTS network this would be a Radio Network Controller 102 and in, for example, an LTE network the control functions of the base station controller 102 may be subsumed into the eNodeB. Radio signals from hand held mobile devices are received at the transmitter 101, processed into signals and transmitted to the core network.

In the case of a GSM or 2G network the signals are passed to a Mobile Switching Centre, MSC, 103, which routes calls. Upon first receiving signal from a mobile it will query the Home Location Register, HLR, 104, which holds data on mobile subscribers to verify if the signal received is from a mobile device which is subscribed to the network. In order to authenticate the mobile device it will use keys held in the Authentication Centre, AuC, 105.

In the case of a UTMS or 3G network the verified and authenticated signals may be routed through a Gateway Support Node106.

In the case of an LTE or 4G network the signals are passed to a Mobility Management Entity, MME, 103 and the mobile is verified and authenticated at the Home Subscriber Server, HSS, 104/105. Calls are then further routed through a Serving Gateway 106 to a further network 107 which may be the internet.

Fig. 2 shows a flow diagram of an embodiment of the invention suitable for detecting excessive attaches of a mobile device to a telecommunications network. In an advantageous embodiment a device attaches 201 to the network at time t_1 through a base station and the network registers the attach, identifies the mobile device and begins authentication procedures. In parallel with the normal processing of the attach request the network performs the following steps. A counter NA, a start time STA and a timer are initiated 202. Typically the counter will be set to zero and in an advantageous embodiment the timer set to time t_1 registered by the network. The counter value and start time are stored 203 for future reference. The next time an attach is registered for the same device, say at time t_2 the elapsed time T, equal to : $t_2 - STA$

is compared with a predetermined time interval ΔA 204.

If : $T = \Delta A$, or, $T > \Delta A$,

the counter NA and the timer are cleared, 202.

If : $T < \Delta A$,

the counter NA is increased by a value of 1 and the value of STA is replaced by the time t_2, 205. NA and STA are again stored 208. In this case the counter value is further compared with a predetermined threshold, LimitA, 206.

If : NA = LimitA,

an alert is set. If not, the method returns to step 204.

The skilled person will understand there are minor variations which can be made to the embodiment which will still work. For example, the counter could be increased if T is less than or equal to ΔA and only cleared if T is greater than ΔA. Also for example, LimitA could be a value which must be exceeded, in which case an alert flag would be set if NA > LimitA. In another advantageous embodiment a counter could be decremented instead of clearing the counter NA in step 202 if the value of the counter is larger than 0.

As the skilled person will understand, appropriate values for LimitA and the predetermined time interval ΔA will vary depending on the network and the customer base. However, suitable values are ΔA = 500ms and LimitA = 10.

The method as described allows a network to detect malicious behaviour in the form of excessive attach requests from an infected mobile and in an advantageous embodiment would be performed in the MSC, Serving Gateway or MME of the network, as appropriate.

Fig. 3 shows a flow diagram of an embodiment of the invention suitable for detecting excessive handovers of a mobile device in a telecommunications network and in a particularly advantageous embodiment would be performed in the MME of the network, which is informed of handovers before the handover takes place, referred to as an S1-handover, or after the handover has occurred, referred to as an X2-handover.

In order to carry out the method the MME performs the following steps for a group of mobile devices in its area. The group of devices monitored could be the group consisting of all mobile devices in its area, but could also be a sub-group of this group or some other further defined group. For example, the group of mobiles which are monitored could consist, say, of all new mobiles, or of mobiles whose previous activity suggests they might be at risk of infection, for example if they make frequent download requests, or of mobiles which are registered to particular users, says users who frequently change mobiles.

In this advantageous embodiment a device attaches 301 to the network at time t_1 through a base station and the network registers the attach, identifies the mobile device and begins authentication procedures. In parallel with the normal processing of the attach request the network performs the

following steps. A counter NH, a start time STH and a timer are initiated 302. Typically the counter will be set to zero and in an advantageous embodiment the timer set to time t_1 registered by the network. The counter value and start time are stored 303 for future reference. The next time an attach is registered by the same device, say at time t_2 the elapsed time T, equal to :

$$t_2 - STH$$

is compared to a predetermined time interval ΔH 304.

If : $T = \Delta H$, or, $T > \Delta H$,

the counter NH and the timer are cleared, 305.

If : $T < \Delta H$,

the counter NH is increased by a value of 1 and the value of STH is replaced by the time t_2, 305. NH and STH are again stored 308. In this case the counter value is further compared with a predetermined threshold, LimitH, 306.

If : $NH = LimitH$,

an alert is set. If not, the method returns to step 304.

Again, the skilled person will understand there are minor variations which can be made to the embodiment which will still work. For example, the counter could be increased if T is less than or equal to ΔA and only cleared if T is greater than ΔA. Also for example, LimitH could be a value which must be exceeded, in which case an alert flag would be set if NH > LimitH.

The particular advantages of the invention are that a telecommunications network can monitor for malicious activity in mobile devices and identify when a particular device is potentially infected by malware. Although use of the invention requires network resources that would otherwise not be expended, it allows the easy identification of devices which may use up far greater network resources if left unidentified.

As the skilled person will understand, appropriate values for LimitH and the predetermined time interval ΔH will vary depending on the network and the customer base. However, suitable values are ΔH = 2s and LimitH = 20.

Claims

1 A system for detecting behaviour of a mobile telecommunications device in a telecommunications network,

the system comprising:

a telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and further to process the signals into data streams,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,

characterised in that,

the network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

2 The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence of data of the first type by counting the number of times data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3 The system according to claim 2 wherein the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4 The system according to claim 3 wherein the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if the following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

5 The system according to claim 1 wherein the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate.

6 The system according to claim 5 wherein the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate the rate as the ratio of the counted detection of occurrence of data of the first type to the time as measured by the timer.

7 The system according to claim 1 wherein the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer.

8 The system according to claim 1 wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9 The system according to claim 1 wherein the data of the first type indicates the setting up of a bearer by the mobile telecommunications device.

10 The system according to claim 1 wherein the data of the first signal type indicate handover of the mobile telecommunications device.

11 The system according to claim 10 wherein the telecommunications network is further arranged to monitor the tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12 The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the MME or SGSN or MSC of the telecommunications network.

13 The system according to claim 1 wherein the a telecommunications network is further configured to

- identify at least one additional mobile telecommunications device,

- to receive signals from the at least one additional device and to process these signals into additional data streams,

- to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14 Device for detecting behaviour of a mobile telecommunications device arranged to transmit signals to a telecommunications network and wherein the signals are processed into data streams within the telecommunications network, and further wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,

wherein the device is:

arranged to be coupled to the telecommunications network and arranged to receive the data streams and further wherein the device is arranged to monitor an occurrence in the data streams of the data of the first type and arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network.

15 A device according to claim 14 wherein the device is further arranged to operate within a MME or SGSN or MSC.

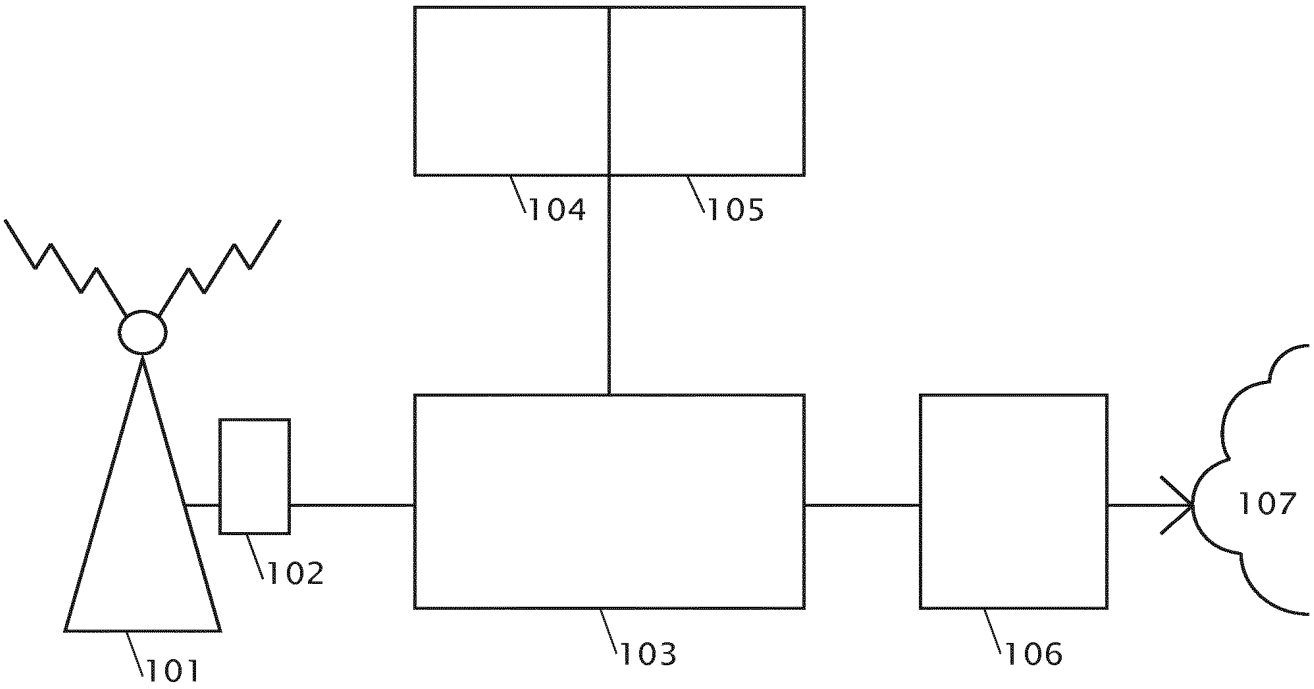


Figure 1

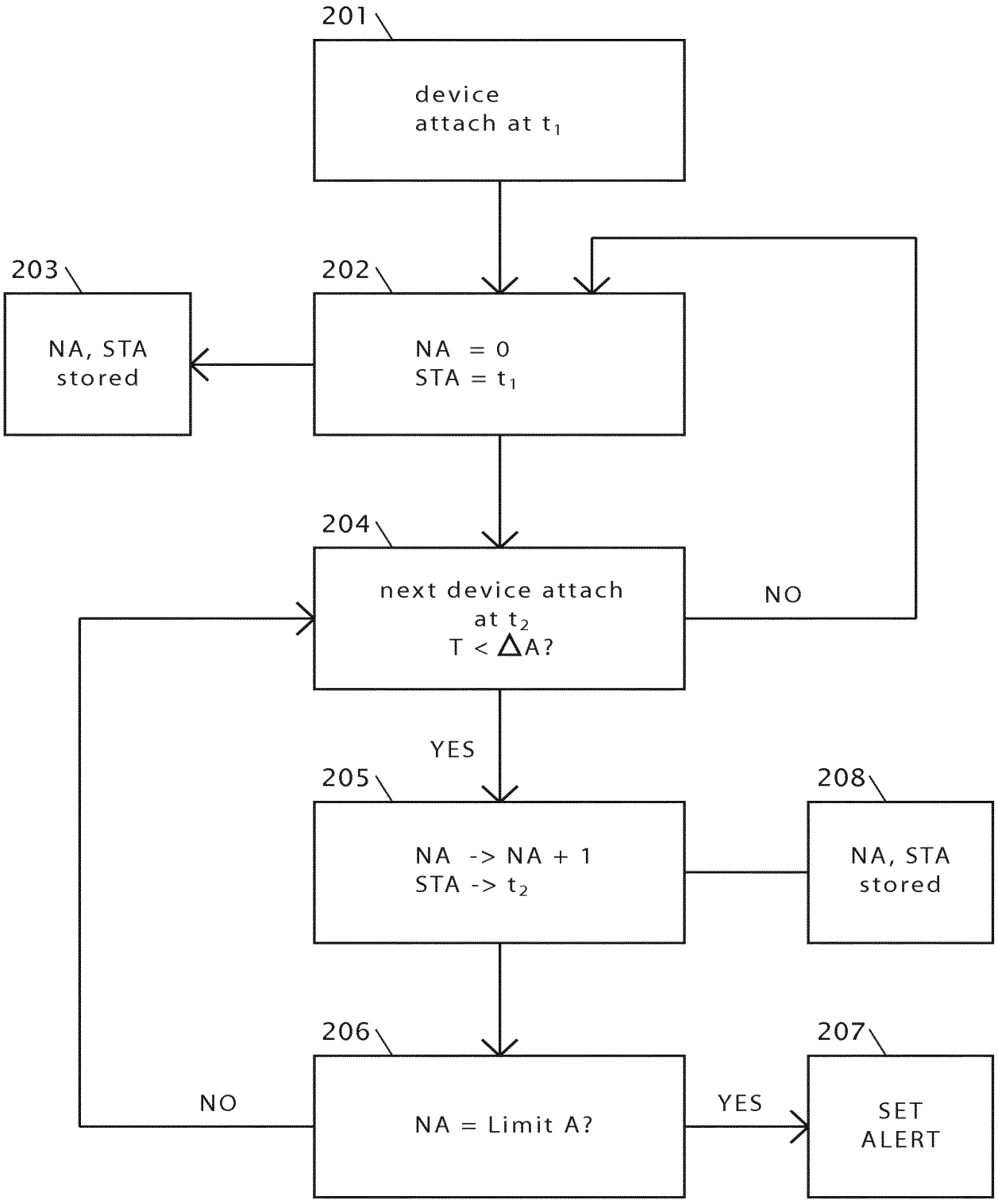

201
device attach at t_1
202
NA = 0
STA = t_1
203
NA, STA stored
204
next device attach at t_2
$T < \Delta A$?
NO
YES
205
NA -> NA + 1
STA -> t_2
208
NA, STA stored
206
NA = Limit A?
NO
YES
207
SET ALERT

Figure 2

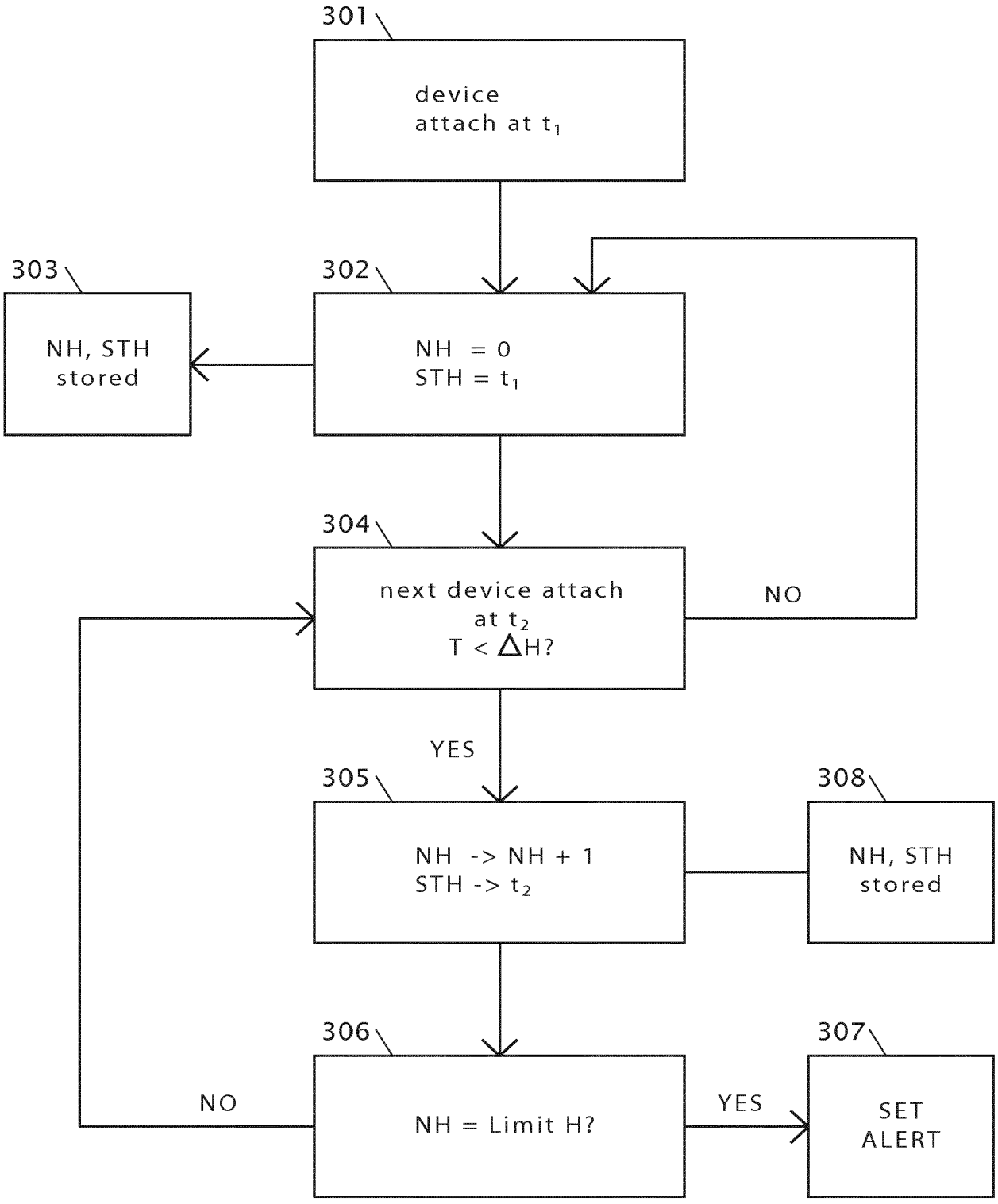

301
device
attach at t_1
303
NH, STH
stored
302
NH = 0
STH = t_1
304
next device attach
at t_2
T < ΔH?
NO
YES
305
NH -> NH + 1
STH -> t_2
308
NH, STH
stored
306
NH = Limit H?
NO
YES
307
SET
ALERT

Figure 3

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED INVENTOR	ATTY. DOCKET NO.
14/646,554	Frank Muller	15-686-WO-US

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

INTERNATIONAL APPLICATION NO.	
PCT/EP2013/074440	
I.A. FILING DATE	PRIORITY DATE
11/22/2013	11/22/2012

CONFIRMATION NO. 4961
371 ACCEPTANCE LETTER

OC000000076153078

Date Mailed: 07/13/2015

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above. A Filing Receipt will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE or 371(c) DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1) and (c)(2) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN BELOW.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363)

05/21/2015
DATE OF RECEIPT OF 35 U.S.C.
371(c)(1) and (c)(2) REQUIREMENTS

The following items have been received:

- Copy of the International Application filed on 05/21/2015
- Copy of the International Search Report filed on 05/21/2015
- Copy of IPE Report filed on 05/21/2015
- Preliminary Amendments filed on 05/21/2015
- Information Disclosure Statements filed on 05/21/2015
- Inventor's Oath or Declaration filed on 05/21/2015
- Request for Immediate Examination filed on 05/21/2015
- U.S. Basic National Fees filed on 05/21/2015
- Priority Documents filed on 05/21/2015
- Application Data Sheet (37 CFR 1.76) filed on 05/21/2015

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

TONI M HOOD

Telephone: (571) 272-3654

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
14/646,554	05/21/2015		1480	15-686-WO-US	15	2

CONFIRMATION NO. 4961

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

FILING RECEIPT

OC000000078153077

Date Mailed: 07/13/2015

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**

Inventor(s)

Frank Muller, Delft, NETHERLANDS;

Applicant(s)

KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

Assignment For Published Patent Application

KONINKLIJKE KPN N.V., The Hague, NL
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2013/074440 11/22/2013

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
EUROPEAN PATENT OFFICE (EPO) 12193884.9 11/22/2012

If Required, Foreign Filing License Granted: 07/07/2015
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/646,554**
Projected Publication Date: 10/22/2015
Non-Publication Request: No
Early Publication Request: No

Title

System to Detect Behaviour in a Telecommunications Network

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/646,554

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	480
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	15 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1480

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	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	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360
(For use with Form PTO/SB/06)

Application Number	Filing Date
14646554	

Applicant(s) Frank Muller

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1					
2		1				
3		1				
4		1				
5		1				
6		1				
7		1				
8		1				
9		1				
10		1				
11		1				
12		1				
13		1				
14	1					
15		1				
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	2		0		0	
Total Depend	13	↵	0	↵	0	↵
Total Claims	15		0		0	

CLAIMS	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

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
14/646,554	05/21/2015	Frank Muller	15-686-WO-US

CONFIRMATION NO. 4961

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

PUBLICATION NOTICE

OC000000078212356

Title: System to Detect Behaviour in a Telecommunications Network

Publication No.US-2015-0304345-A1
Publication Date:10/22/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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

PLUS Search Results for S/N 14646554, Searched Mon May 02 09:35:42 EDT 2016

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

4154984 99
4608685 99
5029204 99
5195126 99
5245636 99
5553223 99
5608781 99
5826191 99
5974126 99
6047385 99
6094681 99
6134618 99
6208718 99
6229887 99
6298039 99
6307841 99
6310950 99
6353902 99
6381453 99
6404734 99
6421323 99
6463287 99
6516195 99
6574216 99
6625460 99
6763190 99
6874022 99
6934367 99
7099660 99
7130397 99
7142853 99
7143153 99
7293082 99
7363548 99
7412600 99
7627348 99
7945252 99
7945252 99
8107951 99
8300644 99
8359022 99
8411846 99
8442233 99
8504846 99
8638717 99
8665325 99
8738004 99
8750906 99
8787869 99
9031206 99

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 05/10/2016

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
05/10/2016	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) MULLER, FRANK	
	Examiner PHY ANH VU	Art Unit 2438	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/21/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-15* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-15* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *05/21/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☒ All b)☐ Some** c)☐ None of the:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *05/21/2015*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 14/646,554 filed on 05/21/2015 is presented for examination by the examiner.

Notice of Pre-AIA or AIA Status

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

Claim Objections

Claims 1-2, 10, 12 and 15 are objected to because of the following informalities:

Claim 1 recites "…a telecommunications network.." and "..a first type.." in lines 4 and 7, which should be ""…**~~a~~** **the** telecommunications network.." and "..**~~a~~** **the** first type.."

Claim also recites "..characterised.." and "..the network.." in lines 9 and 10 respectively, which should be "..characterized.." and "..the telecommunications network.."

Claim 2 recites "..the detected occurrences.." in line 4, which should be "..the **monitored** **~~detected~~** occurences.." Appropriate correction is required.

Claim 10 recites "..the first signal type.." which should be ""..the first **~~signal~~** type.."

Claims 12 and 15 recite "..the MME or SGSN or MSC.." these abbreviations have not been defined in the previous claims. So they need to be clearly defined.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4, 6, 9 and 11 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claim 4 recites the limitation "..the following.." in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 6 recites "…**the** rate as **the** ratio of **the** counted…." There are insufficient antecedent basis for these limitations in the claim.

Claim 9 recites "..**the** setting up.." There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites "..the tracking area.." in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claims 1 and 14, although the preamble of the claims recite "a system" and "device" respectively, the body of the claims do not positively recite any elements of

hardware. Therefore, the nature of the subject matter claimed may reasonably be construed as non-tangible embodiments. The mere recitation of a system in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101.

Claims 2-13 and 15 depend on claims 1 and 14 respectively, as such, they also inherent the 101 rejections as their independent claims above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-10 and 12-15 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu).

Regarding claim 1, Bu discloses a system for detecting behaviour of a mobile telecommunications device in a telecommunications network,

the system comprising:

a telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device and further to process the signals into data streams *([0045]-[0047][0049]-[0053], signals from mobile/user is obtained and are processed into packets)*, and

wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0060], normal/non-attack data)*,

characterised in that,

the network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network *([0049]-[0050][0057], if traffic ratio exceeds a certain threshold, signals as malicious)*.

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence of data of the first type by counting the number of times data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of packets have been flagged as suspicious, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval *([0057], packets flagged have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection

of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if the following detection of data of the first type occurs within the predetermined time interval T as measured by the timer *(table 2; [0050]-[0057], packets are tracked and counted for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate *(table 2; [0054]-[0057], packets are tracked for predetermined threshold)*.

Regarding claim 6, Bu discloses the system according to claim 5. Bu further discloses the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate the rate as the ratio of the counted detection of occurrence of data of the first type to the time as measured by the timer *(table 2; [0054]-[0057], ratio of tracked packets is generated)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates attachment of the mobile

telecommunications device to the telecommunications network *([0019]-[0020][0027]-[0028], establishment data)*.

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates the setting up of a bearer by the mobile telecommunications device *([0025], setup of radio access bearer (RAB))*.

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the data of the first signal type indicate handover of the mobile telecommunications device *(figure 5; [0037]-[0039])*.

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the MME or SGSN or MSC of the telecommunications network *([0021], SGSN)*.

Regarding claim 13, Bu discloses the system according to claim 1. Bu also discloses the telecommunications network is further configured to identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams *([0045]-[0047][0049]-[0053], signals from another mobile/user is obtained and are processed into packets)*,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications

network *([0049]-[0050][0057], if traffic ratio exceeds a certain threshold, signals as malicious)* ,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Regarding claim 14, Bu discloses device for detecting behaviour of a mobile telecommunications device arranged to transmit signals to a telecommunications network and wherein the signals are processed into data streams within the telecommunications network, and further wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0045]-[0047][0049]-[0053], signals from mobile/user are sent and are processed into packets)*,

wherein the device is:

arranged to be coupled to the telecommunications network and arranged to receive the data streams !0 and further wherein the device is arranged to monitor an occurrence in the data streams of the data of the first type and arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if traffic ratio exceeds a certain threshold, signals as malicious)*.

Regarding claim 15, Bu discloses a device according to claim 14. Bu also discloses the device is further arranged to operate within a MME or SGSN or MSC *([0021], SGSN)*.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin).

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0037]-[0039], handover to different BS)*.

Bu does not disclose monitor the tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a

single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on Wed 7:00-5:30, TH-F 7-5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH VU/
Examiner, Art Unit 2438
/TAGHI ARANI/
Supervisory Patent Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/646,554	Applicant(s)/Patent Under Reexamination MULLER, FRANK	
	Examiner PHY ANH VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2006/0230450 A1	10-2006	Bu; Tian	H04L63/1416	726/22
*	B	US-5,953,652 A	09-1999	Amin; Umesh J.	H04L63/1408	455/410
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
H04L 63/14	5/2/2016	PVU
H04L 63/1425	5/2/2016	PVU

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016	PVU

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14/646,554
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	~~TBA~~ 2438
Examiner Name	~~TBA~~ Phy Anh Vu
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/P.V./	1	20060288407	A1	2006-12-21	NASLUND et al.	
/P.V./	2	20110185419	A1	2011-07-28	BOTELER et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/P.V./	1	2 139 279	EP	A1	2009-12-30	TELEFONAKTIEBOLAGET LM ERICSSON		☐
/P.V./	2	98/33340	WO	A2	1998-07-30	AT&T WIRELESS SERVICES, INC.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14/646,554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	~~TBA~~ 2438
	Examiner Name	~~TBA~~ Phy Anh Vu
	Attorney Docket Number	15-686-WO-US

/P.V./	3	98/33340	WO	A3	1998-07-30	AT&T WIRELESS SERVICES, INC.		☐
/P.V./	4	2006/104752	WO	A1	2006-10-05	LUCENT TECHNOLOGIES INC.		☐

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

NON-PATENT LITERATURE DOCUMENTS **Remove**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/P.V./	1	European Search Report, European Patent Application No. 12193884.9, dated March 1, 2013.	☐
/P.V./	2	MULLINER, Collin et al., "Taming Mr. Hayes: Mitigating Signaling Based Attacks on Smartphones", IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), 2012, pp. 1-12.	☐
/P.V./	3	PCT International Search Report, PCT International Application No. PCT/EP2013/074440, dated February 7, 2014.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Phy Anh Vu/	Date Considered	05/02/2016

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

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

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
L2	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
L3	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
L4	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
L5	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
L6	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
L7	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
L8	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
L9	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
L10	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
L11	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
L12	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:32
L13	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L14	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
L15	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	OFF	2016/05/02 11:35

			DERWENT; IBM_TDB			
L16	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
L17	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
L18	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
L19	30	l18 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
L20	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
L21	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23
S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55

5/2/2016 12:57:53 PM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 4961

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/646,554	05/21/2015	726	2438	15-686-WO-US

APPLICANTS

KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

INVENTORS

Frank Muller, Delft, NETHERLANDS;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/EP2013/074440 11/22/2013

**** FOREIGN APPLICATIONS ***************************

EUROPEAN PATENT OFFICE (EPO) 12193884.9 11/22/2012

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

07/07/2015

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/PHY ANH TRAN VU/ Examiner's Signature	☐ Initials	NETHERLANDS	3	15	2

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

System to Detect Behaviour in a Telecommunications Network

FILING FEE RECEIVED		
1480	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	05/02/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO OFFICE ACTION MAILED MAY 10, 2016

This submission is made in response to the Office Action mailed May 10, 2016. In addition, a Petition for Extension of Time under 37 C.F.R. § 1.136(a) (one-month) is enclosed, along with requisite fees.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system for detecting behaviour of a mobile telecommunications device in a telecommunications network, the telecommunications network including a base station,

the system comprising:

the base station for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network;

[[a]] the telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,

~~characterised~~ characterized in that,

the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

2. (Currently amended) The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence of data of the first type by counting the number of ~~times~~ occurrences data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Currently amended) The system according to claim 2 wherein the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Currently amended) The system according to claim 3 wherein the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if ~~the~~ a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

5. (Currently amended) The system according to claim 1 wherein the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate.

6. (Currently amended) The system according to claim 5 wherein the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

further arranged to calculate ~~the~~ a rate as ~~the~~ a ratio of ~~the~~ counted detection of occurrence of data of the first type to ~~the~~ time as measured by the timer.

7. (Currently amended) The system according to claim 1 wherein the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Currently amended) The system according to claim 1 wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9. (Currently amended) The system according to claim 1 wherein the data of the first type indicates ~~the~~ setting up of a bearer by the mobile telecommunications device.

10. (Currently amended) The system according to claim 1 wherein the data of the first ~~signal~~ type indicate handover of the mobile telecommunications device.

11. (Currently amended) The system according to claim 10 wherein the telecommunications network is further arranged to monitor ~~the~~ a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

12. (Currently amended) The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the ~~MME~~ Mobility Management Entity or ~~SGSN~~ Serving Gateway Support Node or ~~MSC~~ Mobile Switching Center of the telecommunications network.

13. (Currently amended) The system according to claim 1 wherein the a telecommunications network is further configured to

identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Currently amended) ~~Device~~ A device for detecting behaviour of a mobile telecommunications device ~~arranged to transmit signals to~~ in a telecommunications network, wherein a base station of the telecommunications network converts radio transmissions received from the mobile telecommunications device into signals and wherein the signals are processed into data streams within the telecommunications network, and further wherein the data streams

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

include data of a first type arranged to cause an event of a first type within the telecommunications network,

wherein the device is:

arranged to be coupled to the telecommunications network and arranged to receive the data streams and further wherein the device is arranged to monitor an occurrence in the data streams of the data of the first type and arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network.

15. (Currently amended) A device according to claim 14 wherein the device is further arranged to operate within a ~~MME~~ Mobility Management Entity or ~~SGSN~~ Serving Gateway Support Node or ~~MSC~~ Mobile Switching Center.

16. (New) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network, the telecommunications network including a base station, the method comprising:

the base station for receiving radio transmissions from the mobile telecommunications device;

the base station converting the received radio transmissions into signals, and sending the signals into the telecommunications network;

the telecommunications network identifying the mobile telecommunications device;

the telecommunications network receiving the signals from the mobile telecommunications device by way of the base station, and processing the signals into data

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

streams, wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network; and

the telecommunications network monitoring for an occurrence in the data streams of the data of the first type and registering when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Office Action

In the Office Action mailed May 10, 2016 ("Current Office Action," hereinafter), the Examiner objected to claims 1-2, 10, 12, and 15 for informalities. The Examiner rejected claims 4, 6, 9, and 11 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph as being allegedly indefinite. The Examiner also rejected claims 1-15 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. The Examiner rejected claims 1-10 and 12-15 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). Finally, the Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-16, of which claims 1, 14, and 16 are independent, and the remaining claims are dependent. Claim 16 is new. Applicant has amended various claims as follows.

Applicant has amended each of claims 1, 2, 10, 12, and 15, generally in accordance with the Examiner's suggestions, to address the objections to these claims, as described below. Applicant has amended each of claims 4, 6, 9, and 11, generally in accordance with the Examiner's suggestions, ensure proper antecedent basis.

Applicant has also amended claim 1 to recite, *inter alia*, a "base station for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

network." Support for these amendments can be found generally throughout the original application, and specifically at least at page 8, lines 5-6, for example.

Applicant has amended claim 14 to recite, *inter alia*, a "base station" in a manner similar to that of claim 1. Support for this amendment is the same as that for claim 1.

Applicant has amended each of claims 1-15 to introduce a period (".") after each claim number. This amendment corrects an inadvertent formatting error.

No new matter has been introduced by way of any of the above amendments.

3. Response to Claim Objections

Examiner objected to claims 1-2, 10, 12, and 15 for informalities. Specifically, the Examiner suggested that the recitation in claim 1 of "a telecommunications network" should be replaced by "the telecommunications network," and the recitation of "an event of a first type" should be replaced by "the event of a first type." Applicant has made the first of these suggested replacements but not the second, because the term "first type" is used in two different contexts in claim 1. Namely, "*data* of a first type" and "*an event* of a first type" (emphasis added). As such, the first usage of the term "first type" is not antecedent basis for the second usage or the term.

The Examiner suggested the term "detected occurrences" in claim 2 be replaced by "monitored occurrences." Applicant has instead amended claim 2 to recite "counting a number of occurrences data of the first type is detected. As such, the term "detected occurrences" is proper and need not be replaced.

Applicant has amended each of claims 10, 12 and 15 in accordance with the Examiner's suggestions.

In view of the above-described amendments and explanations, Applicant respectfully requests the Examiner withdraw the objections to claims 1-2, 10, 12, and 15 for informalities.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

4. Response to Rejections under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph

The Examiner rejected claims 4, 6, 9, and 11 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph as being allegedly indefinite. Specifically, the Examiner asserted insufficient antecedent basis for various terms recited in these claims. As described above, Applicant has amended each of claims 4, 6, 9, and 11, generally in accordance with the Examiner's suggestions, ensure proper antecedent basis. Accordingly, Applicant respectfully requests the Examiner withdraw the rejections to claims 4, 6, 9, and 11 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph.

5. Response to Rejections under 35 U.S.C. § 101

The Examiner rejected claims 1-15 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Specifically, the Examiner asserted that the subject matter of claims 1 and 14 "may reasonably be construed as non-tangible embodiments. Without acquiescing to the Examiner's characterization of claims 1 and 14, Applicant has amended claims 1 and 14 to describe, *inter alia*, a base station that converts received radio transmissions into signals in a network. Applicant submits that these amendments overcome the rejections to claims 1 and 14 under 35 U.S.C. § 101, and respectfully request the Examiner withdraw the rejections of claims 1 and 14, as well as dependent claims 2-13 and 15, under 35 U.S.C. § 101.

6. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-10 and 12-15 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. Applicant submits that Bu fails to teach each and every element set forth in any of claims 1-10 or 12-15, and that these claims are allowable. Applicant first discusses claim 1, then subsequently addresses claims 2-10 and 12-15.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Bu does not teach: "wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network"

Bu teaches methods and devices for defending against signaling attacks in wireless networks by identifying malicious traffic according to excessive "signaling cost(s)" that it introduces into the network (paragraph [0045]). As such, Bu teaches "signaling cost" as a type of data, but it is not "data of a first type" that is included in any data streams, but rather is a derived property of signaling traffic. Furthermore, even if, for the sake of argument, "signaling cost" is considered "data of a first type," Bu does not teach that "signaling cost" causes an "event of a first type within the telecommunications network," but rather that excessive "signaling cost" introduced by malicious traffic can adversely affect the network in general.

The Examiner cited to paragraph [0060] in Bu as disclosing "normal/non-attack data," and asserted that this teaches "wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network" (Current Office Action, page 4). Applicant respectfully disagrees. In paragraph [0060], Bu merely teaches generating a traffic profile for given user "under normal (i.e., non-attack) conditions," which is later used to determine if signaling traffic from the given user violates a threshold. But there is no teaching of "wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network," as recited in claim 1.

Bu does not teach: "the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network"

Bu teaches "a simple, yet novel mechanism of estimating the signaling cost from traffic arrival patterns assuming knowledge of signaling call(s)" (paragraph [0046]). Thus, even if the "signaling cost" in Bu is identified with the "data of the first type" in claim 1, it is not

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

determined by monitoring for its occurrence in "data streams," but rather derived from "from traffic arrival patterns assuming knowledge of signaling call(s)."

Alternatively, the Examiner's assertion that "normal/non-attack data" allegedly disclosed in Bu teaches "wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network" might adopted for the sake of argument. But in this case, there is no teaching in Bu of monitoring the occurrence of "normal/non-attack data" "to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network." Rather, as already noted, Bu teaches generating a traffic profile for given user "under normal (i.e., non-attack) conditions" to later determine if signaling traffic from the given user violates a threshold. Thus, "normal/non-attack data" cannot be both the data used to generate the profile and the "data of the first type" that is later monitored.

For at least the reasons above, Applicant respectfully submits that Bu does not anticipate claim 1, and that claim 1 is therefore allowable.

Claim 14 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 14 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 1-10, 1-13, and 15 depends from one or another of claims 1 and 14, both of which are allowable for at least the reasons above. Applicant therefore submits that claims 1-10, 1-13, and 15 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with any of claims 1-10, 1-13, or 15.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

7. Response to Rejections under 35 U.S.C. § 103(a)

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

8. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: August 26, 2016

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	2483
Examiner Name	Vu, Phy Anh Tran
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120155274		2012-06-21	Wang et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	JP2004-320636	JP		2004-11-11	NIPPON TELEGR & TELEPH CORP <NTT>		☒
	2	JP2006-295240	JP		2006-10-26	MITSUBISHI ELECTRIC CORP		☒
	3	WO2007075423	WO		2007-07-05	Lucent Technologies Inc.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

	4	JP2006-350561	JP		2006-12-28	MATSUSHITA ELECTRIC IND CO LTD		☒

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2016-08-26
Name/Print	David A. Grabelsky	Registration Number	59,208

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

(11)Publication number 2004-320636

(43)Date of publication of application 11.11.2004

(51)Int.Cl. H04L 12/56
G06F 13/00

(21)Application number 2003-114578

(22)Date of filing 18.04.2003

(71)Applicant NIPPON TELEGR & TELEPH CORP <NTT>

(72)Inventor TERAYAMA NAOHIRO

---

(54)DoS ATTACK SOURCE DETECTING METHOD, ITS BLOCKING METHOD, SESSION CONTROL APPARATUS, ROUTER CONTROL APPARATUS, PROGRAM AND ITS STORAGE MEDIUM

(57)Abstract

PROBLEM TO BE SOLVED: To provide a method for detecting various type DoS attack and a regulating method for guarding against the invasion of the DoS attack packets into CA and for preventing a memory leak in CA.
SOLUTION: Within a CA 10, three counters are arranged, i.e., a DoS counter for detecting the DoS attack from a single attack source, a DoS counter for detecting the DoS attack from a plurality of the attack sources, and an unauthorized signal counter for detecting the DoS attack by the unauthorized signal whose format and parameter are abnormal. Thereby, the various type of the DoS attack can be tackled. Further, when the DoS attack is detected, the DoS attack is processed by locked-out in the CA 10 and besides information on an IP address of the attack source is informed to subscriber routers 31, 32, 33 that stores the attack source to perform filtering regulation by the subscriber routers.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
In the network of the bearer and control discrete type in which the present invention used the IP network as the core network, CA is used as a heavy load by requiring service etc. of the session control equipment (CA:Control Agent) which manages session control from attack origin with a terminal etc. continuously mechanically, It is related with the so-called measure technology to the DoS (Denial of Service) attack which makes impossible service of terminals other than an attacking agency, and cyberterrorism preventive-measures technology.
[0002]
[Description of the Prior Art]
In recent years, the network of the bearer and the control discrete type which used the IP network as the core network is advocated. This uses an IP network as a core network, and it constitutes a control network from a CA which performs session control and terminal control, Certainly perform transmission and reception of the control signal between terminals via CA, and it constitutes a bearer network from relay routers which relay bearer signals, such as a sound between the subscriber's router which stores a terminal, and a terminal, or an image, Transmission and reception of the bearer signal between the terminals after session setup are a system held in the form relayed with a bearer network without passing CA. Here, the case of VoIP (Voice Over IP) is made into an example. When the session control of CA performs pictorial communication between terminals, it is also the same as that of VoIP.
[0003]
In the network of a bearer and a control (VoIP call control) discrete type, It is divided roughly into the method of detecting DoS attack origin for the measure against an act (DoS attack) into which the call-processing controllability of terminals other than an attacking agency is made falling impossible by CA, and the method of restricting DoS attack origin by continuing transmitting a lot of packets to CA mechanically from the attack origin of a certain specific terminal.
[0004]
About the method of detecting DoS attack origin, the method of carrying out the thing beyond a threshold value an attacking agency using one kind of counter which counts the number of calling signals or the number of terminal registered signals per unit time per one terminal within CA is proposed conventionally (for example, see nonpatent literature 1). In the case of this method, the DoS attack (single DoS attack) from independent attack origin is detectable, but. When the sending frequency per attacking agency of one is below a threshold value in the case of the DDoS attack (DistributedDoS attack) which carries out a DoS attack from a plurality of attack origin, it cannot detect, even if the sending frequency in the whole attacking agency is beyond a threshold value. Since the case, the DDoS attack, and distinction by an event which carry out access concentration (example: ticket reservation of a popular event) are hard to attach a DDoS attack, there is a possibility of considering that All Users who is accessing for the event is DDoS attack origin.
[0005]

ERICSSON EXHIBIT 1005, Page 209

Furthermore, by the former, since there was no counter which detects DS attack by the signal which has abnormalities in a format and parameter of a signal, such an attack was not able to be detected.
[0006]
On the other hand, about the method of restricting DoS attack origin, before a packet comes into CA conventionally, the method of detecting a DoS attack by a fire wall and performing packet discarding is proposed (for example, see nonpatent literature 2). However, since a fire wall discards the contents of the signal, without seeing, when the signal in the middle of call connection is discarded, there is a possibility of connection processing not being completely completed by CA, but starting a memory leak.
[0007]
[Nonpatent literature 1]
Naohiro Terayama Outside is one person and "the congestion control system at the time of IP telephony offer",
Institute of Electronics, Information and Communication Engineers network system study group technical research report,
NS2001-142, P.7 November 14, 2001 [-12 or] issue
[Nonpatent literature 2]
About offer of "personal firewall service" in NTT Communications News Release and OCN ADSL service (A), July 24, 2002 printing, the
Internet<URL:http://www.ntt.com/release/2002NEWS/0007 / 0724.html>
[0008]
[Problem to be solved by the invention]
In the network of the bearer and control discrete type in which the object of this invention used the IP network as the core network, The access concentration and the DDoS attack by an event are distinguished in CA, and there are the method and format, and parameter which detect only a DDoS attack in providing the method of detecting the DoS attack origin by unusual incorrect signals, its CA, a program, and a recording medium.
[0009]
In the network of the bearer and control discrete type in which another object of the present invention used the IP network as the core network, It is in providing the restriction method of preventing the packet of a DoS attack entering into CA, and not starting a memory leak by CA, its routers OpS and CA, a program, and a recording medium.
[0010]
[Means for solving problem]
[in CA] the present invention, The DoS attack from independent attack origin. The counter (Single DoS counter) to detect, the counter (DDoS counter) which detects the DoS attack from two or more attack origin, and a format and a parameter install three of incorrect-signals counters which detects the DoS attack by unusual incorrect signals, and them a DDoS counter, It is characterized [main] by taking a long monitor cycle and making a threshold value lower [than a SingleDoS counter] than a Single DoS counter. According to these characteristics, correspondence in a DoS attack various type is attained.
[0011]
Although a part of detection function degenerates, it is also possible to suppose that omit an incorrect-signals counter depending on the case, or an incorrect-signals counter and a Single DoS counter should combine.

[0012]
During the period until the present invention detects a DDoS attack at a DDoS counter, By hanging a traffic density restriction (restriction which restricts the total number of calls included in CA per unit time), CA is protected and the target signal is further limited to the start request signal of the registered signal to the service in the service which provides CA (server) and/, or service. According to these characteristics, protection of CA can be attained and the packet discarding in the middle of service can be avoided.
[0013]
After the present invention detects a DoS attack at a Single DoS counter, a DDoS counter, and an incorrect-signals counter, It not only carries out lockout processing by CA, but it notifies to the subscriber's router which stores information on IP address of attacking agency attack-origin further, and a subscriber's router performs IP address filtering (restriction which discards the packet from an applicable IP address). According to these characteristics, the packet of a DoS attack can be beforehand prevented from going into CA.
[0014]
[Mode for carrying out the invention]
Hereinafter, it describes using Drawings about the 1 embodiment of the present invention. Although the case of voice service (VoIP) is described for an example below, it is also the same as when the session control of CA performs pictorial communication between terminals.
[0015]
<Network composition>
Fig.1 is a key map of the network of the bearer and control discrete type which used the premised IP network as the core network by the present invention. As stated previously, in the network of the bearer and control (VoIP call control) discrete type used as the core network, an IP network, The control network 1 comprises the session control equipment (CA:Control Agent) 10 which performs session control and terminal control, and transmission and reception of the control signal between the terminals 11 and 12 are certainly performed via CA10. On the other hand, the bearer network 2 comprises the relay routers 15 and 16 which relay the subscriber's routers 13 and 14 and bearer signal (VoIP audio signal) which store the terminals 11 and 12, Transmission and reception of the bearer signal between the terminals 11 and 12 after session setup are performed in the form relayed with the bearer network 2, without passing CA10.
[0016]
In the network of the bearer and control discrete type which used such an IP network as the core network, When service etc. are mechanically required from the attack origin of a single or multiple terminal etc. continuously to CA10 which controls a session, CA10 becomes a heavy load and service control (session control processing) other than [11 and 12] an attacking agency (for example, terminals) becomes impossible.
[0017]
Below, the specific working example of the DoS attack former detecting method by the present invention and the DoS attack inhibition method is explained in full detail.
[0018]
<DoS attack former detection>
Fig.2 is a configuration diagram of one working example of the session control equipment (CA) by the present invention, and shows only the portion especially related to DoS attack detection. It is the 4th counter for the incorrect-signals counter 101 to detect the DoS attack by incorrect signals with a format or an unusual parameter in Fig.2. The DoS counter 102 is a first counter

ERICSSON EXHIBIT 1005, Page 211

(Single DoS counter) for detecting the DoS attack from independent attack origin. The traffic density counter 103 is the 3rd counter (Distributed DoS counter) for the second counter which counts the total number of calls per [included in CA10] unit time, and the DDoS counter 104 to detect the DoS attack from two or more attack origin. Here, the incorrect-signals counter 101, the DoS counter 102, and the DDoS counter 104 are prepared for every IP address. The monitoring period of the DoS counter 102 is set to $t_1<t_2$, v1> v2, when the monitoring period of v1 and the DDoS counter 104 is made into t_2 and a threshold value is set to v2 for t_1 and a threshold value.
[0019]
The signal-format parameter check part 105 is a processing part which performs the format of a signal and the check of a parameter included in CA10. The packet discard part 106 is a processing part in which the incorrect-signals counter 101 discards the unauthorized packet applicable to the IP address below a prescribed threshold value. The traffic density restriction processing part 107 is a processing part which performs a traffic density restriction (totals, such as a session establishment request signal, are restricted), when the traffic density counter 103 is beyond a prescribed threshold value. The lockout processing part 108 at least one of the incorrect-signals counter 101, the DoS counter 102, and the DDoS counters 104. It is a processing part which locks out to an applicable IP address about the IP address beyond a prescribed threshold value, and the IP address informing part 109 is a processing part which notifies an applicable IP address to the below-mentioned router control device (router OpS). The call processing section 110 is a processing part which performs predetermined processing about a regular call.
[0020]
Each above-mentioned counter 101-104 and operation of each processing part 105-110 are controlled by the control part 100.
[0021]
Fig.3 is a processing flow chart of the DoS attack detection in CA. hereinafter -- being based on Fig.3 -- CA of the configuration example of Fig.2 -- the operation to kick is described.
[0022]
All the signals containing the regular call and DoS attack call included in CA10 are first checked [the format of a signal, and / of a parameter] in the signal-format parameter check part 105 (S11, S12). In the case of NG, in the incorrect-signals counter 101, the number of incorrect signals per unit time is counted for every IP address (S18). If it is beyond a certain threshold value here, while regarding it as the DoS attack by incorrect signals and performing lockout processing to an applicable IP address by the lockout processing part 108, An applicable IP address is notified to an external device (for example, the below-mentioned router OpS) by the IP address informing part 109 (S19, S20). If it is below a threshold value, only abandonment of an applicable packet will be performed (S19, S21).
[0023]
On the other hand, in OK, in the signal-format parameter check part 105, In the DoS counter 102, the signal number of the calling signal per unit time (in the case of SIP INVITE signal) or a terminal registered signal (in the case of SIP REGISTER signal) is counted for every IP address (S13). Here, while regarding it as the DoS attack from independent attack origin in the case of the IP address beyond a threshold value and performing ROKKUAU and processing to an applicable IP address by the lockout processing part 108, an applicable IP address is notified to an external device by the IP address informing part 109 (S14, S20).
[0024]

ERICSSON EXHIBIT 1005, Page 212

In below a threshold value, the counted value of the DoS counter 102 counts the total number of calls per [included in CA10] unit time (in the case of SIP an INVITE number or a REGISTER number) at the traffic density counter 103 about each IP address (S15). Here, if it is below a threshold value, predetermined call processing will be performed in the call processing section 110 (S16, S17).

[0025]

On the other hand, when the traffic density counter 103 is beyond a threshold value, the DDoS counter 104 and the traffic density restriction processing part 107 start simultaneously. In the traffic density restriction processing part 107, the restriction of the traffic density of CA10 is started and congestion is prevented (S22). At the DDoS counter 104, it is a threshold value (value at the time of performing continuous transmission at intervals of such short sending out that it not being the objects to talk over the telephone and terminal register) lower than the DoS counter 102 which is a long-term monitoring period, The signal number of the calling signal per unit time or a terminal registered signal is counted for every IP address (S23). For example, if the threshold value of the DoS counter 102 becomes 50 INVITE/s, the threshold value of the DDoS counter 104 will be set to 30 INVITE(s)/30 s.

[0026]

Here, when the DDoS counter 104 is below a threshold value, the traffic density rule in the traffic density rule processing part 107 is continued as it is (S24, S22). On the other hand, if the DDoS counter 104 has an IP address beyond a threshold value, it will regard it as the DoS attack from two or more attack origin, will release a traffic density rule (S24, S25), and will proceed to Step S20. As stated previously, while performing lockout processing to an applicable IP address by the lockout processing part 108, at Step S20, the IP address informing part 109 notifies a corresponding address to an external device (for example, the below-mentioned router OpS).

[0027]

<DoS attack inhibition>

The key map of one working example of the DoS attack inhibition method according [Fig.4] to the present invention and Fig.5 are operating-sequence figures. Hereinafter, operation of one working example of the DoS attack inhibition method according to the present invention is described based on Fig.4 and Fig.5. Relay routers are omitted in Fig.4 and Fig.5.

[0028]

In the authentication server 20, when a user terminal accesses a subscriber's router and authenticates, the information on the IP address of a user terminal and the information on the IP address of a subscriber's router are collected. Although the maintenance control of a subscriber's router or relay routers is managed generally, the router control device (router OpS) 30, If the notice of the IP address information on the DoS attack terminal (Fig.4 31, 32, 33) detected by the CA10 is here received from the session control equipment (CA) 10, Access the authentication server 20, search the IP address of the subscriber's router (Fig.4 34, 35, 36) which has stored it from the IP address information on a DoS attack terminal, and it receives the subscriber's routers 34, 35, and 36 of relevance, The command of IP address filtering which restricts the packet from a DoS attack terminal (strictly IP address of a DoS attack terminal) is distributed. The subscriber's routers 34, 35, and 36 will carry out IP filtering restriction which restricts the packet from the applicable DoS attack terminals 34, 35, and 36, if a **** command is received from router OpS30.

[0029]

As stated previously, when a DoS attack is detected by CA10, by CA10, lockout processing to an

ERICSSON EXHIBIT 1005, Page 213

attacking agency is performed first. Since it is not processed by this even if a calling signal or a terminal registered signal goes into CA10 from DoS attack origin, the load of CA10 is reduced. However, at this time, the load of the disposal treatment of the packet from DoS attack origin remains.

[0030]

Next, CA10 notifies the IP address information on an attacking agency to router OpS30. The IP address of the subscriber's router which stores an attacking agency using the authentication server 20 from the IP address information on an attacking agency is searched with router OpS30. And router OpS30 relevance distributes IP filtering restriction command which restricts the packet from an attacking agency to a subscriber's router, and a subscriber's router performs IP filtering restriction of DoS attack origin. Thereby, it can prevent that the packet of a DoS attack enters into CA.

[0031]

Fig.6 is a configuration diagram of one working example of the router control device (router OpS) 30 by the present invention. The notice receive section 301 of CA which receives the IP address of DoS attack origin, such as a DoS attack terminal, from CA, and the authentication server 20 are used for this router OpS30, It comprises the authentication server retrieval part 302 which searches the IP address of the subscriber's router which stores DoS attack origin, the restriction command distribution part 303 which distributes a restriction command to the subscriber's router of search results, and the control part 300 which controls operation of these each part 301, 302, and 303. Router OpS30 is omitted here, although it also has the original processing means for router maintenance etc.

[0032]

Fig.7 is a processing flow chart of this router OpS30. If the notice receive section 301 of CA receives the IP address of DoS attack origin, such as a DoS attack terminal, from CA10 (S31), it will start the authentication server retrieval part 302. The authentication server retrieval part 302 transmits the IP address of DoS attack origin to the authentication server 20, Retrieval required of the IP address of the subscriber's router which has stored the terminal of the DoS attack origin concerned, etc. is made, and correspondence with the IP address of DoS attack origin and the IP address of an applicable subscriber's router is acquired from the authentication server 20 as the response (S32). The restriction command distribution part 303 distributes IP filtering restriction command which restricts the packet from the terminal of DoS attack origin, etc. to an applicable subscriber's router based on the subscriber's router IP address of the search results by the authentication server retrieval part 302 (S33).

[0033]

Although router OpS30 was a system which distributes from CA10 the command which restricts the packet from a DoS attack terminal etc. from router OpS30 to the subscriber's router of relevance in response to the notice of IP address information, including a DoS attack former terminal etc., an above-mentioned working example, By mounting the same function as the above-mentioned router OpS30 in CA10, direct CA10 is able to distribute a restriction command to the subscriber's router which stores a DoS attack terminal etc. using the authentication server 20. The operating-sequence figure of this example is shown in Fig.8.

[0034]

If CA10 detects a DoS attack in the case of Fig.8, while performing lockout processing to an attacking agency, the IP address of the subscriber's router which stores an attacking agency using the authentication server 20 from the IP address information on an attacking agency is searched

ERICSSON EXHIBIT 1005, Page 214

itself [the / CA10]. And IP filtering restriction command which restricts the packet from an attacking agency to an applicable subscriber's router is distributed itself [the / CA10]. According to this example, since router OpS30 does not interpose, in an applicable subscriber's router, it becomes possible to restrict the packet from an attacking agency more nearly promptly.
[0035]
The composition of CA10 of this example should just add the authentication server retrieval part 302 and the restriction command distribution part 303 of Fig.6 to the composition of previous Fig.2, and it omits a graphic display. In previous Fig.3, a process flow loses "a notice of an IP address" in Step S20, and should just add Steps S32 and S33 of Fig.7 under the step S20 instead, and it omits a graphic display similarly.
[0036]
In [any] an working example, if router OpS30 or CA10 possess the conversion table of a terminal IP address and a subscriber's router IP address, the processing which searches the authentication server 20 which was described until now is unnecessary.
[0037]
What the processing capability of a part or all of each part in CA and the router OpS which were shown by Fig.2 or Fig.6 can be constituted from a program of a computer, the program can be run using a computer, and the present invention can be realized for, Or it cannot be overemphasized that the procedure shown by Fig.3 or Fig.7 can be constituted from a program of a computer, and a computer can be made to run the program. A program for a computer to realize the processing capability, Or the program for making a computer perform the procedure is recorded on the recording medium which the computer can read, for example, FD, MO, ROM, a memory card, CD, DVD, a removable disc, etc., While being able to save or provide, it is possible to distribute the program through networks, such as the Internet.
[0038]
[Effect of the Invention]
Since it understands whether talking over the telephone and terminal registering by monitoring in the long run at a DDoS counter according to the present invention are the continuous transmission which is not the object, there is an advantage which distinction of the access concentration according whether it is a DDoS attack to an event sticks, and can detect only a DDoS attack. About the attack received by DDoS attack detection, CA can be provisionally protected from an attack by performing a traffic density restriction. Next, a format and a parameter also have an advantage which can detect the DoS attack by unusual incorrect signals by installing an incorrect-signals counter.
[0039]
According to the present invention, CA can be protected from a DoS attack by locking out first by CA, without starting a memory leak. However, although the load of the packet disposal treatment of CA remains at this time, In order that the packet from an attacking agency may not go into CA by hanging IP filtering restriction from the information on the IP address of the attack origin detected by CA with the subscriber's router, CA has an advantage releasable from the load of packet disposal treatment. Since only the packet of an attacking agency is discarded, other users cannot be subject to the influence of a DoS attack, and can perform VoIP.
[Brief Description of the Drawings]
[Drawing 1]It is a key map of the network of premised bearer and control discrete type in the present invention.
[Drawing 2]It is a configuration diagram of one working example of the session control

ERICSSON EXHIBIT 1005, Page 215

equipment (CA) which realizes the DoS attack former detecting method of the present invention.
[Drawing 3]It is a processing flow chart of CA of Fig.2.
[Drawing 4]It is a key map of one working example of the DoS attack inhibition method according to the present invention.
[Drawing 5]It is an operating-sequence figure of the working example of Fig.4.
[Drawing 6]It is a configuration diagram of one working example of the router control device (router OpS) which realizes the DoS attack inhibition method of the present invention.
[Drawing 7]It is a processing flow chart of the router OpS of Fig.6.
[Drawing 8]It is an operating-sequence figure of another working example of the DoS attack inhibition method according to the present invention.
[Explanations of letters or numerals]
1 Control network
2 Bearer network
10 Session control equipment (CA)
11 and 12 Terminal
13, 14, 34, 35, 36 subscriber's routers
15, 16 relay routers
20 Authentication router
30 Router control device (router OpS)
31, 32, 33 DoS-attack terminal
100 Control part
101 Incorrect-signals counter
102 DoS counter
103 Traffic density counter
104 DDoS counter
105 Signal-format parameter check part
106 Packet discard part
107 Traffic density restriction processing part
108 Good out processing part
109 IP address informing part
110 Call processing section
300 Control part
301 Notice receive section of CA
302 Authentication server retrieval part
303 Restriction command distribution part

ERICSSON EXHIBIT 1005, Page 216

CLAIMS

[Claim(s)]
[Claim 1]
In a network of a bearer and a control discrete type which used an IP network as a core network, To session control equipment (the following, CA) which controls a session, carry out continuous transmission mechanically from a certain attack origin, and it uses CA as a heavy load, It is a DoS attack former detecting method in a DoS (Denial of Service) attack which makes impossible session control processing of terminals other than an attacking agency,
A step which counts a terminal registered signal or/and a session establishment request signal number of a predetermined monitoring period for every IP address to the aforementioned CA with the 1st counter,
A step which starts the 3rd counter when a threshold value which counted a terminal registered signal or/and a session establishment request signal number to the aforementioned CA with the 2nd counter, and was preliminarily defined during a predetermined monitoring period is exceeded,
A step which counts a terminal registered signal or/and a session establishment request signal number of a predetermined monitoring period longer than a monitoring period of said 1st counter for every IP address to the aforementioned CA with said 3rd counter,
A step which judges IP address origin which became at either said 1st counter and the 3rd counter beyond a threshold value (however, threshold value of the threshold value > 3rd counter of the 1st counter) to be DoS attack origin,
A ****(ing) DoS attack former detecting method.
[Claim 2]
In the according to claim 1 DoS attack former detecting method,
A DoS attack former detecting method further having a step which restricts a total of a session establishment request signal after starting said 3rd counter until it detects DoS attack origin.
[Claim 3]
In a network of a bearer and a control discrete type which used an IP network as a core network, it is a DoS attack former detecting method in a DoS attack which carries out continuous transmission mechanically from a certain attack origin, uses CA as a heavy load to CA, and makes impossible session control processing of terminals other than an attacking agency,
A step which counts a terminal registered signal or/and a session establishment request signal number of a predetermined monitoring period for every IP address to the aforementioned CA with the 1st counter,
A step among which a format and a parameter check of a monitoring period which exists for every IP address to the aforementioned CA count an unauthorized signal number with the 4th counter,
A step which judges IP address origin which became at the 1st aforementioned counter and one counter of the 4th counter beyond a threshold value to be DoS attack origin,
A ****(ing) DoS attack former detecting method.
[Claim 4]
In Claim 1 or a DoS attack former detecting method of a description to 2,
A format and a parameter check of a predetermined monitoring period for every IP address to the aforementioned CA further have a step which counts an unauthorized signal number with the 4th counter,

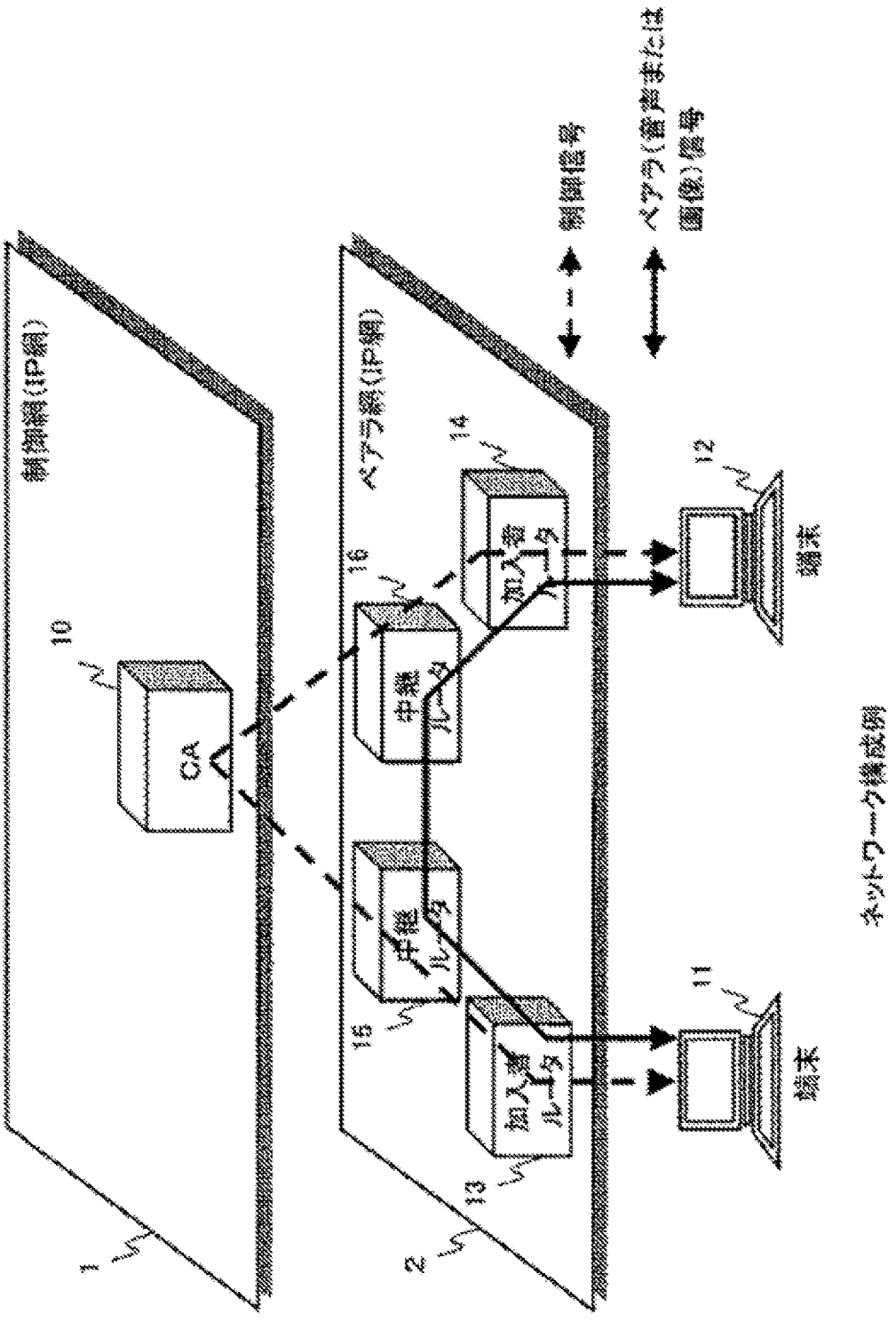
ERICSSON EXHIBIT 1005, Page 217

A DoS attack former detecting method judging IP address origin which became beyond a threshold value at one counter of said 1st counter, the 3rd counter, and the 4th counter to be DoS attack origin.
[Claim 5]
Session control equipment equipping any 1 item of Claims 1-4 with a function to realize a DoS attack former detecting method of a description.
[Claim 6]
A program for performing a function of the session control equipment according to claim 5 by computer.
[Claim 7]
A recording medium which recorded a program for performing a function of the session control equipment according to claim 5 by computer.
[Claim 8]
When a DoS attack is detected in a DoS attack former detecting method of a description in any 1 item of Claims 1-4, A step for which IP address information on DoS attack origin is notified to a router control device (the following, router OpS) while CA continues processing as it is in service under session control and a new session connection demand or a terminal registry request performs lockout processing refused by packet discarding,
A step which distributes a filtering restriction command to which the aforementioned router OpS chooses from IP address information a subscriber's router which has stored DoS attack origin, and discards a packet from the DoS attack origin to the subscriber's router,
A step to which the aforementioned subscriber's router discards a packet from DoS attack origin according to a filtering restriction command,
A ****(ing) DoS attack inhibition method.
[Claim 9]
A router control device provided with a function to realize a DoS attack inhibition method according to claim 8.
[Claim 10]
A program for performing a function of the router control device according to claim 9 by computer.
[Claim 11]
A recording medium which recorded a program for performing a function of the router control device according to claim 9 by computer.
[Claim 12]
When a DoS attack is detected in a DoS attack former detecting method of a description in any 1 item of Claims 1-4,
Service under session control continues processing as it is, and while a new session connection demand or a terminal registry request performs lockout processing refused by packet discarding, CA, A step which distributes a filtering restriction command which chooses from IP address information on DoS attack origin a subscriber's router which has stored DoS attack origin, and discards a packet from DoS attack origin to the subscriber's router,
A step to which the aforementioned subscriber's router discards a packet from DoS attack origin according to a filtering restriction command,
A ****(ing) DoS attack inhibition method.
[Claim 13]
Session control equipment provided with a function to realize a DoS attack inhibition method

according to claim 12.
[Claim 14]
A program for a computer to realize a function of the session control equipment according to claim 13.
[Claim 15]
A recording medium which recorded a program for a computer to realize a function of the session control equipment according to claim 13.

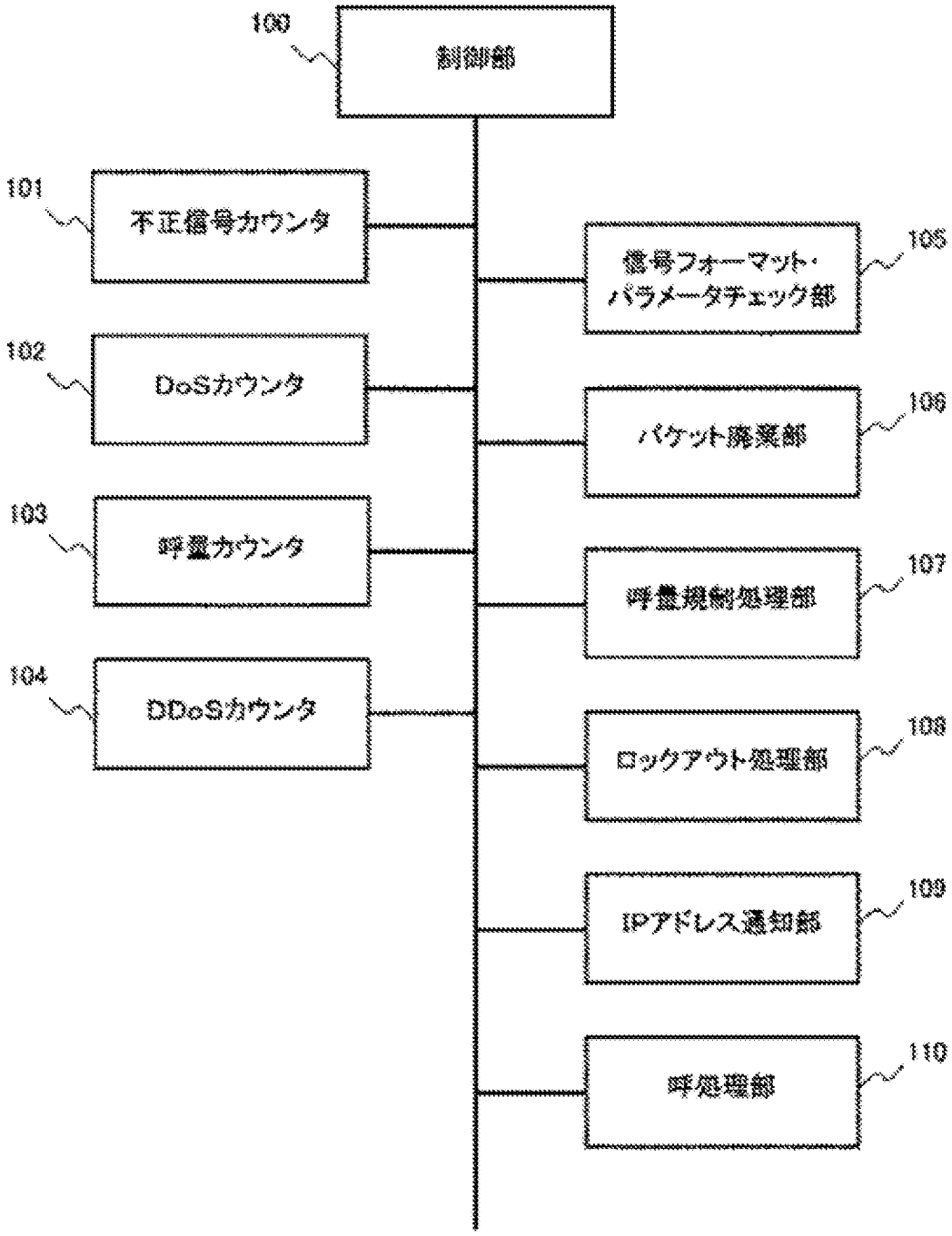
ERICSSON EXHIBIT 1005, Page 219

DRAWINGS



[Drawing 1]

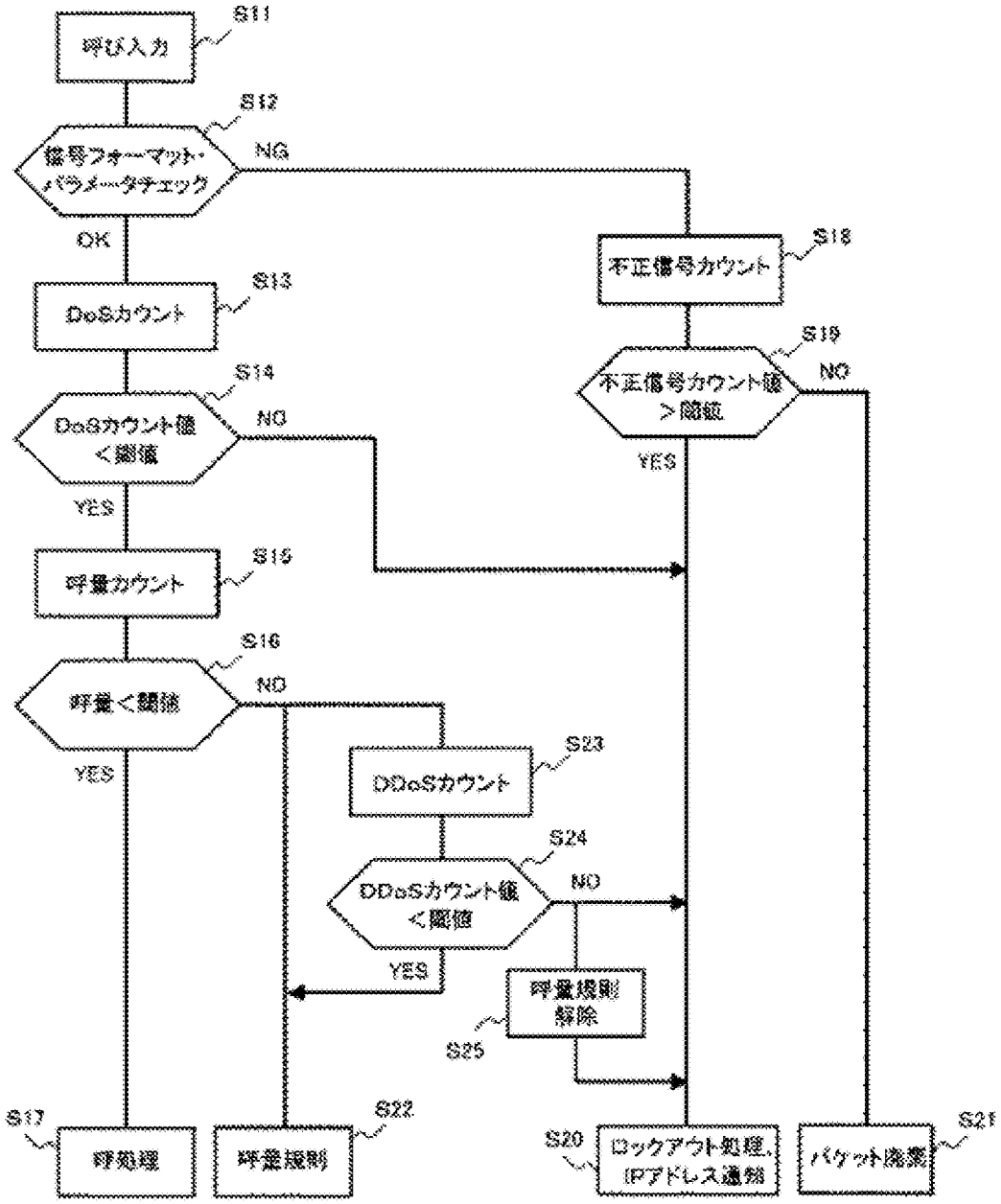
ERICSSON EXHIBIT 1005, Page 220



CAの構成例

[Drawing 2]

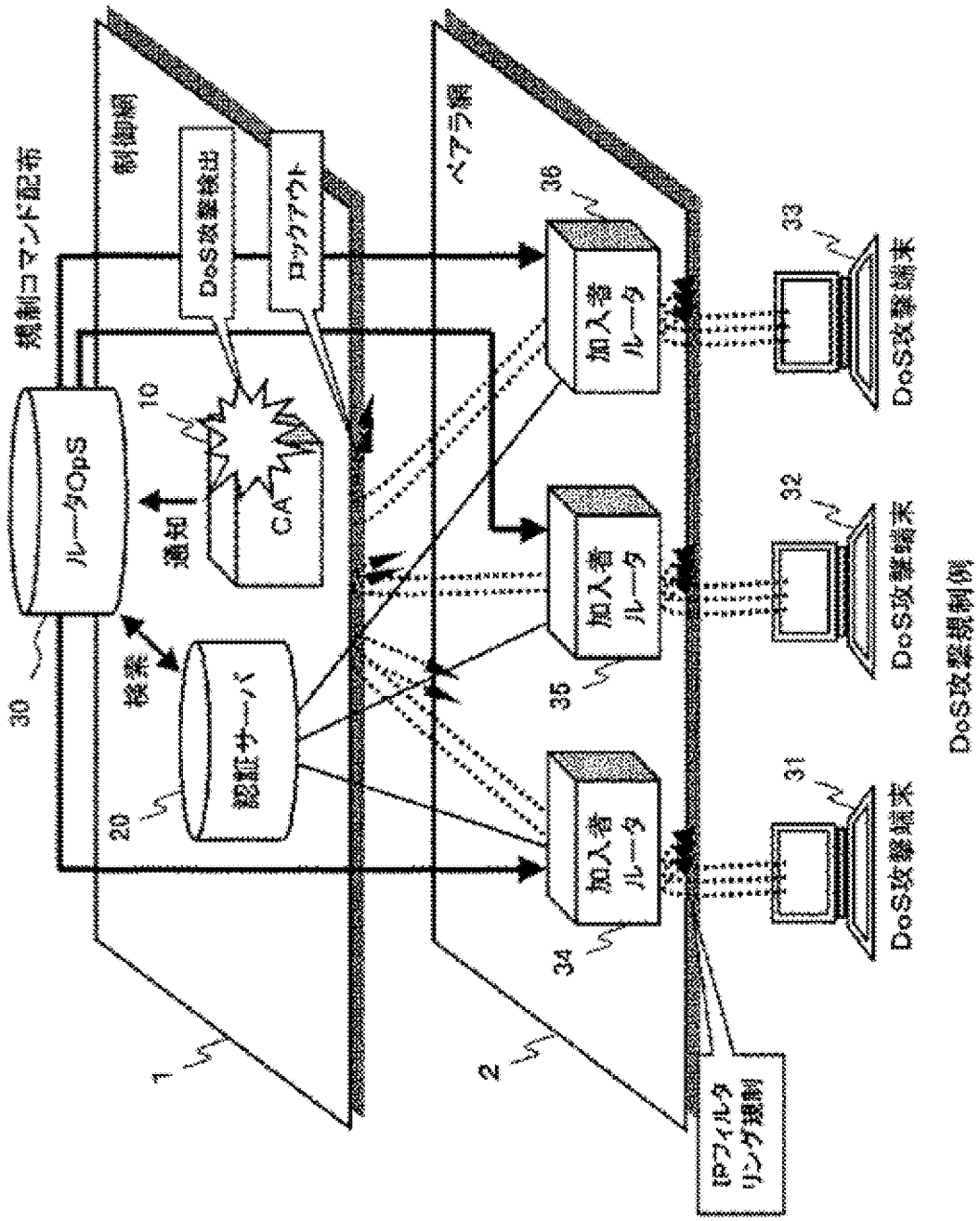
ERICSSON EXHIBIT 1005, Page 221



CA処理フロー例

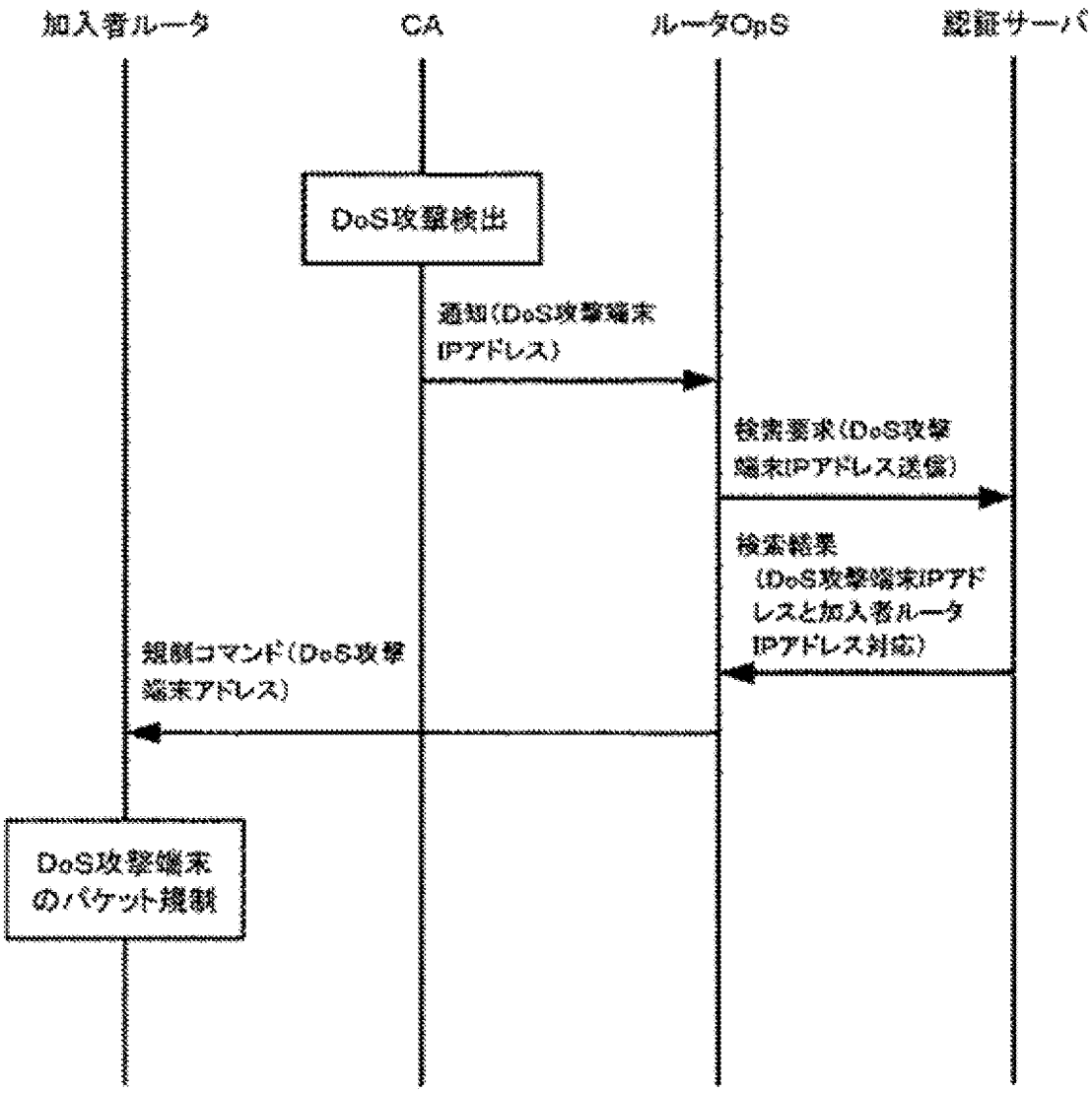
[Drawing 3]

ERICSSON EXHIBIT 1005, Page 222



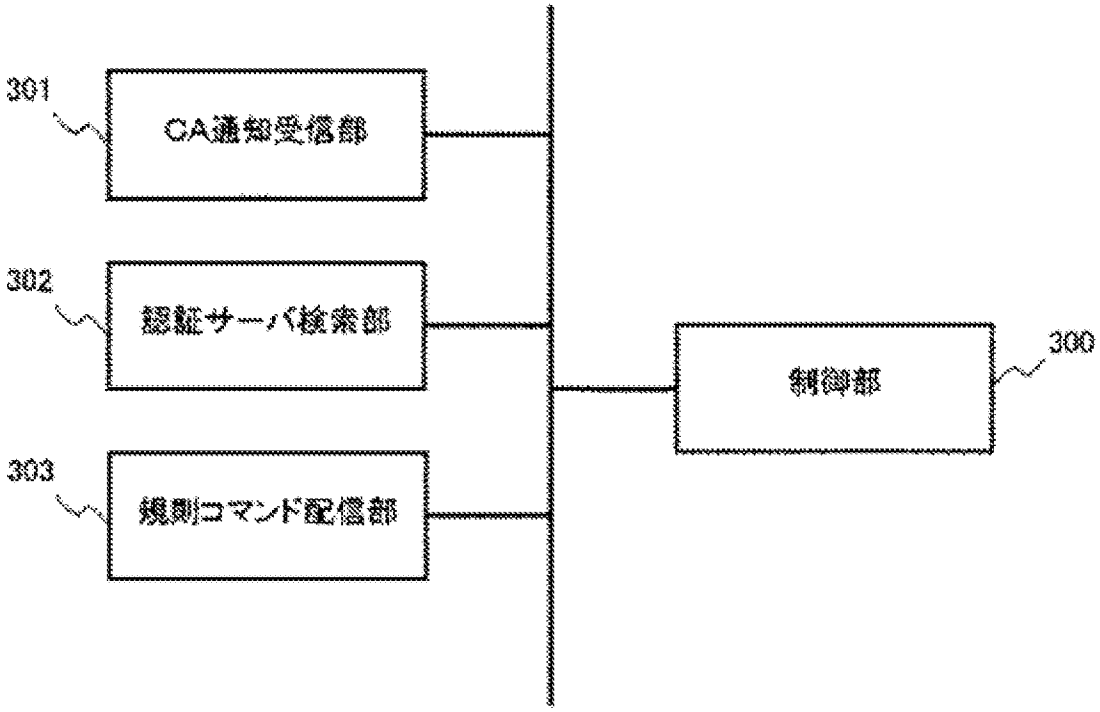
[Drawing 4]

ERICSSON EXHIBIT 1005, Page 223



DoS攻撃規制動作シーケンス例

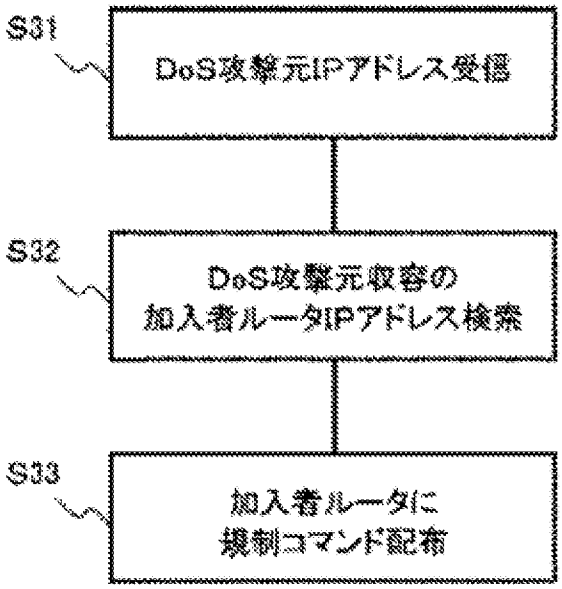
[Drawing 5]



ルータOpSの構成例

[Drawing 6]

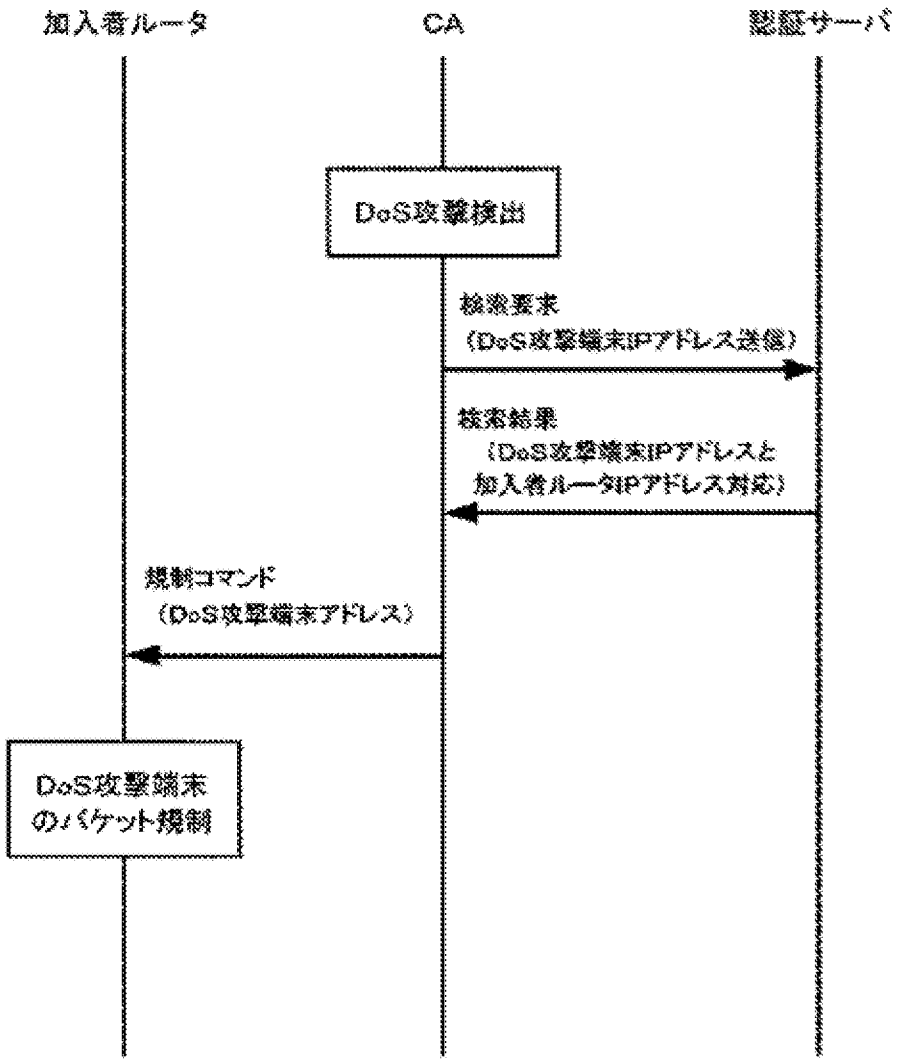
ERICSSON EXHIBIT 1005, Page 225



ルータOpSの処理フロー例

[Drawing 7]

ERICSSON EXHIBIT 1005, Page 226



DoS攻撃規制動作シーケンス例

[Drawing 8]

ERICSSON EXHIBIT 1005, Page 227

(11)Publication number	2006-295240
(43)Date of publication of application	26.10.2006
(51)Int.Cl.	*H04L 12/66 (2006.01)*
(21)Application number	2005-108983
(22)Date of filing	05.04.2005
(71)Applicant	MITSUBISHI ELECTRIC CORP
(72)Inventor	NATORI HIDEO

(54)COMMUNICATION APPARATUS, ADDRESS CONVERTER AND PROGRAM

(57)Abstract

PROBLEM TO BE SOLVED: To provide a distributed countermeasure against denial of service attack in which traffic of the entire network can be reduced by achieving a countermeasure against DDoS through NAT unit.
SOLUTION: A Firewall unit 2 and routers 3a, 3b, 6a, 6b, 6c transmit/receive camouflage ARP packet data incorporating encrypted data of setting/releasing conditions of a discard filter for limiting the transmission band of transmission data of terminals 4 and 7 performing DDoS attack of a defence object server 1 in an ARP packet, and set a filter by decrypting the encrypted data. When the discard filter is set in routers 6a, 6b, 6c being connected with a network B not on the server side 1, an NAT unit 5 generates and transmits camouflage ARP packet data where the address information of information about setting/releasing conditions of the discard filter is converted into the address system of the network B.

ERICSSON EXHIBIT 1005, Page 228

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

This invention relates to the communication apparatus, address conversion device, and program which perform distributed-denial-of-service-attacks measure processing in the Internet or IP-VPN.

[Background of the Invention]

[0002]

In the DDoS (Distributed Denial of Service) attack (it abbreviates to DDoS attack hereafter) measure processing in the conventional network system, If the Web server of a company, etc. receive a DDoS attack from the terminal of a user with bad faith, the communication apparatus (Firewall equipment is called hereafter) which has a Firewall function, for example will detect address information, such as an IP address of an attacking agency, and an operating port number. And Firewall equipment sends out an abandonment filter condition and its condition resolutive to the upper level router which adjoins based on the routing information of self-equipment at the same time it sets up an abandonment filter based on the detected address information.

[0003]

In a contiguity router, an abandonment filter condition and a condition resolutive are transmitted to an upper level router at the same time it sets an abandonment filter to self-equipment based on the setups of the received abandonment filter. By repeating this processing, an abandonment filter is set up to the router which has stored the terminal of an attacking agency. If the router of an endmost part judges that self-equipment has stored the DDoS attack person based on the received abandonment filter condition, as [that measure processing was made] it is not recognized by the aggressor, it will not be transmitted to the terminal of abandonment filter condition and its condition resolutive attack-origin.

[0004]

Thus, the packet by a DDoS attack is eliminated from on a network, and not only the server of a target of attack but the load of the whole network is reduced. Such conventional DDoS attack measure processing is disclosed, for example in the Patent document 1.

[0005]

[Patent document 1] JP,2003-283554,A

[Description of the Invention]

[Problem to be solved by the invention]

[0006]

When the computer for defense is attacked via NAT (Network Address Translation) equipment in the conventional DDoS attack measure processing from an attacking agency, Since the address information of the terminal of an attacking agency is converted to the address information of the network of the side which the computer for defense connects with NAT equipment, It cannot be distinguished whether the communication apparatus stored in self-equipment is a terminal which carries out a DDoS attack via NAT equipment, and whether the router which adjoins NAT equipment within the network of the side for defense is NAT equipment. For this reason, the router contiguous to NAT equipment does not transmit setting out and the condition resolutive of an abandonment filter. Thereby, rather than NAT equipment, DDoS measure processing was not made but the network on the terminal side of an attacking agency

had the problem that the traffic in other registered users' terminal will be affected by the load by a DDoS attack packet.

[0007]

In the former, since an abandonment filter condition and its condition resolutive are transmitted according to the routing information of self-equipment, Even if it is a network of an attack drawer back from NAT equipment as the communication path of NAT equipment and DDoS attack Sakima is unsymmetrical, DDoS attack measure processing may not become effective. The problem that other registered users' traffic was affected from NAT equipment by the load by a DDoS attack packet by this even if it is a network of an attack drawer back occurred.

[0008]

This invention was made in order to solve the above problems, and an object of invention is to acquire the communication apparatus, address conversion device, and program which can realize the measure against a DDoS attack through address conversion devices, such as NAT equipment, and can reduce the traffic of the whole network.

[Means for solving problem]

[0009]

A communication apparatus of the present invention is characterized by comprising:

A filter information generation part which generates information about setting out and a condition resolutive of a filter which restrict a transmission band of send data from a communication apparatus which carries out the distributed denial of service attacks of the computer for defense.

A filtering control part which sets up a filter based on information about setting out and a condition resolutive of a filter.

A filter information transmission and reception section which exchanges information about setting out and a condition resolutive of a filter among other communication apparatus containing an address conversion device linked to a network.

[Effect of the Invention]

[0010]

The filter information generation part which generates the information about setting out and the condition resolutive of a filter which restrict the transmission band of the send data from the communication apparatus which carries out the distributed denial of service attacks of the computer for defense according to this invention, The filtering control part which sets up a filter based on the information about setting out and the condition resolutive of a filter, Since it has a filter information transmission and reception section which exchanges the information about setting out and the condition resolutive of a filter among other communication apparatus containing the address conversion device linked to a network, From the information about setting out and the condition resolutive of a filter being acquirable also in an address conversion device, The measure against a DDoS attack between the networks with which addressing architectures differ is realized, and it is effective in the ability to inhibit the increase in the traffic resulting from the DDoS attack of these whole networks.

[Best Mode of Carrying Out the Invention]

[0011]

Embodiment 1.

ERICSSON EXHIBIT 1005, Page 230

Fig.1 is the figure showing the network system to which the distributed-denial-of-service-attacks measure method according to this embodiment of the invention 1 is applied. In the example shown in the figure, the two networks A and B are connected via the NAT equipment (address conversion device) 5, and the server device (computer for defense) 1 has connected via the Firewall equipment (communication apparatus) 2 into the network A. In this network A, the NAT equipment 5 is connected via the routers (communication apparatus) 3a and 3b from the Firewall equipment 2, and the terminal 4 other than the NAT equipment 5 is stored in the router 3b.

[0012]

This terminal 4 is a terminal of the bad faith user who becomes DDoS attack origin, and can carry out the DDoS attack of the server 1 on the connecting relation within the network A, without passing the NAT equipment 5. The routers (communication apparatus) 6a, 6b, and 6c connect with the network (other networks) B in order from the NAT equipment 5, and the terminal 7 is stored in the router 6c. This terminal 7 is a terminal of the bad faith user who becomes DDoS attack origin, and performs the DDoS attack which passed the NAT equipment 5 to the server 1 within the network A.

[0013]

Fig.2 is a block diagram showing the composition of the Firewall equipment by embodiment 1. As shown in the figure, the Firewall equipment 2, the DDoS attack primary detecting element 8, the abandonment / condition-resolutive generation part 9 (filter information generation part), the filtering control part 10, the routing table 11, and an encryption section (an encryption section --) It comprises the filter information transmission and reception section 12, the padding control part (filter information transmission and reception section) 13, the header control part (filter information transmission and reception section) 14, and the camouflage ARP generation part (a packet generation part, a filter information transmission and reception section) 15. The DDoS attack primary detecting element 8 receives the data to the server 1 in communication traffic, analyzes the existence of the DDoS packet, and detects address information, such as an IP address of DDoS attack origin, and an operating port number. Abandonment / condition-resolutive generation part 9 generates the information about setting out of the abandonment filter which restricts abandonment or its transmission band for the data transmitted from the attacking agency terminal specified by the address information concerned, and its condition resolutive based on the address information of the attack origin which the DDoS attack primary detecting element 8 detected.

[0014]

The filtering control part 10 sets an abandonment filter to the self-equipment 2 based on setting out of the abandonment filter which abandonment / condition-resolutive generation part 9 generated, and its condition resolutive. The routing table 11 is a table which stores the routing information which specifies the communication path on the network to the self-equipment 2 by address information etc., and is built on the memory of the computer which functions as the self-equipment 2. The encryption section 12 enciphers the information about setting out and its release of the abandonment filter which abandonment / condition-resolutive generation part 9 generated by DES, 3DES, etc.

[0015]

The padding control part 13 performs processing which builds data into the padding part of an ARP (Address Resolution Protocol) request. For example, if it is at the usual ARP request sending-out time, the data which enciphered invalid data is embedded as padding data, and is sent out. The header

ERICSSON EXHIBIT 1005, Page 231

control part 14 performs processing which builds into the header of an ARP request the destination IP addresses specified from the address information of the routing table 11. The camouflage ARP generation part 15 carries out capsuling of the encipherment information by the encryption section 12 to the padding part of an ARP request by the padding control part 13, generates the camouflage ARP request which built destination IP addresses into the header by the header control part 14, and sends it out to the router 3a.

[0016]

The DDoS attack primary detecting element 8, the abandonment / condition-resolutive generation part 9, the filtering control part 10, the encryption section 12, the padding control part 13, the header control part 14, and the camouflage ARP generation part 15 which were mentioned above, For example, it can embody by making the computer which mounted the function which communicates with an external device run the distributed-denial-of-service-attacks measure program according to the present invention.

[0017]

That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The function as the DDoS attack primary detecting element 8 which shows Fig.2, the abandonment / condition-resolutive generation part 9, the filtering control part 10, the encryption section 12, the padding control part 13, the header control part 14, and the camouflage ARP generation part 15 can be given on the computer concerned. The routing table 11 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.

[0018]

In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the Firewall equipment 2 of the present invention, A person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is omitted. The Firewall equipment 2 may be constituted as a separate communication apparatus in the network A, and may be provided as one function of the server 1.

[0019]

Fig.3 is a block diagram showing the composition of the router by embodiment 1. As shown in the figure, the routers 3a, 3b, 6a, 6b, and 6c, the ARP primary detecting element (a receive section, a filter information transmission and reception section) 16, the padding extraction part 17, and a decoding section (a decoding part --) the filter information transmission and reception section 18, the abandonment / condition-resolutive generation part 19 (filter information generation part), the filtering control part 20, the routing table 21, and an encryption section (an encryption section --) It comprises the filter information transmission and reception section 22, the padding control part (filter information transmission and reception section) 23, the header control part (filter information transmission and reception section) 24, and the camouflage ARP generation part (a packet generation part, a filter information transmission and reception section) 25. The ARP primary detecting element 16 receives the data transmitting from the communication apparatus which a self-router stores, and a Firewall equipment fork end besides the usual ARP request detects the camouflage ARP request from lower routers. The padding extraction part 17 extracts padding data from the padding part of the camouflage

ERICSSON EXHIBIT 1005, Page 232

ARP request which the ARP primary detecting element 16 detected. The decoding rule for decoding the data enciphered by the encryption section 12 of the Firewall equipment 2 is set up, and the decoding section 18 decodes padding data in accordance with this decoding rule.

[0020]

Abandonment / condition-resolutive generation part 19 detects the information about setting out and the condition resolutive of an abandonment filter from the data which the decoding section 18 decoded. The filtering control part 20 sets an abandonment filter to a self-router based on the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-resolutive generation part 19 detected. The routing table 21 is a table which stores the routing information which specifies the communication path on the network to a self-router by address information etc., and is built on the memory of the computer which functions as a self-router. The encryption section 22 enciphers the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-resolutive generation part 19 detected by DES, 3DES, etc.

[0021]

The padding control part 23 performs processing which builds data into the padding part of an ARP request. The header control part 24 performs processing which builds into the header of an ARP request the destination IP addresses specified from the address information of the routing table 21. The camouflage ARP generation part 25 carries out capsuling of the encipherment information by the encryption section 22 to the padding part of an ARP request by the padding control part 23, It sends out to the communication apparatus which generates the camouflage ARP request which built destination IP addresses into the header by the header control part 24, and a self-router stores.

[0022]

The ARP primary detecting element 16, the padding extraction part 17 and the decoding section 18 which were mentioned above, the abandonment / condition-resolutive generation part 19, the filtering control part 20, the encryption section 22, the padding control part 23, the header control part 24, and the camouflage ARP generation part 25, For example, it can embody by making the computer which mounted the function which communicates with an external device run the distributed-denial-of-service-attacks measure program according to the present invention.

[0023]

That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The function as the ARP primary detecting element 16 which shows Fig.3, the padding extraction part 17, the decoding section 18, the abandonment / condition-resolutive generation part 19, the filtering control part 20, the encryption section 22, the padding control part 23, the header control part 24, and the camouflage ARP generation part 25 can be given on the computer concerned. The routing table 21 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.

[0024]

In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the routers 3a, 3b, 6a, 6b, and 6c of the present invention, A person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is

ERICSSON EXHIBIT 1005, Page 233

omitted.
[0025]
Fig.4 is a block diagram showing the composition of the NAT equipment by embodiment 1. As shown in the figure, the NAT equipment 5, An ARP primary detecting element. (Receive section) 26, the padding extraction part 27, the decoding section 28, the abandonment / condition-resolutive generation part 29, the address conversion section 30, the NAT table 31, the attack side NW abandonment / condition-resolutive generation part 32, the filtering control part 33, the routing table 34, the encryption section 35, the padding control part 36, It comprises the header control part 37 and the camouflage ARP generation part (packet generation part) 38. The ARP primary detecting element 26 receives the data transmitting from lower routers, and detects the camouflage ARP request from lower routers besides the usual ARP request. The padding extraction part 27 extracts padding data from the padding part of the camouflage ARP request which the ARP primary detecting element 26 detected.
[0026]
The decoding section 28 decodes the padding data which the padding extraction part 27 extracted. Abandonment / condition-resolutive generation part 29 detects the information about setting out and its release of an abandonment filter from the data which the decoding section 28 decoded. The address conversion section 30 converts the network address system of the address information in the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-resolutive generation part 29 detected based on the NAT information on the NAT table 31. As for the NAT table 31, the NAT information as which the relation of the address information between the networks A and B described it is stored. Based on setting out and the condition resolutive of an abandonment filter which were converted to the network address system of DDoS attack origin by the address conversion section 30, attack side NW abandonment / condition-resolutive generation part 32, Setting out and the condition resolutive of the abandonment filter for setting to the communication apparatus on the network on the DDoS attack origin side are generated.
[0027]
The filtering control part 33 sets an abandonment filter to the self-equipment 5 based on the information about setting out and the condition resolutive of an abandonment filter which attack side NW abandonment / condition-resolutive generation part 32 generated. The routing table 34 is a table which stores the routing information which specifies the communication path on the network to the self-equipment 5 by address information etc., and is built on the memory of the computer which functions as the self-equipment 5. The encryption section 35 enciphers the information about setting out and its release of the abandonment filter which attack side NW abandonment / condition-resolutive generation part 32 generated by DES, 3DES, etc.
[0028]
The padding control part 36 performs processing which builds data into the padding part of an ARP request. The header control part 37 performs processing which builds into the header of an ARP request the destination IP addresses specified from the address information of the routing table 34. The camouflage ARP generation part 38 carries out capsuling of the encipherment information by the encryption section 35 to the padding part of an ARP request by the padding control part 36, generates the camouflage ARP request which built destination IP addresses into the header by the header control part 37, and sends it out to lower routers.

ERICSSON EXHIBIT 1005, Page 234

[0029]
It mentioned above, The ARP primary detecting element 26, the padding extraction part 27, the decoding section 28, the abandonment / condition-resolutive generation part 29, the address conversion section 30, the attack side NW abandonment / condition-resolutive generation part 32, the filtering control part 33, the encryption section 35, the padding control part 36, the header control part 37, and the camouflage ARP generation part 38, For example, it can embody by making the computer which mounted the function which communicates with an external device run the distributed-denial-of-service-attacks measure program according to the present invention.
[0030]
That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The ARP primary detecting element 26 which shows Fig.4 on the computer concerned, the padding extraction part 27, the decoding section 28, the abandonment / condition-resolutive generation part 29, the address conversion section 30, the attack side NW abandonment / condition-resolutive generation part 32, the filtering control part 33, the encryption section 35, the padding control part 36, The function as the header control part 37 and the camouflage ARP generation part 38 can be given. The NAT table 31 and the routing table 34 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.
[0031]
In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the NAT equipment 5 by the present invention, a person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is omitted.
[0032]
Next, it describes about operation.
The flow chart and Fig.6 in which operation according [Fig.5] to the Firewall equipment of embodiment 1 is shown, It is a flow chart which shows operation by the router of embodiment 1, and a flow chart which shows operation by the NAT equipment of embodiment 1, and describes the distributed-denial-of-service-attacks measure method according to embodiment 1 along with these figures.
[0033]
First, the case where the DDoS attack of the server 1 is carried out from the terminal 4 in the network A is described.
Packet information is received from communication traffic, a receive packet judges whether a predetermined attack detection condition is followed, and the DDoS attack primary detecting element 8 of the Firewall equipment 2 detects a DDoS attack (step ST1 of Fig.5). As an attack detection condition, for example, it specified preliminarily as a DDoS attack packet, information, including the attribute of data, a detection interval, etc., can be considered. When traffic coincides with this attack detection condition, it is recognized as the communication packet of this traffic being a DDoS attack packet.
[0034]
If a DDoS attack packet is detected, the DDoS attack primary detecting element 8 will analyze the contents, and will detect address information, such as an IP address of the terminal 4 of DDoS attack origin, and an operating port number (step ST2 of Fig.5). The address information of the detected attack

ERICSSON EXHIBIT 1005, Page 235

origin is outputted to abandonment / condition-resolutive generation part 9 from the DDoS attack primary detecting element 8. In abandonment / condition-resolutive generation part 9, it carries out based on the address information of the attack origin which the DDoS attack primary detecting element 8 detected, The information about setting out and the condition resolutive of the abandonment filter for restricting abandonment or its transmission band for the commo data from the terminal 4 specified by the address information concerned is generated (step ST3 of Fig.5).

[0035]

Then, abandonment / condition-resolutive generation part 9 sends out the information about setting out and the condition resolutive of an abandonment filter which were generated to the filtering control part 10 and the encryption section 12. In the filtering control part 10, an abandonment filter is set to the self-equipment 2 based on setting out of this abandonment filter, and a condition resolutive (step ST4 of Fig.5).

[0036]

Abandonment / condition-resolutive generation part 9 searches the IP address of the communication apparatus on the upper level side next hop from the routing table 11, and is taken as destination IP addresses (step ST5 of Fig.5). The encryption section 12 enciphers the information about setting out and the condition resolutive of the abandonment filter received from abandonment / condition-resolutive generation part 9 by DES, 3DES, etc., and sends it out to the padding control part 13 (step ST6 of Fig.5).

[0037]

The communication apparatus on the upper level side next hop, When the communication apparatus for a FIRITA ring has connected with a network directly, it is this communication apparatus itself, and when the communication apparatus for a FIRITA ring has connected with a network indirectly via a router, it is a router linked to the network "nearest to" the equipment concerned. For example, when the communication apparatus for a FIRITA ring is on the network of self-equipment 2 directly under, the address is determined as an address address.

[0038]

The information about setting out and the condition resolutive of an abandonment filter which were enciphered by the encryption section 12 is sent out to the padding control part 13 from the encryption section 12, and the destination IP addresses which searched the routing table 11 and were determined are sent out to the header control part 14. The camouflage ARP generation part 15 performs by this capsuling which includes the information about setting out and the condition resolutive of an abandonment filter in the padding part of an ARP request by the padding control part 13, Destination IP addresses are built into the header of an ARP request by the header control part 14, and a usual ARP request and data form generate the ARP request the same and camouflaged to the terminal of an attacking agency (step ST7 of Fig.5). Thus, the created camouflage ARP request is transmitted to the router 3a corresponding to destination IP addresses from the camouflage ARP generation part 15 (step ST8 of Fig.5).

[0039]

In the ARP primary detecting element 16 of the router 3a contiguous to the Firewall equipment 2, the packet information of the camouflage ARP request from the Firewall equipment 2 is received like the reception of the usual ARP request (step ST1a of Fig.6). The packet information concerning this camouflage ARP request is outputted to the padding extraction part 17 from the ARP primary detecting

ERICSSON EXHIBIT 1005, Page 236

element 16. In the padding extraction part 17, the code data built into the padding part of the packet information input from the ARP primary detecting element 16 is extracted (step ST2a of Fig.6). If the ARP request which the ARP primary detecting element 16 detected is a camouflage ARP request, the information about setting out and the condition resolutive of an abandonment filter which were included in the padding part and which were enciphered will be extracted, and it will be outputted to the decoding section 18.

[0040]

The decoding rule for decoding the data enciphered by the encryption section 12 of the Firewall equipment 2 in the decoding section 18. (For example, the decoding rule of the code by DES and 3DES) is set up, and the encoded data which the padding extraction part 17 extracted in accordance with this decoding rule is decoded, and it outputs to abandonment / condition-resolutive generation part 19 (step ST3a of Fig.6). In abandonment / condition-resolutive generation part 19, the information about setting out and the condition resolutive of an abandonment filter which were generated with the Firewall equipment 2 is detected from decode data (step ST4a of Fig.6). Then, abandonment / condition-resolutive generation part 19 sends out the information about setting out and the condition resolutive of an abandonment filter which were detected to the filtering control part 20 and the encryption section 22. In the filtering control part 20, the abandonment filter to the data from the terminal 4 is set as the self-equipment 3a based on setting out and the condition resolutive of an abandonment filter (step ST5a of Fig.6).

[0041]

Abandonment / condition-resolutive generation part 19 searches the IP address of the communication apparatus on the upper level side next hop from the routing table 21, and is taken as destination IP addresses (step ST6a of Fig.6). The destination IP addresses which searched the routing table 21 and were determined are sent out to the header control part 24. The encryption section 22 enciphers the information about setting out and the condition resolutive of the abandonment filter received from abandonment / condition-resolutive generation part 19 by DES, 3DES, etc., and sends it out to the padding control part 23 (step ST7a of Fig.6).

[0042]

The camouflage ARP generation part 25 performs capsuling which includes the information about setting out and the condition resolutive of an abandonment filter in the padding part of an ARP request by the padding control part 23, Destination IP addresses are built into the header of an ARP request by the header control part 24, and the ARP request by which a usual ARP request and data form were the same, and were camouflaged to the terminal of an attacking agency is generated (step ST8a of Fig.6). Thus, the created camouflage ARP request is transmitted to the router 3b corresponding to destination IP addresses from the camouflage ARP generation part 25 (step ST9a of Fig.6).

[0043]

If the packet information of a camouflage ARP request is received like the reception of the usual ARP request in the router 3b, Processing from step ST1a to step ST9a mentioned above is performed, and the camouflage ARP request which enciphered the information about setting out and the condition resolutive of an abandonment filter to the terminal 4 of an attacking agency, and carried out capsuling to the padding part is transmitted to the terminal 4 and the NAT equipment 5.

[0044]

ERICSSON EXHIBIT 1005, Page 237

In the terminal 4 of an attacking agency, since the information about setting out and the condition resolutive of an abandonment filter is camouflaged by the ARP request packet and also it is enciphered even if it receives a camouflage ARP request from the router 3b, it cannot distinguish from the usual ARP request. Thereby, the terminal 4 of an attacking agency does not recognize that DDoS attack measure processing was made.

[0045]

By thus, the thing for which capsuling of the encoded data of the information about setting out of an abandonment filter and its condition resolutive is carried out to the usual ARP request and the camouflage ARP request of the same data form, and it is transmitted to them when the terminal 4 on the network A is an attacking agency, DDoS attack measure processing can be validated between the communication apparatus in the network A which has a decoding section which decodes the encoded data of a camouflage ARP request.

[0046]

A camouflage ARP request is transmitted also to the communication apparatus on the network B via the NAT equipment 5, and it may be made to set up the abandonment filter to the terminal 4. In this case, the address conversion section 30 of the NAT equipment 5 mentioned below, The address information of the information about setting out of the abandonment filter which should be built into a camouflage ARP request, and its condition resolutive is converted to the addressing architecture of the network B which is not an attacking agency side, Attack side NW abandonment / condition-resolutive generation part 32 generates the information about setting out of the abandonment filter by this addressing architecture, and its condition resolutive.

[0047]

Next, the case where the DDoS attack of the server 1 is carried out via the NAT equipment 5 from the terminal 7 in the network B is described.

The DDoS attack to the server 1 through the NAT equipment 5 from the terminal 7 on the network B, It is detected by the DDoS attack primary detecting element 8 of the Firewall equipment 2, According to the processing shown in Fig.5, the camouflage ARP request to which capsuling of the encoded data of the information about setting out and the condition resolutive of the abandonment filter for restricting abandonment or its transmission band was carried out is generated, and the data of the terminal 7 is transmitted to the router 3a. In the routers 3a and 3b, a camouflage ARP request is generated according to the processing shown in Fig.6, and it transmits to the NAT equipment 5.

[0048]

In the ARP primary detecting element 26 of the NAT equipment 5, the packet information of a camouflage ARP request is received like the reception of the usual ARP request (step ST1b of Fig.7). The packet information concerning this camouflage ARP request is outputted to the padding extraction part 27 from the ARP primary detecting element 26. In the padding extraction part 27, the code data built into the padding part of the packet information input from the ARP primary detecting element 26 is extracted (step ST2b of Fig.7). If the ARP request which the ARP primary detecting element 26 detected is a camouflage ARP request, the information about setting out and the condition resolutive of an abandonment filter which were included in the padding part and which were enciphered will be extracted, and it will be outputted to the decoding section 28.

[0049]

ERICSSON EXHIBIT 1005, Page 238

The decoding rule for decoding the data enciphered by the encryption section 22 of the router 3b in the decoding section 28. (For example, the decoding rule of the code by DES and 3DES) is set up, and the encoded data which the padding extraction part 27 extracted is decoded, and it outputs to abandonment / condition-resolutive generation part 29 (step ST3b of Fig.7). In abandonment / condition-resolutive generation part 29, the information about setting out and the condition resolutive of an abandonment filter is detected from decode data (step ST4b of Fig.7). Then, abandonment / condition-resolutive generation part 29 sends out the information about setting out and the condition resolutive of an abandonment filter which were detected to the address conversion section 30.

[0050]

The address conversion section 30 converts the address information in the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-resolutive generation part 29 detected based on the NAT information on the NAT table 31 to the addressing architecture of the network B with which the terminal 7 of an attacking agency exists (step ST5b of Fig.7). This conversion information is sent out to attack side NW abandonment / condition-resolutive generation part 32 from the address conversion section 30. In attack side NW abandonment / condition-resolutive generation part 32, based on setting out and the condition resolutive of the abandonment filter with which the addressing architecture was converted to the network B by the address conversion section 30 from the network A, Setting out and the condition resolutive of the abandonment filter for setting to the communication apparatus on the network B are generated (step ST6b of Fig.7).

[0051]

In the filtering control part 33, the abandonment filter to the data from the terminal 7 is set as the self-equipment 5 based on setting out and the condition resolutive of the abandonment filter from attack side NW abandonment / condition-resolutive generation part 32 (step ST7b of Fig.7). Abandonment / condition-resolutive generation part 29 searches the IP address of the communication apparatus on the upper level side next hop from the routing table 34, and is taken as destination IP addresses (step ST8b of Fig.7). The destination IP addresses which searched the routing table 34 and were determined are sent out to the header control part 37. The encryption section 35 enciphers the information about setting out and the condition resolutive of the abandonment filter received from abandonment / condition-resolutive generation part 29 by DES, 3DES, etc., and sends it out to the padding control part 36 (step ST9b of Fig.7).

[0052]

The camouflage ARP generation part 38 performs capsuling which includes the information about setting out and the condition resolutive of an abandonment filter in the padding part of an ARP request by the padding control part 36, Destination IP addresses are built into the header of an ARP request by the header control part 37, and the ARP request by which a usual ARP request and data form were the same, and were camouflaged to the terminal of an attacking agency is generated (step ST10b of Fig.7). Thus, the created camouflage ARP request is transmitted to the router 6a on the network B corresponding to destination IP addresses from the camouflage ARP generation part 38 (step ST11b of Fig.7).

[0053]

Henceforth, the same processing as the routers 3a and 3b is performed with the routers 6a, 6b, and 6c. Thereby, even if it is a case where the DDoS attack of the server 1 is carried out via the NAT equipment 5

ERICSSON EXHIBIT 1005, Page 239

from the terminal 7 in the network B, an abandonment filter can be set to the communication apparatus on the networks A and B, and the measure against a DDoS attack can be validated. The Firewall equipment 2, the routers 3a and 3b, the NAT equipment 5, and the routers 6a, 6b, and 6c release the set-up abandonment filter, when the condition resolutive set up considering the camouflage ARP request as a medium is satisfied.

[0054]

As mentioned above, according to this embodiment 1, the Firewall equipment 2 and the routers 3a, 3b, 6a, 6b, and 6c, The camouflage ARP packet information which built into the ARP packet setting out of an abandonment filter and the encoded data of a condition resolutive which restrict the transmission band of the send data of the terminals 4 and 7 which carry out the DDoS attack of the server 1 for defense is exchanged, In decoding encoded data, setting up a filter and setting to the routers 6a, 6b, and 6c with which the NAT equipment 5 connects an abandonment filter to the network B which is not the server 1 side, Since the camouflage ARP packet information which converted the address information of the information about setting out and the condition resolutive of an abandonment filter to the addressing architecture of the network B is generated and it transmits, When the terminal 4 in the network A with which the server 1 of a target of attack exists is DDoS attack origin, it cannot make it able to recognize that DDoS attack measure processing was made, but can validate this. Even if it is a case where the terminal 7 on the network B through the NAT equipment 5 is DDoS attack origin, Setting out of an abandonment filter and transmission of a condition resolutive are attained over the NAT equipment 5 at the routers 6a, 6b, and 6c of the network B, and the DDoS attack packet from the terminal 7 can be eliminated also from on the network B. By this, the measure against a DDoS attack can be realized, the traffic of the whole network can be reduced, and it becomes possible to lower these loads.

[0055]

Although the case where the DDoS attack by the terminal 4 on the network A and the DDoS attack by the terminal 7 on the network B were made separate was described in the above-mentioned embodiment 1, Even if it is a case where the attacking agency terminal of both networks performs a DDoS attack simultaneously, DDoS attack measure processing can be validated by setting up the abandonment filter by the camouflage ARP request mentioned above in the networks A and B.

[0056]

Embodiment 2.

By the above-mentioned embodiment 1, after enciphering setting out and the condition resolutive of an abandonment filter, the example which implements the measure against a DDoS attack by carrying out capsuling to an ARP request packet, and transmitting to an upper level router was shown, but. The encryption and decoding processing of information about an abandonment filter are needed to all the communication apparatus in a network. For this reason, in order expensive apparatus with encryption and an indispensable decoding processing function is required or for all the communication apparatus to perform encryption and decoding processing, the processing performance of the whole network may fall.

[0057]

Then, the router 3b is made to recognize the address of NAT equipment in this embodiment 2 by embedding the code which shows that it is from the NAT equipment 5 to the padding region of the ARP request packet from the NAT equipment 5, and an ARP reply packet. Setting out and the condition

ERICSSON EXHIBIT 1005, Page 240

resolutive of the abandonment filter between communication apparatus are transmitted with an SNMP (Simple Network Management Protocol) protocol etc., without enciphering. Only when the address of the information about setting out and the condition resolutive of an abandonment filter is a thing addressed to NAT equipment 5, the router 3b contiguous to the NAT equipment 5, The information concerned is sent out to the NAT equipment 5 (if setting out of an abandonment filter and the address of a condition resolutive are not the things of the NAT equipment 5, they send nothing out).

[0058]

Fig.8 is the figure showing the network system to which the distributed-denial-of-service-attacks measure method according to this embodiment of the invention 2 is applied. Like the Fig.1 described by the above-mentioned embodiment 1, the two networks A and B are connected via the NAT equipment 5, and the server device (computer for defense) 1 has connected the example shown in Fig.8 via the Firewall equipment (communication apparatus) 2 into the network A. In this network A, the NAT equipment 5 is connected via the routers (communication apparatus) 3a and 3b from the Firewall equipment 2, and the terminal 4 other than the NAT equipment 5 is stored in the router 3b. The routers (communication apparatus) 6a, 6b, and 6c connect with the network (other networks) B in order from the NAT equipment 5, and the terminal 7 is stored in the router 6c.

[0059]

Fig.9 is a block diagram showing the composition of the Firewall equipment by embodiment 2. As shown in the figure, the Firewall equipment 2, It comprises the DDoS attack primary detecting element 39, the abandonment / condition-resolutive generation part 40 (filter information generation part), the filtering control part 41, the routing table 42, the header control part 43, and the abandonment / condition-resolutive report packet generation part 44 (a filter information reporting part, a filter information transmission and reception section). The DDoS attack primary detecting element 39 receives the data to the server 1 in communication traffic like the above-mentioned embodiment 1, analyzes the existence of the DDoS packet, and detects address information, such as an IP address of DDoS attack origin, and an operating port number. Abandonment / condition-resolutive generation part 40 generates the information about setting out and the condition resolutive of the abandonment filter for restricting abandonment or its transmission band for the data transmitted from the attacking agency terminal specified by the address information concerned based on the address information of the attack origin which the DDoS attack primary detecting element 39 detected.

[0060]

The filtering control part 41 sets an abandonment filter to the self-equipment 2 based on setting out of the abandonment filter which abandonment / condition-resolutive generation part 40 generated, and its condition resolutive. The routing table 42 is a table which stores the routing information which specifies the communication path on the network to the self-equipment 2 by address information etc., and is built on the memory of the computer which functions as the self-equipment 2. The header control part 43 performs processing which builds the destination IP addresses specified from the address information of the routing table 42 into the header of the abandonment / condition-resolutive report packet which abandonment / condition-resolutive report packet generation part 44 generates. Abandonment / condition-resolutive report packet generation part 44 generates the abandonment / condition-resolutive report packet which expressed with the SNMP protocol etc. the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-

ERICSSON EXHIBIT 1005, Page 241

resolutive generation part 40 generated.
[0061]
The Firewall equipment 2 mentioned above the DDoS attack primary detecting element 39, the abandonment / condition-resolutive generation part 40, the filtering control part 41, the header control part 43, and the abandonment / condition-resolutive report packet generation part 44, For example, it can embody by making the computer which mounted the function which communicates with an external device run the distributed-denial-of-service-attacks measure program according to the present invention.
[0062]
That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The Firewall equipment 2 shown in Fig.9 on the computer concerned can give the function as the DDoS attack primary detecting element 39, the abandonment / condition-resolutive generation part 40, the filtering control part 41, the header control part 43, and the abandonment / condition-resolutive report packet generation part 44. The routing table 42 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.
[0063]
In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the Firewall equipment 2 of the present invention, A person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is omitted. The Firewall equipment 2 may be constituted as a separate communication apparatus in the network A, and may be provided as one function of the server 1.
[0064]
Fig.10 is a block diagram showing the composition of the router by embodiment 2, and shows the composition of the routers 3a, 6a, 6b, and 6c excluding the router 3b which adjoins the NAT equipment 5 on the network A on the server 1 side used as a target of attack. As shown in the figure, the routers 3a, 6a, 6b, and 6c, It comprises abandonment / the condition-resolutive report packet receive section 45, the abandonment / condition-resolutive generation part 46 (filter information generation part), the filtering control part 47, the routing table 48, the header control part 49, and the abandonment / condition-resolutive report packet generation part 50 (filter information reporting part). Abandonment / condition-resolutive report packet receive section 45 receives the packet information from the communication apparatus which a self-router stores. Abandonment / condition-resolutive generation part 46 detects the information about setting out and its release of an abandonment filter from the packet which the packet receive section 45 received.
[0065]
The filtering control part 47 sets an abandonment filter to a self-router based on setting out of the abandonment filter which abandonment / condition-resolutive generation part 46 detected, and its condition resolutive. The routing table 48 is a table which stores the routing information which specifies the communication path on the network to a self-router by address information etc., and is built on the memory of the computer which functions as a self-router. The header control part 49 performs processing which builds into the header of an ARP request the destination IP addresses specified from

ERICSSON EXHIBIT 1005, Page 242

the address information of the routing table 48. Abandonment / condition-resolutive report packet generation part 50 is sent out to the communication apparatus which generates the abandonment / condition-resolutive report packet by which the header control part 49 built destination IP addresses into the header for the information from abandonment / condition-resolutive generation part 46 with the SNMP protocol etc., and a self-router stores.

[0066]

The abandonment / condition-resolutive report packet receive section 45, the abandonment / condition-resolutive generation part 46, the filtering control part 47, the header control part 49, and the abandonment / condition-resolutive report packet generation part 50 mentioned above, For example, it can embody by making the computer which mounted the function which communicates with an external device run the distributed-denial-of-service-attacks measure program according to the present invention.

[0067]

That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The function as the abandonment / condition-resolutive report packet receive section 45 which shows Fig.10, the abandonment / condition-resolutive generation part 46, the filtering control part 47, the header control part 49, and the abandonment / condition-resolutive report packet generation part 50 can be given on the computer concerned. The routing table 48 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.

[0068]

In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the routers 3a, 6a, 6b, and 6c of the present invention, A person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is omitted.

[0069]

Fig.11 is a block diagram showing the composition of the router by embodiment 2, and shows the composition of the router 3b which adjoins the NAT equipment 5 on the network A on the server 1 side of a target of attack. As shown in the figure, the router 3b, Abandonment / condition-resolutive report packet receive section 45, the abandonment / condition-resolutive primary detecting element 51, the ARP receive section (receive section) 52, the decoding part 53, the equipment type code primary detecting element 55, the equipment classification table 56, the filtering control part 57, the abandonment / condition-resolutive generation part 58 (filter information generation part), It comprises the routing table 59, the header control part 60, and the abandonment / condition-resolutive report packet generation part 61 (filter information reporting part). Abandonment / condition-resolutive report packet receive section 45 receives the packet information from the communication apparatus which a self-router stores. Abandonment / condition-resolutive primary detecting element 51 detects the information about setting out and its release of an abandonment filter from the packet which the packet receive section 45 received.

[0070]

The ARP receive section 52 receives the data transmitting from the communication apparatus which a self-router stores, and detects the camouflage ARP request from the NAT equipment 5 besides the usual

ARP request. The decoding rule for decoding the data enciphered by the encryption section 69 of the NAT equipment 5 is set up, and the decoding part 53 decodes the padding data of a camouflage ARP request in accordance with this decoding rule. The equipment type code primary detecting element 55 detects the information about the equipment classification of an opposite unit from the padding data of the camouflage ARP request decoded by the decoding part 53. The equipment classification table 56 is a table where the IP address of the NAT equipment 5 is stored, and when opposite unit classification is NAT equipment, the IP address of the opposite unit detected from the camouflage ARP request is registered. The filtering control part 57 sets an abandonment filter to a self-router based on setting out of the abandonment filter which abandonment / condition-resolutive primary detecting element 51 detected, and its condition resolutive.

[0071]

Abandonment / condition-resolutive generation part 58 searches the routing table 59 based on setting out of the abandonment filter which abandonment / condition-resolutive primary detecting element 51 detected, and its condition resolutive, and generates the information about setting out/condition resolutive of the abandonment filter addressed to an upper level next hop address. The routing table 59 is a table which stores the routing information which specifies the communication path on the network to a self-router by address information, and is built on the memory of the computer which functions as a self-router. The header control part 60 performs processing which builds into the header of an ARP request the destination IP addresses specified from the address information of the routing table 59. Abandonment / condition-resolutive report packet generation part 61 embeds the information from abandonment / condition-resolutive generation part 58 to a padding region, and sends it out to the communication apparatus which generates the abandonment / condition-resolutive report packet which built destination IP addresses into the header by the header control part 60, and a self-router stores.

When the abandonment/release information received by abandonment / condition-resolutive report packet are registered into the equipment classification table by the address information which is carrying out direct housing to self-equipment, regard it as NAT equipment, and transmit abandonment / condition-resolutive report packet, but. When not registering with an equipment classification registration table, it is regarded as a DDoS attack person and nothing is transmitted.

[0072]

The abandonment / condition-resolutive report packet receive section 45 which mentioned above, the abandonment / condition-resolutive primary detecting element 51, the ARP receive section 52, the decoding part 53, the equipment type code primary detecting element 55, the filtering control part 57, the abandonment / condition-resolutive generation part 58, the header control part 60, and the abandonment / condition-resolutive report packet generation part 61, For example, it can embody by making the computer which mounted the function which communicates with an external device run the distributed-denial-of-service-attacks measure program according to the present invention.

[0073]

That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The abandonment / condition-resolutive report packet receive section 45 which shows Fig.11 on the computer concerned, the abandonment / condition-resolutive primary detecting element 51, the ARP receive section 52, the

ERICSSON EXHIBIT 1005, Page 244

decoding part 53, the equipment type code primary detecting element 55, the filtering control part 57, the abandonment / condition-resolutive generation part 58, the header control part 60. And the function as abandonment / condition-resolutive report packet generation part 61 can be given. The equipment classification table 56 and the routing table 59 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.

[0074]

In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the router 3b of the present invention, a person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is omitted.

[0075]

Fig.12 is a block diagram showing the composition of the NAT equipment by embodiment 2. As shown in the figure, the NAT equipment 5, Abandonment / condition-resolutive report packet receive section 62, the abandonment / condition-resolutive primary detecting element 63, the address conversion section 64, the attack side NW abandonment / condition-resolutive generation part 65 (filter information generation part), the NAT table 66, the routing table 67, the equipment type code generation part 68, the encryption section 69, It comprises the camouflage ARP generation part 70, the filtering control part 71, the header control part 72, and the abandonment / condition-resolutive report packet generation part 73 (filter information reporting part). Abandonment / condition-resolutive report packet receive section 62 receives the packet information from the communication apparatus which the self-equipment 5 stores. Abandonment / condition-resolutive primary detecting element 63 detects the information about setting out and its release of an abandonment filter from the packet which the packet receive section 62 received. The address conversion section 64 converts the network address system of the address information in the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-resolutive primary detecting element 63 detected based on the NAT information on the NAT table 66.

[0076]

Based on setting out of the abandonment filter converted to the network address system of DDoS attack origin by the address conversion section 64, and its condition resolutive, attack side NW abandonment / condition-resolutive generation part 65, Setting out and the condition resolutive of the abandonment filter for setting to the communication apparatus on the network on the DDoS attack origin side are generated. As for the NAT table 66, the NAT information as which the relation of the address information between the networks A and B described it is stored. The routing table 67 is a table which stores the routing information which specifies the communication path on the network to the self-equipment 5 by address information etc., and is built on the memory of the computer which functions as the self-equipment 5. The equipment type code generation part 68 will generate the equipment type code which identifies that it is the self-equipment 5, if the ARP request to the self-equipment 5 is received.

[0077]

The encryption section 69 enciphers the equipment type code for making the self-equipment 5 which the equipment type code generation part 68 generated identify by DES, 3DES, etc. The camouflage ARP generation part 70 carries out capsuling of the equipment type code enciphered by the encryption

ERICSSON EXHIBIT 1005, Page 245

section 69 to the padding part of an ARP request packet and an ARP reply packet, and sends it out to lower routers. The filtering control part 71 sets an abandonment filter to the self-equipment 5 based on setting out of the abandonment filter which attack side NW abandonment / condition-resolutive generation part 65 generated, and its condition resolutive.

[0078]

The header control part 72 performs processing which builds into the header of an ARP request packet or an ARP reply packet the destination IP addresses specified from the address information of the routing table 67. Abandonment / condition-resolutive report packet generation part 73 embeds the information from attack side NW abandonment / condition-resolutive generation part 65 to a padding region, and sends it out to the communication apparatus which generates the abandonment / condition-resolutive report packet which built destination IP addresses into the header by the header control part 72, and a self-router stores.

[0079]

It mentioned above, Abandonment / condition-resolutive report packet receive section 62, the abandonment / condition-resolutive primary detecting element 63, the address conversion section 64, the attack side NW abandonment / condition-resolutive generation part 65, the equipment type code generation part 68, the encryption section 69, the camouflage ARP generation part 70, the filtering control part 71, the header control part 72. And abandonment / condition-resolutive report packet generation part 73 can be embodied by making the computer which mounted the function which communicates with an external device, for example run the distributed-denial-of-service-attacks measure program according to the present invention.

[0080]

That is, by making the distributed-denial-of-service-attacks measure program according to the present invention read into the above-mentioned computer, and controlling the operation, The abandonment / condition-resolutive report packet receive section 62 which shows Fig.12 on the computer concerned, the abandonment / condition-resolutive primary detecting element 63, the address conversion section 64, the attack side NW abandonment / condition-resolutive generation part 65, the equipment type code generation part 68, the encryption section 69, the camouflage ARP generation part 70, the filtering control part 71, The function as the header control part 72, and the abandonment / condition-resolutive report packet generation part 73 can be given. The NAT table 66 and the routing table 67 can also constitute on memory storage, such as a hard disk with which the above-mentioned computer was equipped.

[0081]

In the following descriptions, about the composition and its fundamental function of the computer itself which embodies the NAT equipment 5 of the present invention, a person skilled in the art can recognize easily based on the technical common knowledge of the technical field concerned, and since it is not directly concerned with the essence of the present invention, a detailed description is omitted.

[0082]

Next, it describes about operation.

Fig.13 is a flow chart which shows operation of the Firewall equipment in Fig.9. Fig.14 is a flow chart which shows operation of the router in Fig.10, Fig.15 is a flow chart which shows the operation in Fig.11 according [the flow chart and Fig.16 in which operation of a router is shown] to the NAT equipment in

ERICSSON EXHIBIT 1005, Page 246

Fig.12, and it describes the distributed-denial-of-service-attacks measure method according to embodiment 2 along with these figures.

[0083]

First, the case where the DDoS attack of the server 1 is carried out from the terminal 4 in the network A is described.

Packet information is received from communication traffic, a receive packet judges whether a predetermined attack detection condition is followed, and the DDoS attack primary detecting element 39 of the Firewall equipment 2 detects a DDoS attack (step ST1c of Fig.13). As an attack detection condition, for example, it specified preliminarily as a DDoS attack packet, information, including the attribute of data, a detection interval, etc., can be considered. When traffic coincides with this attack detection condition, it is recognized as the communication packet of this traffic being a DDoS attack packet.

[0084]

If a DDoS attack packet is detected, the DDoS attack primary detecting element 39 will analyze the contents, and will detect address information, such as an IP address of the terminal 4 of DDoS attack origin, and an operating port number (step ST2c of Fig.13). The address information of the detected attack origin is outputted to abandonment / condition-resolutive generation part 40 from the DDoS attack primary detecting element 39. In abandonment / condition-resolutive generation part 40, it carries out based on the address information of the attack origin which the DDoS attack primary detecting element 39 detected, The information about setting out and the condition resolutive of the abandonment filter for restricting abandonment or its transmission band for the commo data from the terminal 4 specified by the address information concerned is generated (step ST3c of Fig.13).

[0085]

Then, abandonment / condition-resolutive generation part 40 sends out the information about setting out and the condition resolutive of an abandonment filter which were generated to the filtering control part 41, and the abandonment / condition-resolutive report packet generation part 44. In the filtering control part 41, an abandonment filter is set to the self-equipment 2 based on setting out of this abandonment filter, and a condition resolutive (step ST4c of Fig.13).

[0086]

Abandonment / condition-resolutive generation part 40 searches the IP address of the communication apparatus on the upper level side next hop from the routing table 42, and is taken as destination IP addresses (step ST5c of Fig.13). The communication apparatus on the upper level side next hop, When the communication apparatus for a FIRITA ring has connected with a network directly, it is this communication apparatus itself, and when the communication apparatus for a FIRITA ring has connected with a network indirectly via a router, it is a router linked to the network "nearest to" the equipment concerned.

[0087]

For example, when the communication apparatus for a FIRITA ring is on the network of self-equipment 2 directly under, the address is determined as an address address. The destination IP addresses which searched the routing table 42 and were determined are sent out to the header control part 43.

[0088]

Abandonment / condition-resolutive report packet generation part 44 builds destination IP addresses

ERICSSON EXHIBIT 1005, Page 247

into a header by the header control part 43, The abandonment / condition-resolutive report packet which expressed the information about setting out and the condition resolutive of the abandonment filter from abandonment / condition-resolutive generation part 40 with the usual management protocol under TCP/IP network environments, such as an SNMP protocol, without enciphering are generated (step ST6c of Fig.13). This abandonment / condition-resolutive report packet are transmitted to the router 3a corresponding to destination IP addresses from abandonment / condition-resolutive report packet generation part 44 (step ST7c of Fig.13).

[0089]

In abandonment / condition-resolutive report packet receive section 45 of the router 3a contiguous to the Firewall equipment 2, the abandonment / condition-resolutive report packet information from the Firewall equipment 2 are received like the usual packet information reception (step ST1d of Fig.14). In abandonment / condition-resolutive generation part 46, the information about setting out and the condition resolutive of an abandonment filter is extracted from the packet information of the SNMP protocol input from the packet receive section 45. Then, abandonment / condition-resolutive generation part 46 sends out the information about setting out of an abandonment filter, and its condition resolutive to the filtering control part 47, and the abandonment / condition-resolutive report packet generation part 50. In the filtering control part 47, the abandonment filter to the data from the terminal 4 is set as the self-equipment 3a based on setting out and the condition resolutive of an abandonment filter (step ST2d of Fig.14).

[0090]

Abandonment / condition-resolutive generation part 46 searches the IP address of the communication apparatus on the upper level side next hop from the routing table 48, and is taken as destination IP addresses (step ST3d of Fig.14). The destination IP addresses which searched the routing table 48 and were determined are sent out to the header control part 49. Abandonment / condition-resolutive report packet generation part 50 builds destination IP addresses into a header by the header control part 49, The abandonment / condition-resolutive report packet which expressed the information about setting out and the condition resolutive of the abandonment filter from abandonment / condition-resolutive generation part 46 with the usual management protocol under TCP/IP network environments, such as an SNMP protocol, without enciphering are generated (step ST4d of Fig.14). This abandonment / condition-resolutive report packet are transmitted to the router 3b corresponding to destination IP addresses from abandonment / condition-resolutive report packet generation part 50 (step ST5d of Fig.14).

[0091]

Abandonment / condition-resolutive report packet receive section 45 of the router 3b which adjoins the NAT equipment 5 on the network A on the server 1 side receive the abandonment / condition-resolutive report packet information from the router 3a like the usual packet information reception (step ST1e of Fig.15). In abandonment / condition-resolutive primary detecting element 51, the information about setting out and the condition resolutive of an abandonment filter is detected from the packet information of the SNMP protocol input from the packet receive section 45. Then, abandonment / condition-resolutive primary detecting element 51 sends out the information about setting out of an abandonment filter, and its condition resolutive to the filtering control part 57, and the abandonment / condition-resolutive generation part 58. In the filtering control part 57, the abandonment filter to the

ERICSSON EXHIBIT 1005, Page 248

data from the terminal 4 is set as the self-equipment 3b based on setting out and the condition resolutive of an abandonment filter (step ST2e of Fig.15).

[0092]

In the ARP receive section 52, the packet information of camouflage ARP from the NAT equipment 5 is received like the reception of the usual ARP (step ST3e of Fig.15). Then, the ARP receive section 52 detects the code data built into the padding part of the packet information of received camouflage ARP (step ST4e of Fig.15). The decoding rule for decoding the data enciphered by the encryption section 69 of the NAT equipment 5 in the decoding part 53. (For example, the decoding rule of the code by DES and 3DES) is set up, and the encoded data which the ARP receive section 52 extracted in accordance with this decoding rule is decoded (step ST5e of Fig.15).

[0093]

In the equipment type code primary detecting element 55, the equipment type code generated with the NAT equipment 5 is detected from decode data (step ST6e of Fig.15). When the equipment type code of the NAT equipment 5 is detected as an equipment classification of an opposite unit at this time, the equipment type code primary detecting element 55, The IP address of that opposite unit (NAT equipment 5) is detected from camouflage ARP in which this equipment type code was included, and it registers with the equipment classification table 56 (step ST7e of Fig.15). Adding the information which identifies the NAT equipment 5 to the usual ARP table as an example of this equipment classification table 56 etc. is mentioned.

[0094]

If the information about setting out and the condition resolutive of an abandonment filter is detected by step ST1e, abandonment / condition-resolutive primary detecting element 51 will search the equipment classification table 56, and will judge whether an opposite unit is the NAT equipment 5 (step ST8e of Fig.15). When the address of the opposite unit which is a candidate for a report of abandonment/condition resolutive is not the NAT equipment 5 at this time, abandonment / condition-resolutive generation part 58, In order not to make it recognize that the opposite unit judged it as the DDoS attack person, and the measure against a DDoS attack was made, sending out of abandonment / condition-resolutive report packet is not performed (step ST9e of Fig.15).

[0095]

On the other hand, if the ARP reply to the ARP request which transmitted to the opposite unit is judged as it being camouflage ARP and an opposite unit being the NAT equipment 5 as an arrow shows in Fig.8 for example, Abandonment / condition-resolutive primary detecting element 51 sends out the information about setting out and the condition resolutive of the detected that and abandonment filter to abandonment / condition-resolutive generation part 58. If it is reported from abandonment / condition-resolutive primary detecting element 51 that an opposite unit is the NAT equipment 5, the IP address of the communication apparatus on the upper level side next hop will be searched with abandonment / condition-resolutive generation part 58 from the routing table 59, and it will be considered as destination IP addresses by it (step ST10e of Fig.15). Based on the information about setting out and the condition resolutive of an abandonment filter which abandonment / condition-resolutive primary detecting element 51 detected, the information about setting out and the condition resolutive of an abandonment filter corresponding to an opposite unit is generated, and it sends out to abandonment / condition-resolutive report packet generation part 61.

ERICSSON EXHIBIT 1005, Page 249

[0096]
Abandonment / condition-resolutive report packet generation part 61 builds destination IP addresses into a header by the header control part 60, The abandonment / condition-resolutive report packet which expressed the information about setting out and the condition resolutive of the abandonment filter from abandonment / condition-resolutive generation part 58 with the usual management protocol under TCP/IP network environments, such as an SNMP protocol, without enciphering are generated (step ST11e of Fig.15). This abandonment / condition-resolutive report packet are transmitted to the NAT equipment 5 corresponding to destination IP addresses from abandonment / condition-resolutive report packet generation part 61 (step ST12e of Fig.15).
[0097]
The equipment type code generation part 68 of the NAT equipment 5 will generate the equipment type code for identifying that it is the self-equipment 5, if the Request to Send (ARP request) of ARP is received (step ST1f of Fig.16 (a)) (step ST2f of Fig.16 (a)). The encryption section 69 enciphers the equipment type code which the equipment type code generation part 68 generated by DES, 3DES, etc. (step ST3f of Fig.16 (a)).
[0098]
The camouflage ARP generation part 70 carries out capsuling of the equipment type code enciphered by the encryption section 69 to the padding part of an ARP reply packet, The destination IP addresses which searched and determined the routing table 67 are built into a header, and camouflage ARP is generated (step ST4f of Fig.16 (a)). This camouflage ARP is sent out to lower routers (router 3b) from the camouflage ARP generation part 70 (step ST5f of Fig.16 (a)).
[0099]
Thus, in the NAT equipment 5 by this embodiment 2, In order to notify lower routers (router 3b) that the self-equipment 5 is NAT equipment, camouflage ARP containing the data which enciphered the equipment type code which shows that it is the NAT equipment 5 generated by the equipment type code generation part 68 is sent out to lower routers at the time of the ARP solution processing at the time of transmitting data. Since it has a decoding part for decoding the encoded data based on the encryption section 69 of the NAT equipment 5 which was mentioned above if the router which received camouflage ARP is based on a regular user at this time, this decodes an equipment type code and it is specified whether it is the NAT equipment 5. On the other hand, since the above-mentioned encoded data cannot be decoded even if the terminal of an attacking agency receives camouflage ARP, it cannot distinguish from the usual ARP and does not recognize that the measure against a DDoS attack is taken.
[0100]
Abandonment / condition-resolutive report packet is transmitted also to the communication apparatus on the network B via the NAT equipment 5, and it may be made to set up the abandonment filter to the terminal 4. In this case, the address conversion section 64 of the NAT equipment 5 mentioned below, The address information in abandonment / condition-resolutive report is converted to the addressing architecture of the network B which is not an attacking agency side, and attack side NW abandonment / condition-resolutive generation part 65 generates the information about setting out of the abandonment filter by this addressing architecture, and its condition resolutive.
[0101]
Next, the case where the DDoS attack of the server 1 is carried out via the NAT equipment 5 from the

ERICSSON EXHIBIT 1005, Page 250

terminal 7 in the network B is described.
The DDoS attack to the server 1 through the NAT equipment 5 from the terminal 7 on the network B, It is detected by the DDoS attack primary detecting element 39 of the Firewall equipment 2, According to the processing shown in Fig.13, abandonment / condition-resolutive report packet of the information about setting out and the condition resolutive of the abandonment filter for restricting abandonment or its transmission band are generated, and the data of the terminal 7 is transmitted to the router 3a. In the routers 3a and 3b, according to the processing shown in Fig.14 and Fig.15, respectively, abandonment / condition-resolutive report packet is generated, and it transmits to the NAT equipment 5.
[0102]
In abandonment / condition-resolutive report packet receive section 62 of the NAT equipment 5, the abandonment / condition-resolutive report packet information from the router 3b are received like the usual packet information reception (step ST1g of Fig.16 (b)). In abandonment / condition-resolutive primary detecting element 63, the information about setting out and the condition resolutive of an abandonment filter is detected from the packet information of the SNMP protocol input from the packet receive section 62. Then, abandonment / condition-resolutive primary detecting element 63 sends out the information about the setups of an abandonment filter, and its condition resolutive to the address conversion section 64.
[0103]
In the address conversion section 64, the address information in the information about setting out and the condition resolutive of an abandonment filter is converted to the addressing architecture of the network B with which the terminal 7 of an attacking agency exists based on the NAT information on the NAT table 66 (step ST2g of Fig.16 (b)). This conversion information is sent out to attack side NW abandonment / condition-resolutive generation part 65 from the address conversion section 64. In attack side NW abandonment / condition-resolutive generation part 65, based on setting out and the condition resolutive of the abandonment filter with which the addressing architecture was converted to the network B by the address conversion section 64 from the network A, Setting out and the condition resolutive of the abandonment filter for setting to the communication apparatus on the network B are generated (step ST3g of Fig.16 (b)).
[0104]
In the filtering control part 71, the abandonment filter to the data from the terminal 7 is set as the self-equipment 5 based on setting out and the condition resolutive of the abandonment filter from attack side NW abandonment / condition-resolutive generation part 65 (step ST4g of Fig.16 (b)). Attack side NW abandonment / condition-resolutive generation part 65 searches the IP address of the communication apparatus on the upper level side next hop from the routing table 67, and is taken as destination IP addresses (step ST5g of Fig.16 (b)). The destination IP addresses which searched the routing table 67 and were determined are sent out to the header control part 72.
[0105]
Abandonment / condition-resolutive report packet generation part 73 builds destination IP addresses into a header by the header control part 72, The information about setting out and the condition resolutive of the abandonment filter from attack side NW abandonment / condition-resolutive generation part 65, The abandonment / condition-resolutive report packet denoted by the usual

ERICSSON EXHIBIT 1005, Page 251

management protocol under TCP/IP network environments, such as an SNMP protocol, are generated, without enciphering (step ST6g of Fig.16 (b)). This abandonment / condition-resolutive report packet are transmitted to the lower routers 6a in the network B corresponding to destination IP addresses from abandonment / condition-resolutive report packet generation part 73 (step ST7g of Fig.16 (b)).

[0106]

Henceforth, the same processing as the router 3a is performed with the routers 6a, 6b, and 6c. Thereby, even if it is a case where the DDoS attack of the server 1 is carried out via the NAT equipment 5 from the terminal 7 in the network B, an abandonment filter can be set to the communication apparatus on the networks A and B, and the measure against a DDoS attack can be validated. The Firewall equipment 2, the routers 3a and 3b, the NAT equipment 5, and the routers 6a, 6b, and 6c release the set-up abandonment filter, when the condition resolutive set up considering the camouflage ARP request as a medium is satisfied.

[0107]

As mentioned above, according to this embodiment 2, the Firewall equipment 2 and the routers 3a, 6a, 6b, and 6c, Transmit the information about setting out and the condition resolutive of an abandonment filter which restrict the transmission band of the send data of the terminals 4 and 7 which carry out the DDoS attack of the server 1 for defense from an upper level communication apparatus, and it sets up an abandonment filter, The NAT equipment 5 generates the camouflage ARP packet information which built the encoded data of the identification information of self-equipment into the ARP packet, The router 3b which transmits to the adjoining router 3b and adjoins the NAT equipment 5, The ARP packet information received from the upper level communication apparatus to store is camouflage ARP packet information, Since the information about setting out and the condition resolutive of an abandonment filter is transmitted to the communication apparatus concerned when this communication apparatus is judged to be the NAT equipment 5 from the identification information produced by decoding this, Since it becomes unnecessary to perform encryption/decoding processing with all the communication apparatus on a network, reduction of equipment costs can be aimed at and the throughput of the whole network can be made to UP.

[0108]

Although the case where the DDoS attack by the terminal 4 on the network A and the DDoS attack by the terminal 7 on the network B were made separate was described in the above-mentioned embodiment 2, Even if it is a case where the attacking agency terminal of both networks performs a DDoS attack simultaneously, DDoS attack measure processing can be validated by setting up the abandonment filter by the camouflage ARP request mentioned above in the networks A and B.

The present invention may be applied to the network through address conversion devices other than the NAT equipment by a Proxy server etc. That is, not only conversion of an IP address but NAPT (IP masquerade) dynamically converted to the port number of TCP/UDP which is the higher-level protocol is included in NAT in the present invention.

[Brief Description of the Drawings]

[0109]

[Drawing 1]It is the figure showing the network system to which the distributed-denial-of-service-attacks measure method according to this embodiment of the invention 1 is applied.

[Drawing 2]It is a block diagram showing the composition of the Firewall equipment by embodiment 1.

ERICSSON EXHIBIT 1005, Page 252

[Drawing 3]It is a block diagram showing the composition of the router by embodiment 1.
[Drawing 4]It is a block diagram showing the composition of the NAT equipment by embodiment 1.
[Drawing 5]It is a flow chart which shows operation of the Firewall equipment by embodiment 1.
[Drawing 6]It is a flow chart which shows operation of the router by embodiment 1.
[Drawing 7]It is a flow chart which shows operation of the NAT equipment by embodiment 1.
[Drawing 8]It is the figure showing the network system to which the distributed-denial-of-service-attacks measure method according to this embodiment of the invention 2 is applied.
[Drawing 9]It is a block diagram showing the composition of the Firewall equipment by embodiment 2.
[Drawing 10]It is a block diagram showing the composition of the router by embodiment 2.
[Drawing 11]It is a block diagram showing the composition of the router contiguous to the NAT equipment by embodiment 2.
[Drawing 12]It is a block diagram showing the composition of the NAT equipment by embodiment 2.
[Drawing 13]It is a flow chart which shows operation of the Firewall equipment by embodiment 2.
.
[Drawing 14]It is a flow chart which shows operation of the router by embodiment 2.
[Drawing 15]It is a flow chart which shows operation of the router which adjoins NAT equipment on the network on the server side of the target of attack by embodiment 2.
[Drawing 16]It is a flow chart which shows operation of the NAT equipment by embodiment 2.
[Explanations of letters or numerals]
[0110]
1 A server (computer for defense), 2 Firewall equipment (communication apparatus), 3a, 3b, 6a, 6b, and 6c A router (communication apparatus), and 4 and 7 Terminal, 5 NAT equipment (address conversion device), 8, 39 DDoS-attack primary detecting element, 9, 19, 29, 40, 46, and 58 Abandonment / condition-resolutive generation part (filter information generation part), 10, 20, 33, 41, 47, 57, and 71 Filtering control part, 11, 21, 34, 42, 48, 59, and 67 Routing table, 12, 22, 35, and 69 Encryption section (an encryption section, a filter information transmission and reception section), 13, 23, and 36 A padding control part, 14, 24, 37, 43, 49 and 60, 72 header control parts, 15, 25, 38, and 70 Camouflage ARP generation part (a packet generation part, a filter information transmission and reception section), 16, 26 ARP primary detecting element, and 17 and 27 Padding extraction part (filter information transmission and reception section), 18 and 28 A decoding section (a decoding part, a filter information transmission and reception section), 30, 64 address conversion sections, 31, 66 NAT table, and 32 and 65 -- attack side NW abandonment / condition-resolutive generation part (filter information generation part), 44, 50 and 61, and 73 abandonment / condition-resolutive report packet generation part (a filter information reporting part --) A filter information transmission and reception section, and 45 and 62 Abandonment / condition-resolutive report packet receive section (filter information generation part), 51 and 63 [An equipment classification table and 68 / Equipment type code generation part.] Abandonment / condition-resolutive primary detecting element, 52 ARP receive section (receive section), and 53 A decoding part and 55 An equipment type code primary detecting element and 56

ERICSSON EXHIBIT 1005, Page 253

CLAIMS

[Claim(s)]

[Claim 1]

In a communication apparatus linked to a network which has a computer for defense, and an address conversion device which takes correspondence of address information between networks with which addressing architectures differ,

A filter information generation part which generates information about setting out and a condition resolutive of a filter which restrict a transmission band of send data from a communication apparatus which carries out the distributed denial of service attacks of the computer for [aforementioned] defense,

A filtering control part which sets up the aforementioned filter based on information about setting out and a condition resolutive of the aforementioned filter,

A communication apparatus provided with a filter information transmission and reception section which exchanges information about setting out and a condition resolutive of the aforementioned filter among other communication apparatus containing an address conversion device linked to the aforementioned network.

[Claim 2]

A filter information transmission and reception section,

An encryption section which uses information about setting out and a condition resolutive of a filter as encoded data,

A decoding part which decodes the aforementioned encoded data,

The communication apparatus according to claim 1 provided with a packet generation part which transmits to a communication apparatus which generates packet information incorporating the aforementioned encoded data, and contains an address conversion device.

[Claim 3]

A filter information transmission and reception section,

A receive section which receives packet information incorporating encoded data of device identification information,

A decoding part which decodes the aforementioned encoded data,

The communication apparatus according to claim 1 having determined transmission destination equipment based on the aforementioned device identification information, and having a filter information reporting part which transmits packet information incorporating information about setting out and a condition resolutive of a filter.

[Claim 4]

The communication apparatus according to claim 2 or 3, wherein packet information incorporating encoded data is ARP packet information.

[Claim 5]

In an address conversion device which a network which a computer for defense connects, and this network are arranged between networks which differ in an addressing architecture, and takes correspondence of address information,

A receive section which receives information about setting out and a condition resolutive of a filter which restrict a transmission band of send data from a communication apparatus which carries out the

ERICSSON EXHIBIT 1005, Page 254

distributed denial of service attacks of the computer for [aforementioned] defense,
An address conversion device having an address conversion section which converts the address information to address information corresponding to an addressing architecture of a transmission destination network in transmitting information about setting out and a condition resolutive of the aforementioned filter ranging over a different network.
[Claim 6]
The address conversion device comprising according to claim 5:
A packet generation part which generates, transmits and receives camouflage ARP packet information which built setting out of a filter, and encoded data of a condition resolutive into an ARP packet.
A decoding part which decodes the aforementioned encoded data.

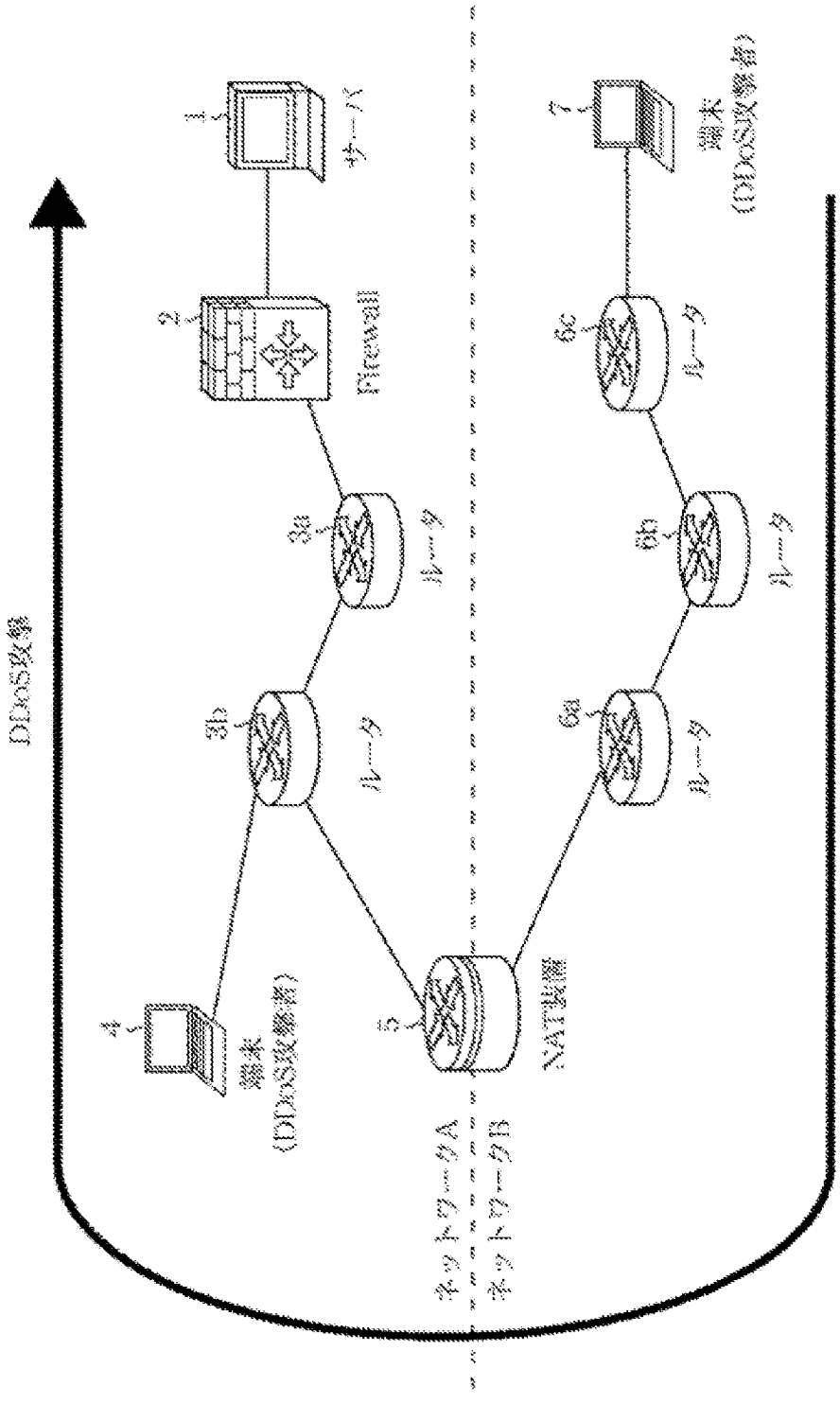
[Claim 7]
The address conversion device comprising according to claim 5:
An encryption section which uses as encoded data device identification information which identifies self-equipment.
A packet generation part which generates, transmits and receives camouflage ARP packet information which built the aforementioned encoded data into an ARP packet.

[Claim 8]
In a program as which a computer is operated as a communication apparatus linked to a network which has a computer for defense, and an address conversion device which takes correspondence of address information between networks with which addressing architectures differ,
A filter information generation part which generates information about setting out and a condition resolutive of a filter which restrict a transmission band of send data from a communication apparatus which carries out the distributed denial of service attacks of the computer for [aforementioned] defense,
A filtering control part which sets up the aforementioned filter based on information about setting out and a condition resolutive of the aforementioned filter,
A program as which the aforementioned computer is operated as a filter information transmission and reception section which exchanges information about setting out and a condition resolutive of the aforementioned filter among other communication apparatus containing an address conversion device linked to the aforementioned network.
[Claim 9]
In a program as which a computer is operated as an address conversion device which a network which a computer for defense connects, and this network are arranged between networks which differ in an addressing architecture, and takes correspondence of address information,
A receive section which receives information about setting out and a condition resolutive of a filter which restrict a transmission band of send data from a communication apparatus which carries out the distributed denial of service attacks of the computer for [aforementioned] defense,
A program as which the aforementioned computer is operated as an address conversion section which converts the address information to address information corresponding to an addressing architecture of

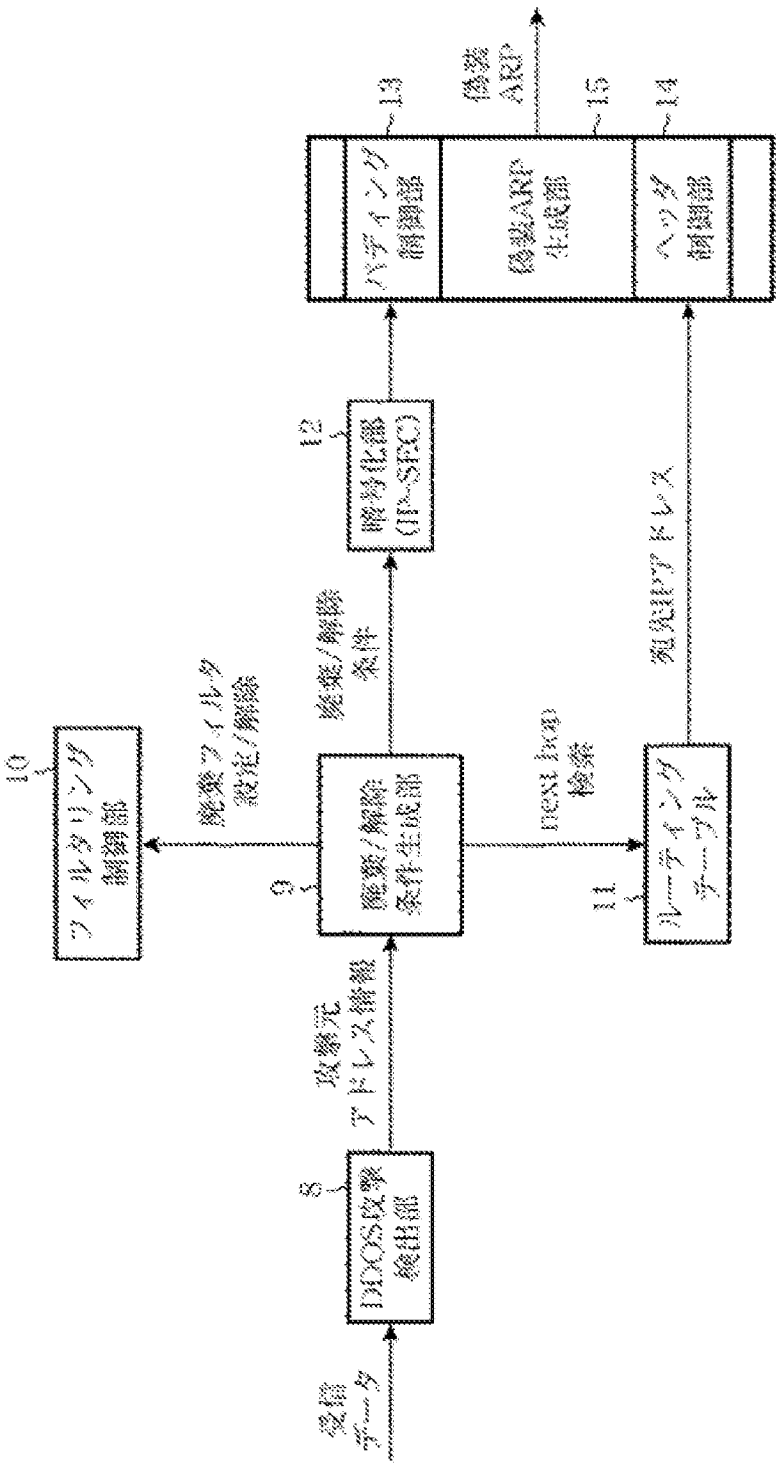
ERICSSON EXHIBIT 1005, Page 255

a transmission destination network in transmitting information about setting out and a condition resolutive of the aforementioned filter ranging over a different network.

ERICSSON EXHIBIT 1005, Page 256

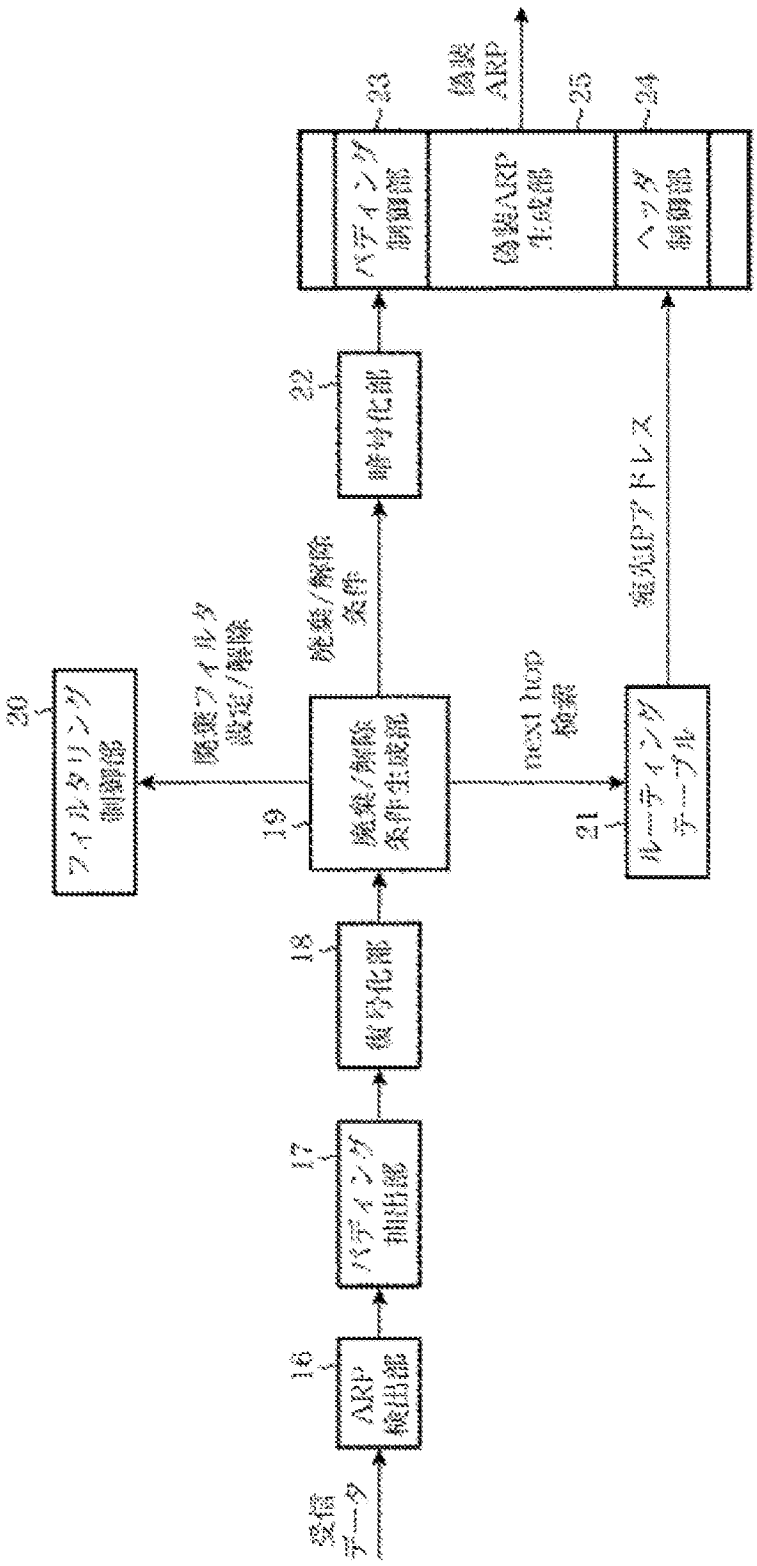

DDoS攻撃
1
サーバ
2
Firewall
3a
ルータ
3b
ルータ
4
端末
(DDoS攻撃者)
5
NAT装置
6a
ルータ
6b
ルータ
6c
ルータ
7
端末
(DDoS攻撃者)
ネットワークA
ネットワークB

[Drawing 1]



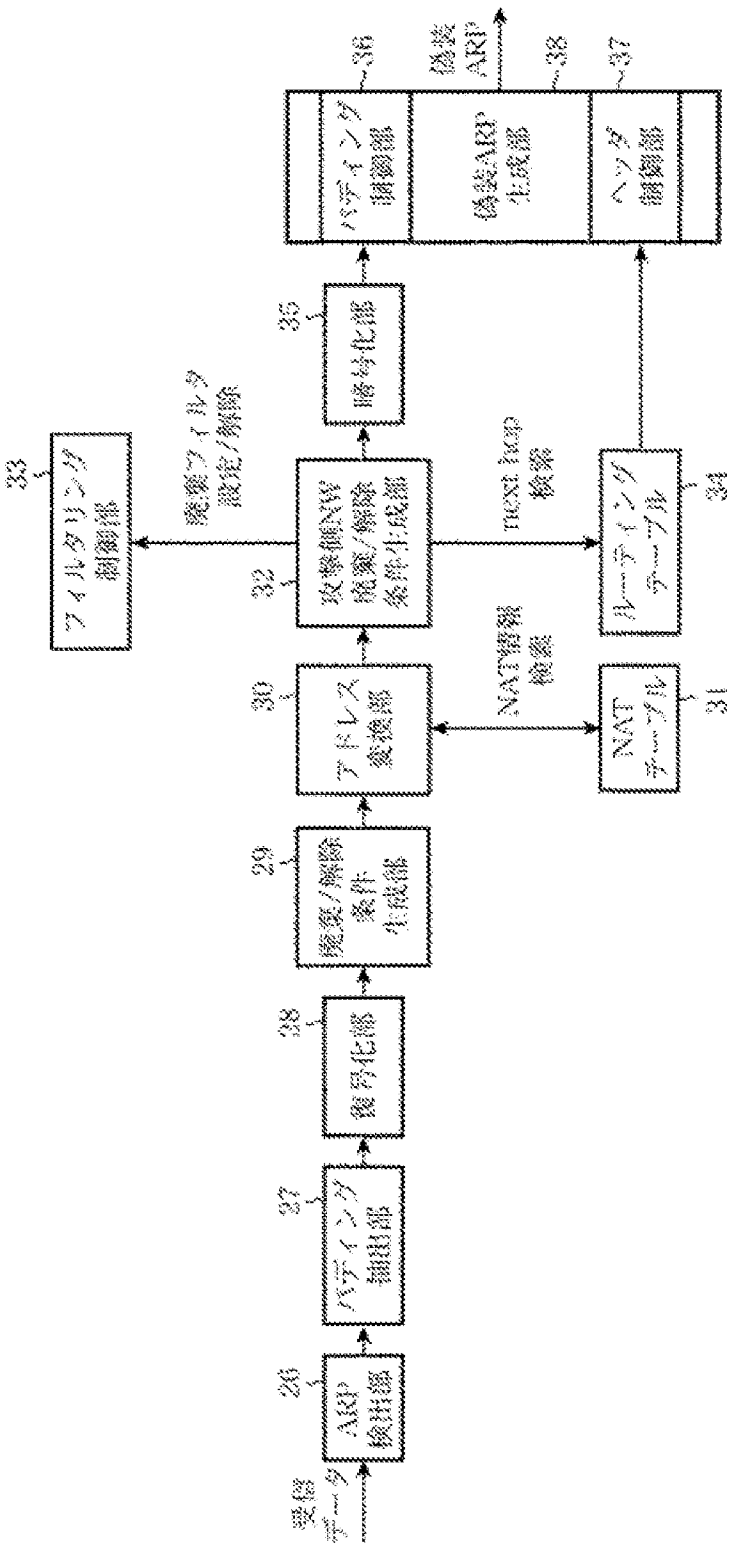
[Drawing 2]

ERICSSON EXHIBIT 1005, Page 258

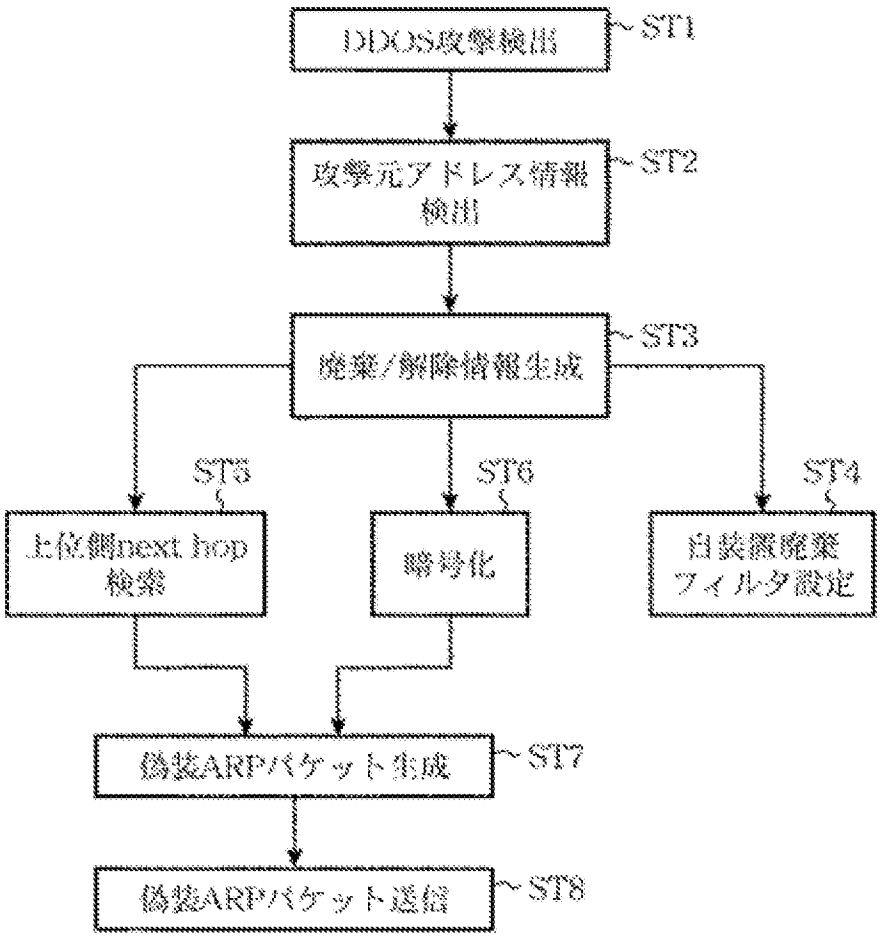


[Drawing 3]

ERICSSON EXHIBIT 1005, Page 259

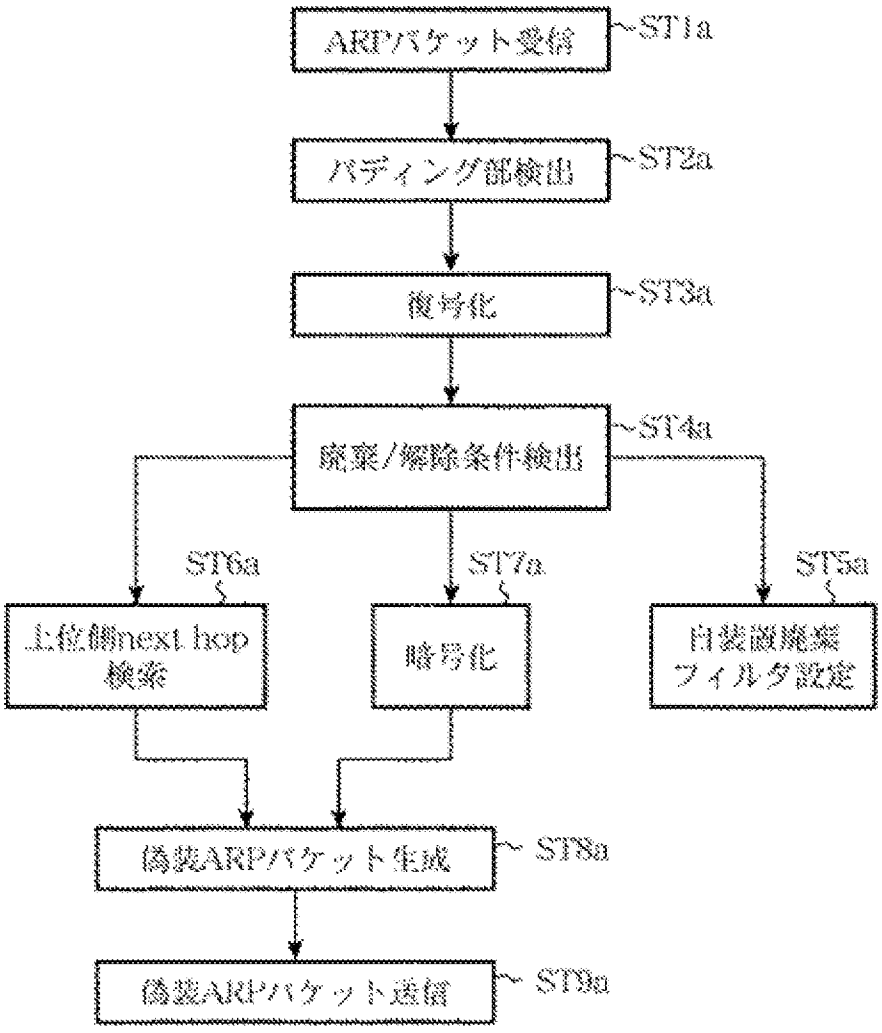

受信データ
ARP検出部
パケット分析部
復号化部
攻撃/解除条件生成部
アドレス変換部
攻撃情報NW設置/解除条件生成部
フィルタリング制御部
NAT情報検索
next hop検索
NATテーブル
ルーティングテーブル
暗号化部
パケット制御部
偽装ARP生成部
ヘッダ制御部
偽装ARP
フィルタリング設定/解除

[Drawing 4]

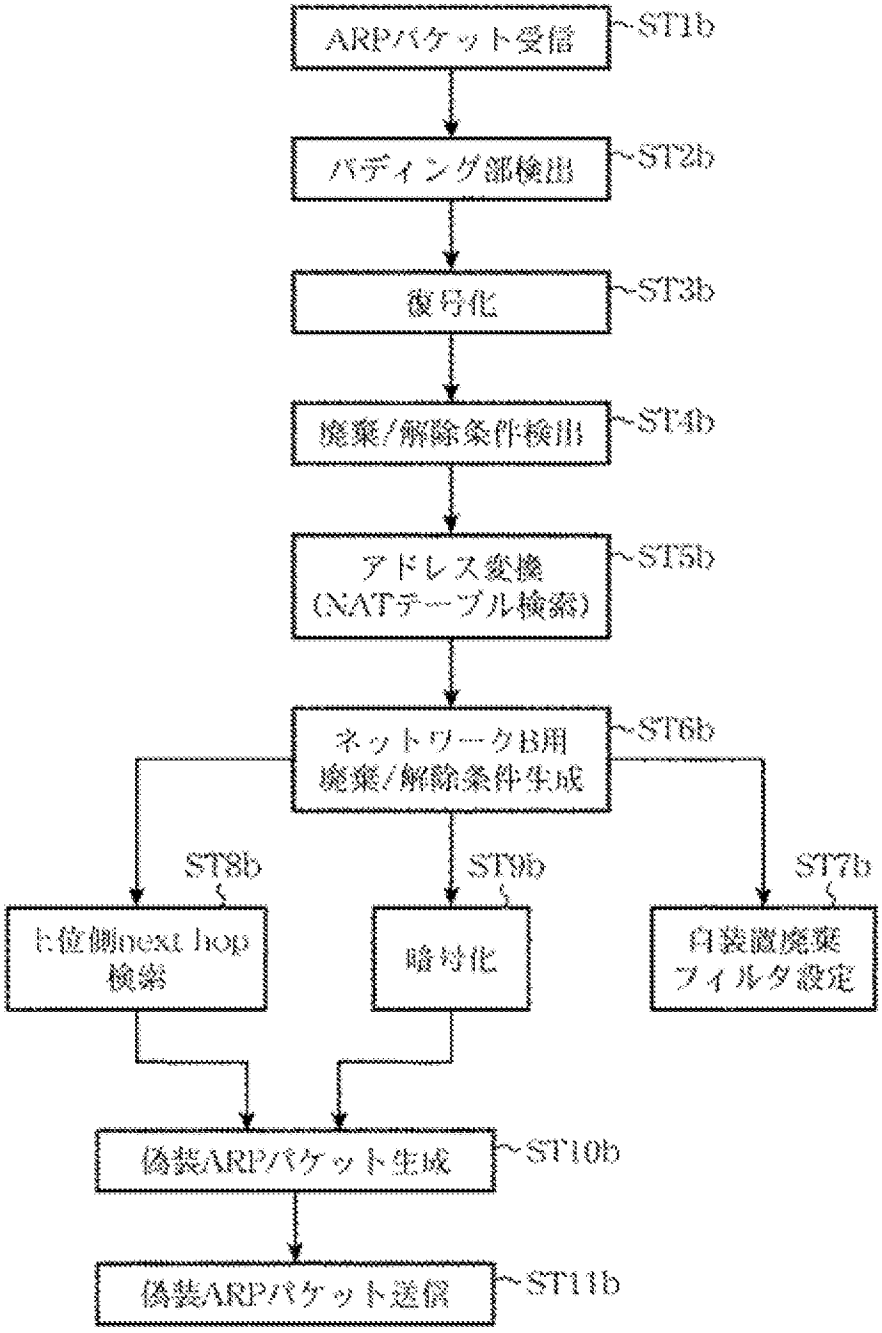


[Drawing 5]

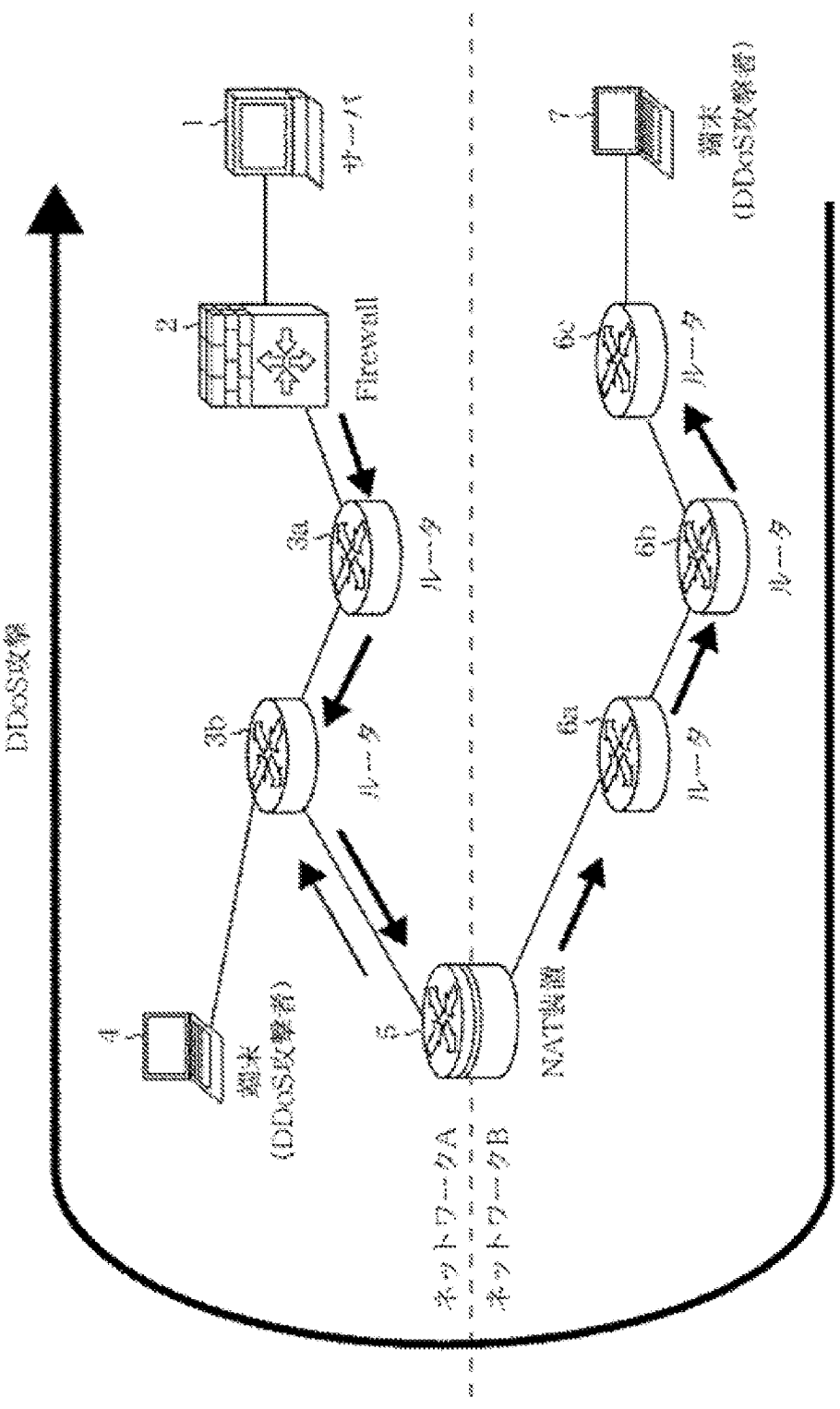
ERICSSON EXHIBIT 1005, Page 261


ARPパケット受信
ST1a
パディング部検出
ST2a
復号化
ST3a
廃棄/削除条件検出
ST4a
ST6a
ST7a
ST5a
上位側next hop
検索
暗号化
自装置廃棄
フィルタ設定
偽装ARPパケット生成
ST8a
偽装ARPパケット送信
ST9a

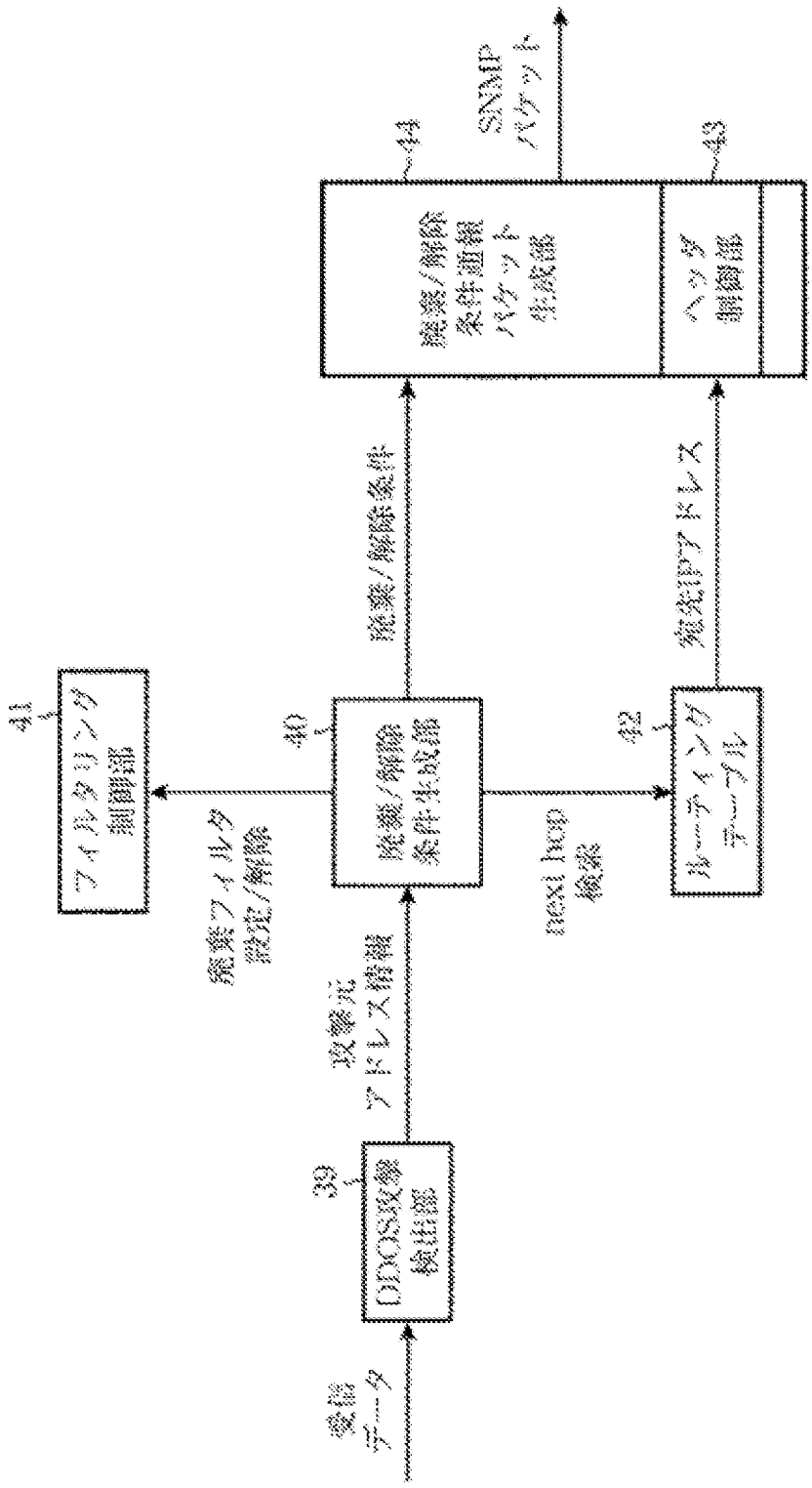
[Drawing 6]


ARPパケット受信
ST1b
パディング部検出
ST2b
復号化
ST3b
廃棄/解除条件検出
ST4b
アドレス変換
(NATテーブル検索)
ST5b
ネットワークB用
廃棄/解除条件生成
ST6b
ST8b
ST9b
ST7b
上位側next hop
検索
暗号化
自装置廃棄
フィルタ設定
偽装ARPパケット生成
ST10b
偽装ARPパケット送信
ST11b

[Drawing 7]

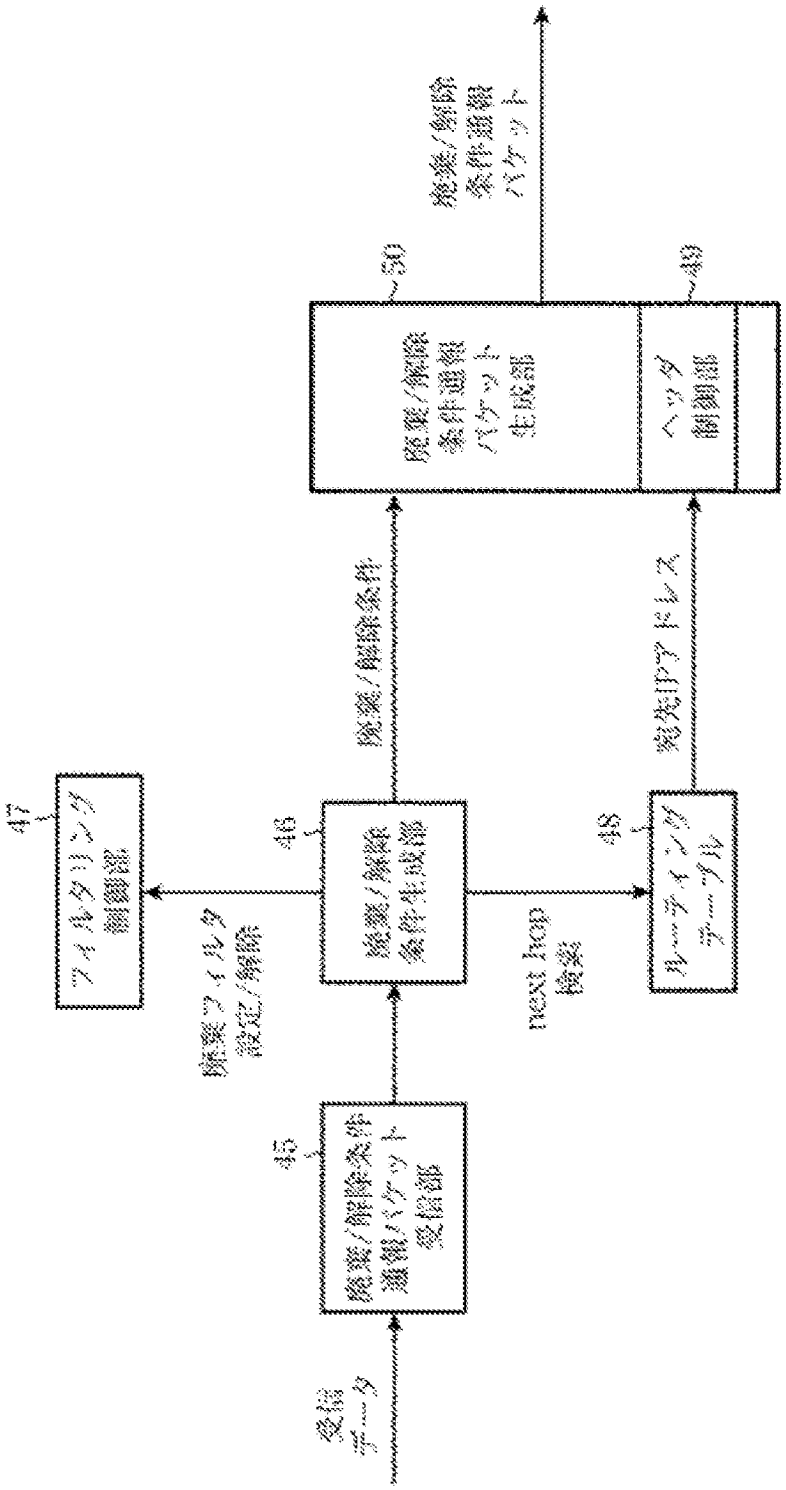

DDoS攻撃
サーバ
1
Firewall
2
ルータ
3a
ルータ
3b
端末
(DDoS攻撃者)
4
5
NAT装置
ネットワークA
ネットワークB
ルータ
6a
ルータ
6b
ルータ
6c
端末
(DDoS攻撃者)
7

[Drawing 8]



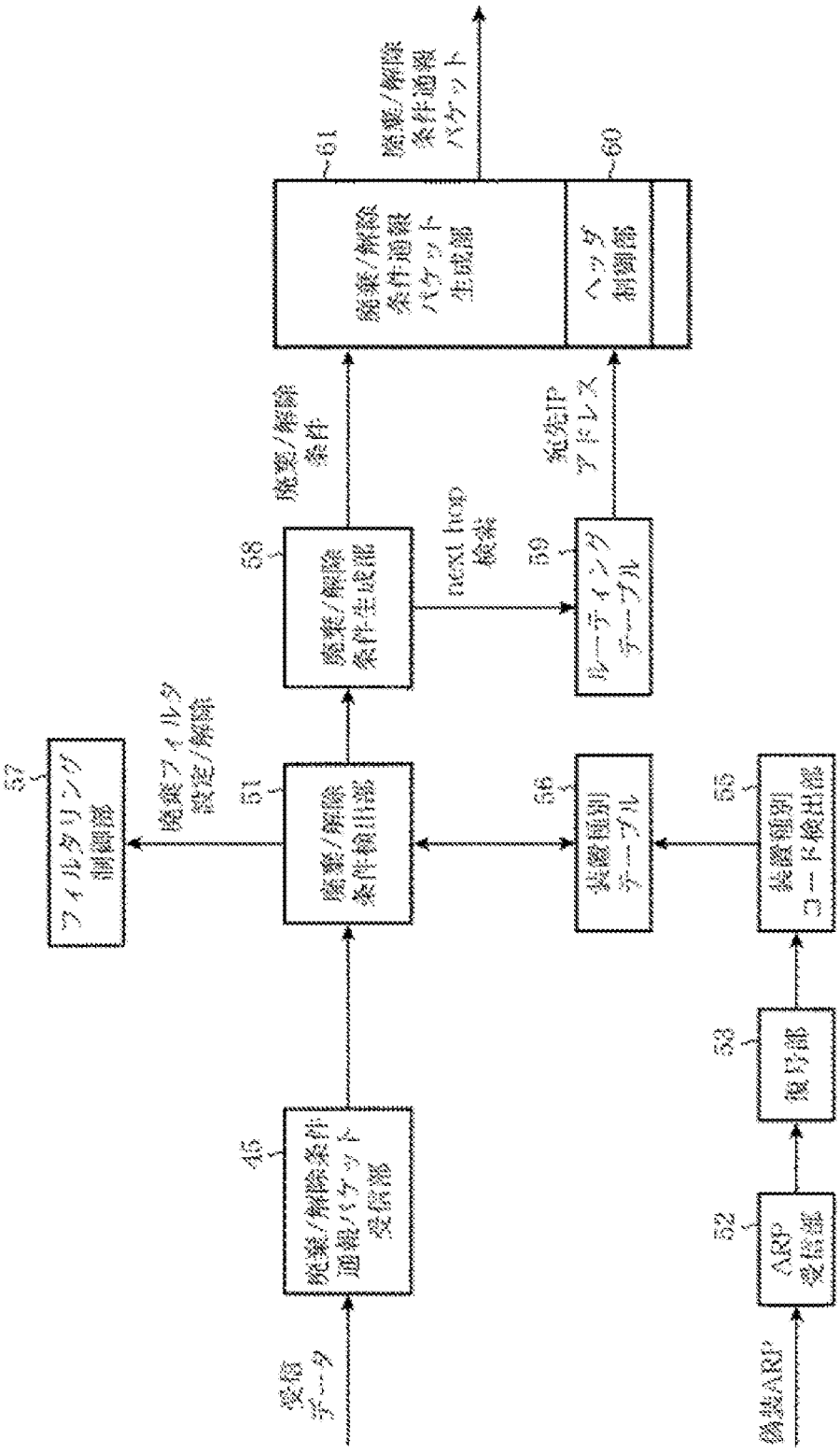
[Drawing 9]

ERICSSON EXHIBIT 1005, Page 265



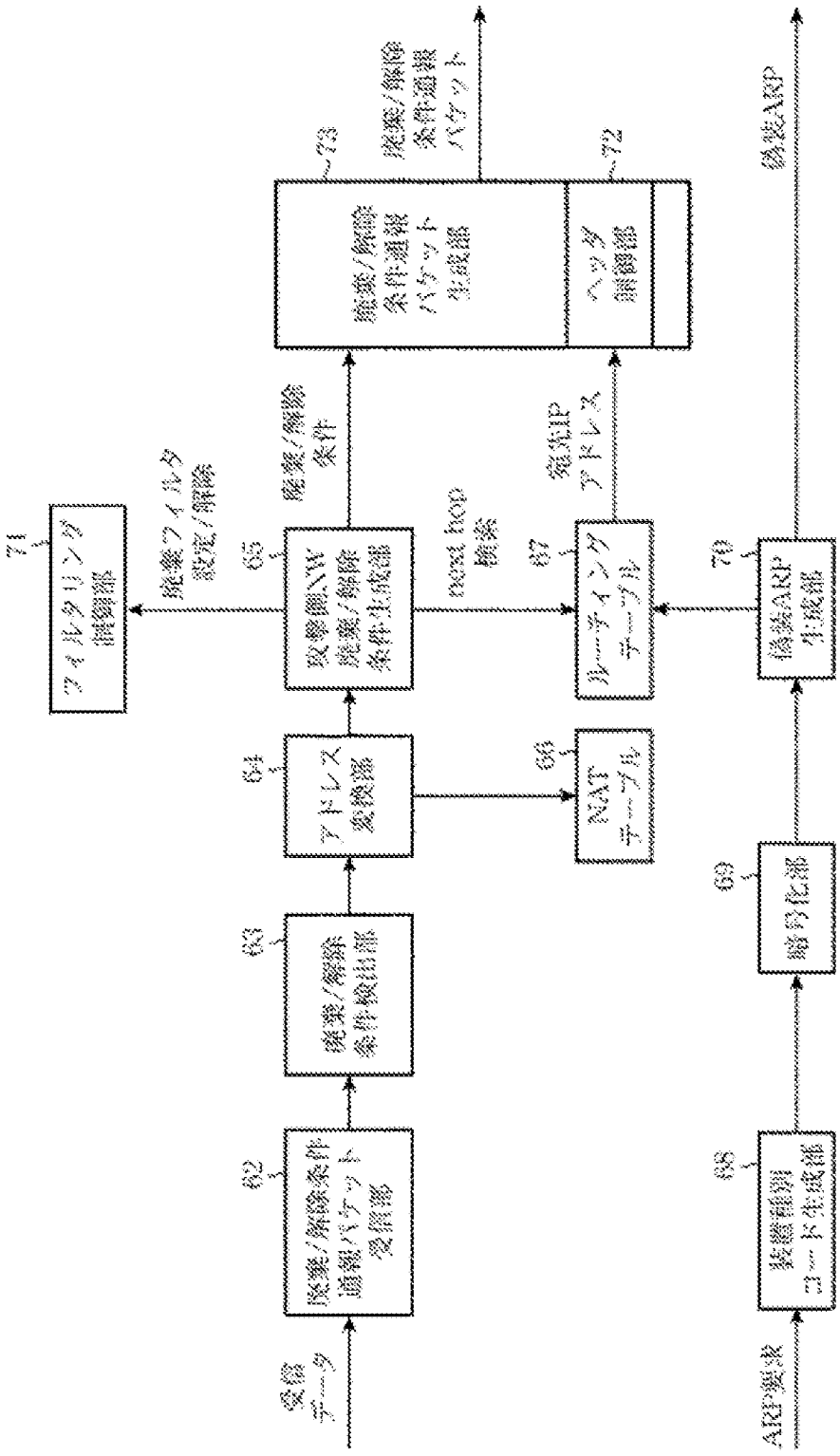
[Drawing 10]

ERICSSON EXHIBIT 1005, Page 266



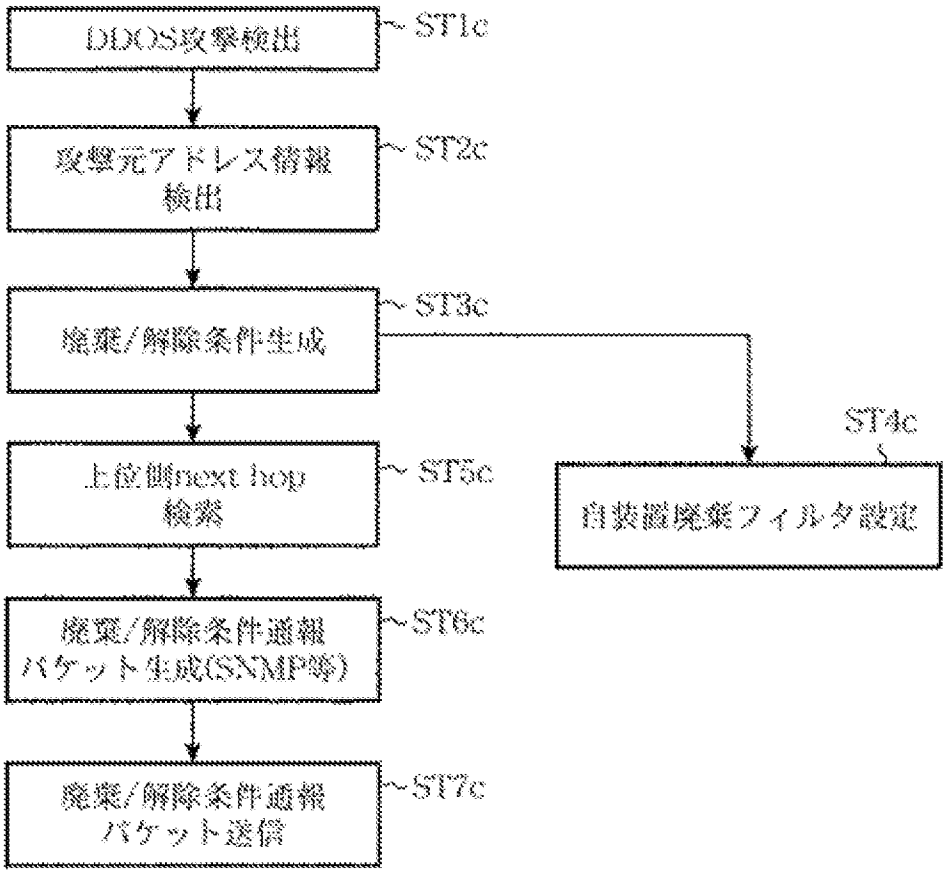
[Drawing 11]

ERICSSON EXHIBIT 1005, Page 267

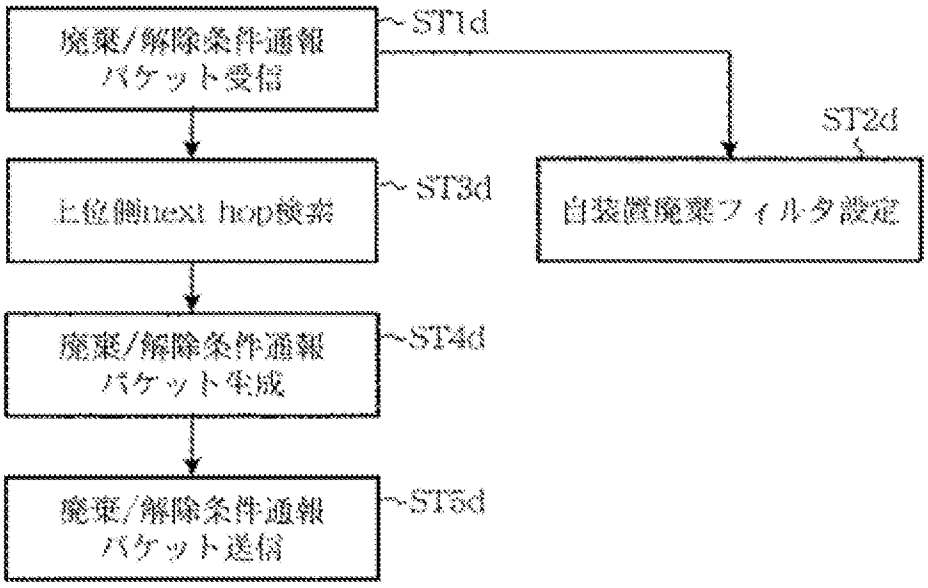


[Drawing 12]

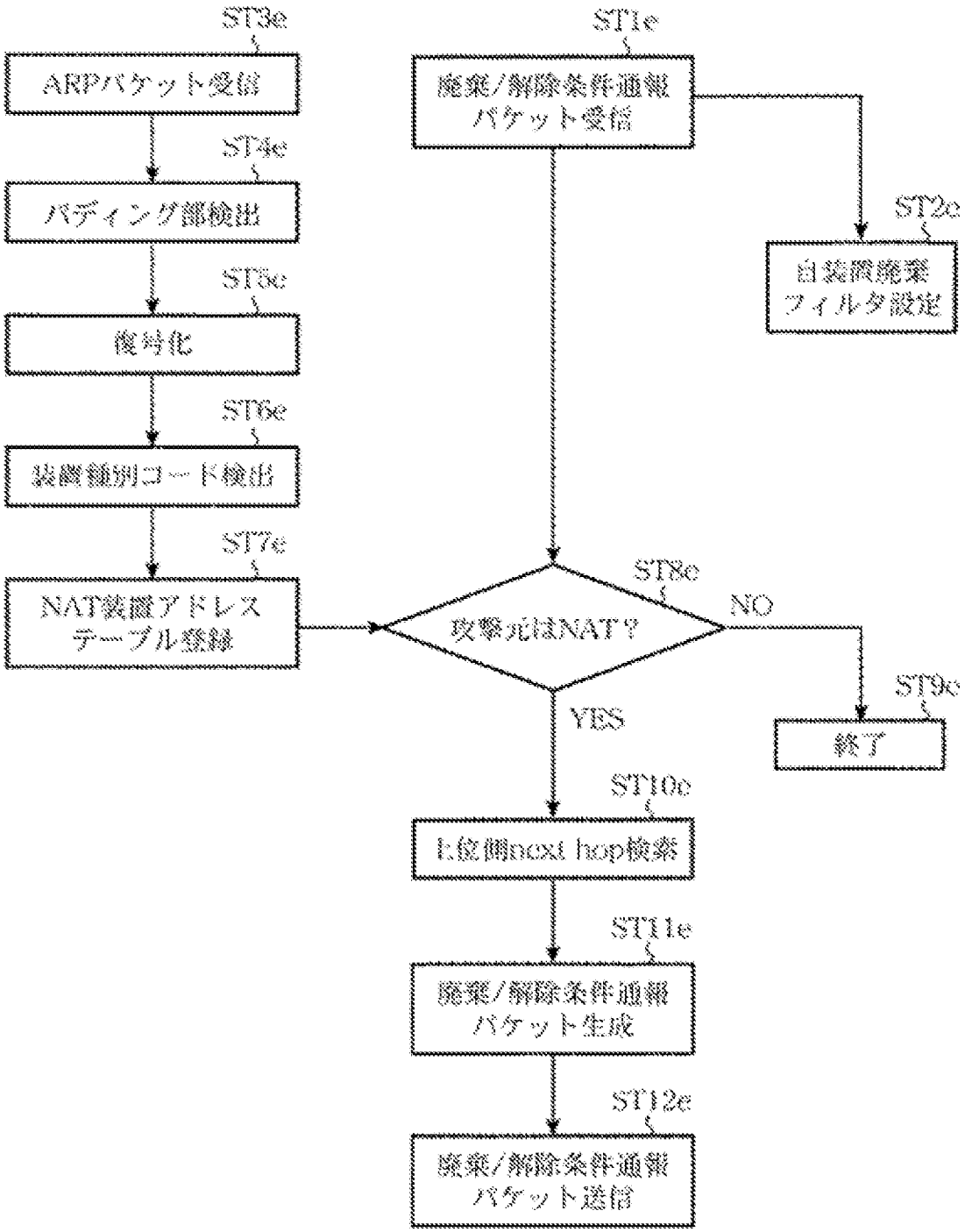
ERICSSON EXHIBIT 1005, Page 268


DDOS攻撃検出
ST1c
攻撃元アドレス情報
検出
ST2c
廃棄/解除条件生成
ST3c
ST4c
自装置廃棄フィルタ設定
上位側next hop
検索
ST5c
廃棄/解除条件通報
パケット生成(SNMP等)
ST6c
廃棄/解除条件通報
パケット送信
ST7c

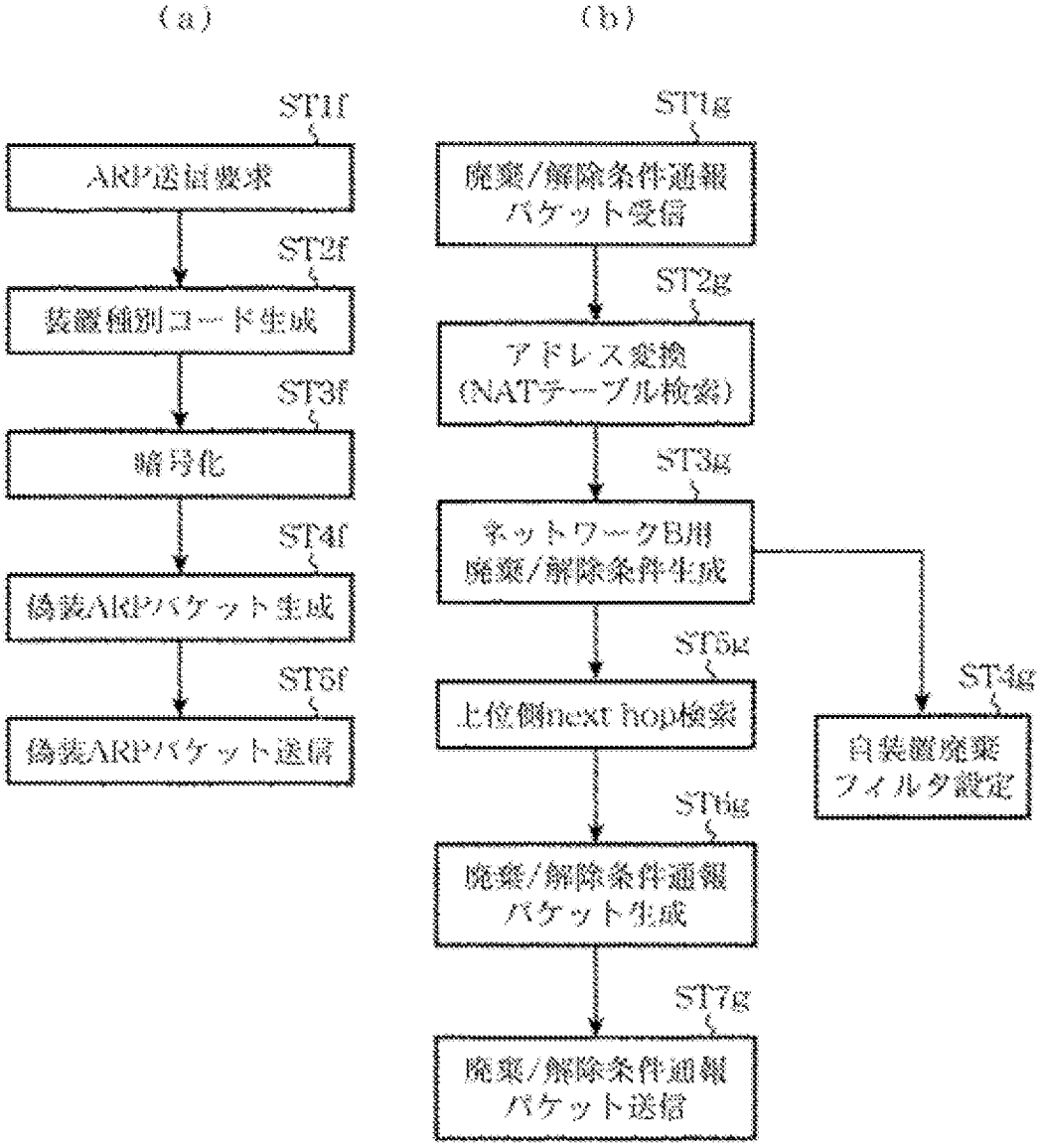
[Drawing 13]


廃棄/解除条件通報
パケット受信
ST1d
ST2d
上位側next hop検索
ST3d
自装置廃棄フィルタ設定
廃棄/解除条件通報
パケット生成
ST4d
廃棄/解除条件通報
パケット送信
ST5d

[Drawing 14]


ST3e
ARPパケット受信
ST4e
パディング部検出
ST5e
復号化
ST6e
装置種別コード検出
ST7e
NAT装置アドレス
テーブル登録
ST1e
廃棄/解除条件通報
パケット受信
ST2e
自装置廃棄
フィルタ設定
ST8e
攻撃元はNAT？
NO
YES
ST9e
終了
ST10e
上位側next hop検索
ST11e
廃棄/解除条件通報
パケット生成
ST12e
廃棄/解除条件通報
パケット送信

[Drawing 15]



[Drawing 16]

ERICSSON EXHIBIT 1005, Page 272

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 July 2007 (05.07.2007)

PCT

(10) International Publication Number
WO 2007/075423 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/047929

(22) International Filing Date:
15 December 2006 (15.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/303,915 19 December 2005 (19.12.2005) US

(71) Applicant *(for all designated States except US)*: **LUCENT TECHNOLOGIES INC.** [US/US]; 600 Mountain Avenue, Murray Hill, NJ 07974-0636 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BU, Tian** [CN/US]; 57 J Reading Road, Edison, NJ 08817 (US). **NORDEN, Samphel** [IN/US]; 75 Larkin Circle, West Orange, NJ 07052 (US). **WOO, Thomas, Y.** [US/US]; 2 Exeter Road, Short Hills, NJ 07078 (US).

(74) Agent: **CURTIN, John, E.**; LUCENT TECHNOLOGIES INC., Docket Administrator - Room 2F-190, 600 Mountain Avenue, Murray Hill, NJ 07974-0636 (US).

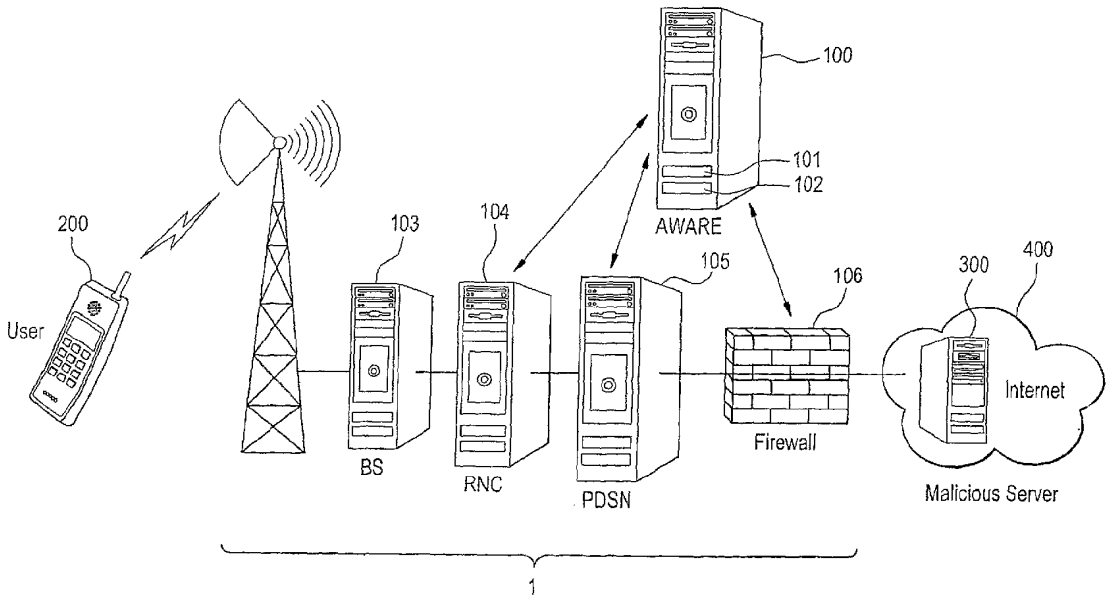
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, 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, 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: METHODS AND DEVICES FOR DEFENDING A 3G WIRELESS NETWORK AGAINST MALICIOUS ATTACKS



(57) Abstract: Wireless state information collected or inferred from a 3G wireless network is used to detect and prevent malicious attacks against the network.

WO 2007/075423 A2

METHODS AND DEVICES FOR DEFENDING A 3G WIRELESS NETWORK AGAINST MALICIOUS ATTACKS

BACKGROUND OF THE INVENTION

[0001] The frequency and magnitude of malicious attacks against wireless networks have been steadily increasing.

[0002] A large variety of solutions have been proposed to counter malicious attacks against communication networks. While these schemes may mitigate the threat of attacks against wireline networks they are inadequate for wireless networks.

[0003] For example, in a wireline Denial of Service (DoS) attack it takes a long period of time, relatively speaking, for a server to be disabled because such machines have a larger processing capacity than a wireless endpoint (mobile) which has limited processing and battery lifetime. In addition, a wireless link is severely bandwidth-constrained when compared to a wireline network. Thus, if traffic from an attack reaches a mobile, the attack has already succeeded in wasting critical resources of the wireless link, the wireless infrastructure, and the battery power of the mobile. This is in contrast to typical wireline DoS attacks that must overwhelm processing resources at a server in order to succeed.

[0004] There are numerous types of attacks that are attempted against wireless networks, two of which are signaling type attacks and battery (i.e., sleep deprivation) attacks. Co-pending U.S. Patent Applications No. _____ and _____, incorporated herein in full as if set forth in full herein discuss such attacks and propose specific techniques for defending against such attacks.

[0005] However, attacks against a 3G wireless network are not limited to just signaling and battery attacks.

[0006] It is desirable, therefore, to provide methods and devices for defending many types of 3G wireless networks against numerous types of attacks.

SUMMARY OF THE INVENTION

[0007] The present inventors have recognized that attacks against 3G wireless networks may be prevented, or substantially reduced, by making use of collected or inferred wireless state information.

ERICSSON EXHIBIT 1005, Page 274

[0008] More specifically, one embodiment (i.e., example) of the present invention provides for the detection of an attack against a 3G wireless network by obtaining wireless state information and comparing the obtained information to a profile to determine whether an attack is directed at an element in the network.

[0009] By using wireless state information the present inventors believe attacks can be more readily detected and prevented.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 depicts an example of an architecture for defending a 3G wireless network against attacks according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION, WITH EXAMPLES

[0011] To defend mobile devices in 3G wireless networks against numerous types of attacks, the present invention provides a novel architecture referred to as an architecture for Wireless Attack Resistance (AWARE).

[0012] FIG. 1 depicts one example of an AWARE architecture according to one embodiment of the invention.

[0013] In one embodiment of the present invention, an AWARE architecture (e.g., enabled device) 100 may comprise a *learning database* or *profiler* 101, and a *detection engine* or *detector* 102. The profiler 101 may be operable to collect wireless state information from the different elements of the wireless infrastructure 1 (e.g., network) including a base station (BS) 103, radio network controller (RNC) 104 and Packet Data Service Node PDSN, 105. In an alternative embodiment of the invention, the AWARE enabled device 100 may infer state information from its knowledge of the wireless network 1 when collection is not possible.

[0014] The profiler 101 is operable to capture and store information about a user 200, typically during a pre-processing step, in order to generate a traffic profile for a given user under normal (i.e., non-attack) conditions using, for example one or more statistical measures. In a further embodiment of the invention, after an initial profile is created the profiler 101 may update the profile regularly based on changes to a user's behavior. Information used in building the profile includes, but is not limited to, packet arrival times, IP addresses and port numbers of source(s), and destination(s). It should be understood that the profiler 101 may comprise one or

ERICSSON EXHIBIT 1005, Page 275

more databases. These databases may communicate with other user databases and profilers for cross-mobile, cross RNC, or cross PDSN correlations. For example, data from multiple databases associated with one or more PDSNs may be aggregated and analyzed for similarities, for example. A similarity may indicate the onset or presence of an attack that spans multiple PDSNs.

[0015] One novel aspect of the profiling mechanisms provided by the present invention is the ability to correlate user, application, as well as server related profiles. By user profile, we refer to the statistics for an individual user. This division can be further categorized by individual application. For instance, web surfing is the most frequently used service by most users. Similarly, a video-on-demand server may use RTP packets to broadcast video to users. Statistics on an individual web server basis or any IP source can also be compiled by logging the arrival of HTTP/RTP packets.

[0016] To enable scalability, the profiler 101 may be operable to aggregate profiles across users with similar behaviors using, for example, the same metric. Aggregation allows profiles to be stored in a scalable manner so that it may, for example, be more easily correlated later on. For example, current traffic may be compared to an aggregated profile to detect inconsistencies. Aggregated profiles may also be maintained for popular servers and applications. The flexibility of using different classification approaches allows a more comprehensive and accurate characterization of what is considered as normal traffic.

[0017] Turning now to the detector 102, it is operable to detect a 3G wireless attack using one or more detection heuristics.

[0018] In slightly more detail, one example of a signaling cost which may be used is the signaling cost as traffic traverses through the wireless network 1. Malicious traffic may be identified because it introduces excessive signaling cost. The cost of signaling can be obtained in various ways depending on the cooperation that can be obtained from elements within the wireless network 1.

[0019] In one embodiment of the present invention, the detector 102 may be operable to compare a stored non-attack or normal profile with current traffic conditions to determine whether current traffic for a user or set of users 200 violates the normal profile.

ERICSSON EXHIBIT 1005, Page 276

[0020] Once an attack is detected and the attacker identified, the AWARE enabled device 100 may block all future traffic from the suspected attacker by, for example, re-configuring or configuring the firewall 106 (e.g., setting rules in the firewall).

[0021] As mentioned before, AWARE enabled devices provided by the present invention collect wireless specific state information including the setup and release of wireless data channels, and the time that a mobile is active. The inventors know of no other device as of this date that collects wireless state information and uses it to detect 3G wireless attacks in a manner akin to the present invention.

[0022] In further embodiments of the present invention, the AWARE-enabled device 100 may be operable to maintain information at different levels of granularity (for the same measurement parameter). Said another way, for the same measurement parameter, different aggregation levels may be used. For example, a per-mobile, per-RNC, per-BS, per-PDSN or per-external-source basis. This allows the detection heuristic to find anomalies at multiple levels, preventing an attacker from spreading malicious traffic across different RNCs or launching an attack that doesn't limit itself to a particular BS.

[0023] In accordance with the present invention, the location of an AWARE-enabled device may be varied.

[0024] For example, an AWARE-enabled device may be co-located with a firewall 106 of a wireless service provider. If such a design is chosen then it may not be necessarily assumed that any other part of the wireless network 1 has knowledge of the presence of the AWARE-enabled device 100 or interacts with the AWARE-enabled device 100.

[0025] In a further embodiment of the present invention, the profiler 101 of such a co-located AWARE-enabled device 100 may use IP layer information, such as packet arrivals and information from IP/TCP and application layer headers, to build profiles. This assumes that the AWARE-enabled device 100 can look inside a packet. If an *IPsec* (tunnel mode) has been enabled, the AWARE-enabled device 100 may be co-located with an *IPsec* gateway in the domain so as to be able to decrypt and inspect packet headers and payloads.

[0026] In a "least-invasive" design, the AWARE-enabled device 100 looks at IP packets that are passed on from the firewall 106 before they reach the PDSN 105. All

of the necessary information is contained in the TCP and IP headers and the payload itself. Information needed by the profiler 101 to build a profile can be extracted from the above headers and payload.

[0027] If a AWARE-enabled device is not co-located with an *IPsec* gateway, there needs to be a so-called security association with the gateway so it can decrypt and process ESP-encapsulated packets in a tunnel mode.

[0028] If an AWARE-enabled device is not co-located with a firewall, an interface may be used to communicate with most commercial firewalls, such as Checkpoint's Firewall-1, so that an AWARE-enabled device may configure the firewall's filters, etc.

[0029] In an alternative embodiment of the present invention, an AWARE-enabled device 100 may operate between a PDSN 105 and an RNC 104. In such a design, the device may interact with the PDSN 105 to obtain information as to how packets are distributed to different RNC's.

[0030] In addition, when an AWARE-enabled device operates between a PDSN and RNC more user-specific state information may be gathered. This provides finer grain information, such as: the number of signaling events for a FCH & SCH setup/release, the timestamp(s) of signaling messages, and power control information via a base station that estimates mobile power consumption. An AWARE-enabled device may also be able to obtain mobility related information because a mobile may cross over from one RNC to another. The impact of mobility information on the detection heuristic is worth analyzing, because highly mobile end-users can contribute significantly to the load of an network. Launching a wireless DoS attack, for example, against highly mobile users requires additional tasks, such as more frequent paging, that can add substantially to processing overhead. Also, a mobile may initiate a PPP connection with the PDSN before initiating a transfer. An AWARE-enabled device may also query the PDSN to obtain a PPP state history.

[0031] An AWARE-enabled device can also query an RNC for channel setup events as well as power control messages that are sent to the mobile to indicate at what power the mobile should transmit the data.

[0032] AWARE-compatible interfaces may also be provided by the present invention. In further embodiments of the present invention, AWARE-compatible interfaces are

ERICSSON EXHIBIT 1005, Page 278

provided to allow an AWARE-enabled device, for example, to query wireless user/mobile state(s). Such an interface may also allow an AWARE-enabled device (or devices) to communicate in a secure manner with elements of a wireless network in order to obtain mobile/user-specific information.

[0033] It should be understood that the methods of the present invention, the AWARE-enabled devices, interfaces, and any subcomponents (e.g., learning database, profiler, detector, etc.) may be realized in hardware, software, firmware or some combination of the three. For example, one or more programmable or programmed controllers, processors, or computer readable mediums, separately or in combination, may be operable to store one or more instructions, programs or code (and data) that, in turn, is operable to carry out the features and functions of the present invention described above and in the claims that follow.

ERICSSON EXHIBIT 1005, Page 279

We claim:

1. A method for detecting an attack against a 3G wireless network comprising:

obtaining wireless state information; and

comparing the obtained information to a profile to determine whether an attack is directed at an element in the network.

2. The method as in claim 1 further comprising preventing malicious traffic intended for a mobile device in the network from reaching the device when the comparison indicates an attack.

3. The method as in claim 1 wherein the state information is collected from one or more network elements in the network.

4. The method as in claim 1 wherein the state information is inferred from knowledge of the network.

5. A device for detecting an attack against a 3G wireless network operable to:

obtain wireless state information; and

compare the obtained information to a profile to determine whether an attack is directed at an element in the network.

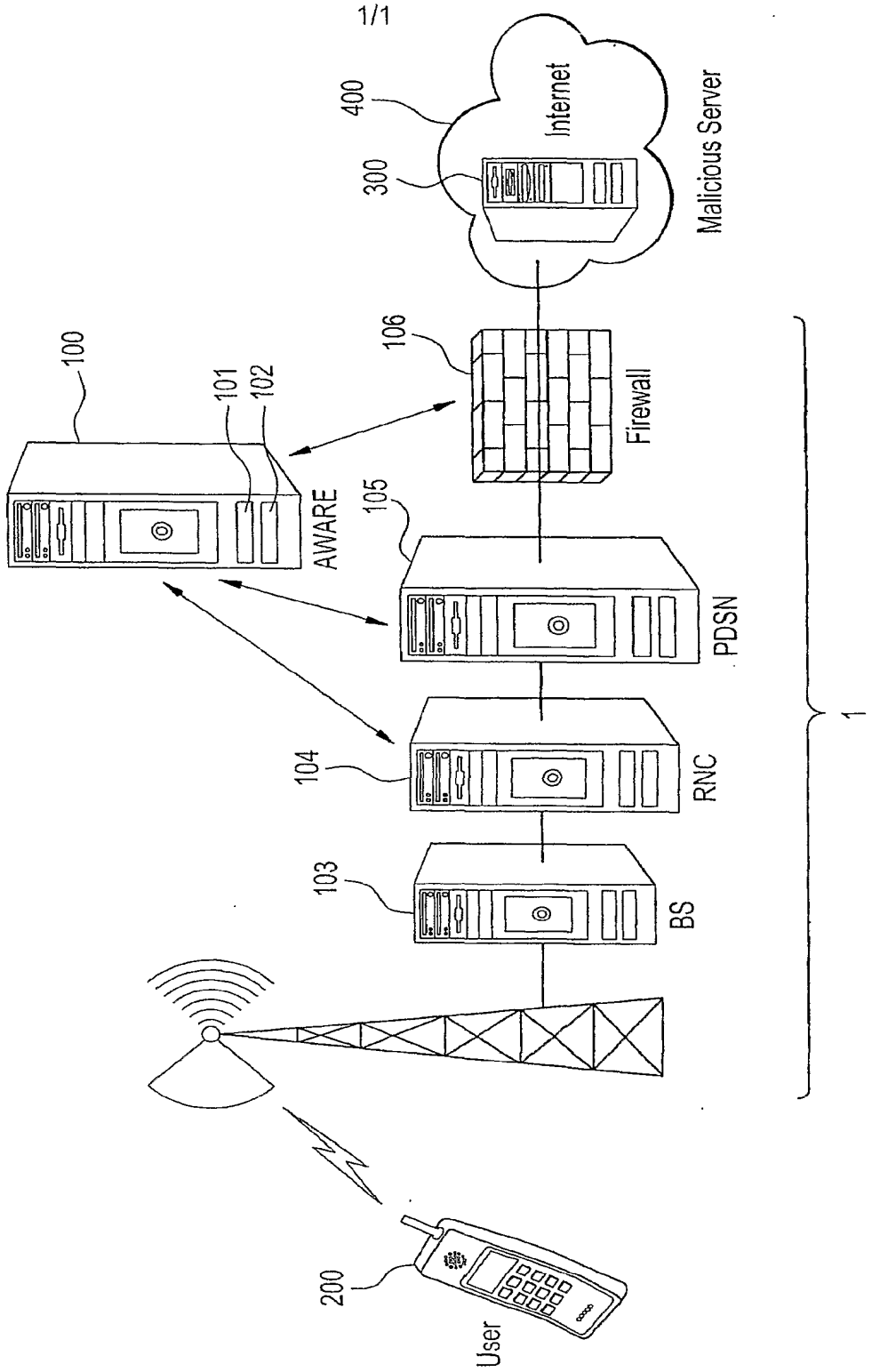
6. The device as in claim 5 further operable to prevent malicious traffic intended for a mobile device in the network from reaching the device when the comparison indicates an attack.

7. The device as in claim 5 wherein the device is further operable to collect the state information from one or more elements in the network.

8. The device as in claim 5 wherein the device is further operable to infer state information from knowledge of the network.

ERICSSON EXHIBIT 1005, Page 280

FIG. 1


Internet
400
300
Malicious Server
106
Firewall
100
101
102
AWARE
105
PDSN
104
RNC
103
BS
1
200
User

(11)Publication number	2006-350561
(43)Date of publication of application	28.12.2006
(51)Int.Cl.	*G06F 13/00 (2006.01)* *G06F 21/20 (2006.01)* *H04L 12/22 (2006.01)*
(21)Application number	2005-174279
(22)Date of filing	14.06.2005
(71)Applicant	MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor	ITO YUKIKO

(54)ATTACK DETECTION DEVICE

(57)Abstract

PROBLEM TO BE SOLVED: To provide an attack detection device for detecting whether or not equipment or a system on a network becomes the step device of a DoS attack or DDoS attack. SOLUTION: An attack detection device is provided with a log collecting means 301 for collecting destination log information showing destination to which information has been transmitted by each equipment from a plurality of registration equipment 104 to 107 and an illegal access judging means 302 for detecting whether or not the number of information to be transmitted from the plurality of registration equipment 104 to 107 to the same destination exceeds a predetermined threshold based on the collected destination log information, and for judging that any illegal access to the destination has occurred when detecting that the information whose number exceeds the threshold has been transmitted to the same destination.

ERICSSON EXHIBIT 1005, Page 282

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

The present invention relates to the technology of coping with unlawful access to apparatus and the system on a communication network, and relates to the attack detection device which detects the distributed denial of service attacks to apparatus and the system on a communication network especially.

[Background of the Invention]

[0002]

In recent years, Web access and service using networks including an E-mail are increasing increasingly with the spread of the Internet. However, on the other hand, the increase also of the danger that normal employment of service will be barred, and its measure are needed by unlawful access and the virus through a network.

[0003]

For example, the measure of installing a firewall and an intrusion detection system (IDS:Intrusion Detection System) in a network is the typical thing. In IDS, it checks by the rule called the "signature" which described the attack pattern of the attack detection target, and detects an attack.

[0004]

In however, the case of the denial-of-service attack (DoS:Denial of Services) which bars normal employment of the system of an attack place by transmitting a lot of [intentionally] processing demand. Since a processing demand of each was what is used at the time of normal, IDS was difficult to detect this attack by a signature. In the case of the distributed denial of service attacks (DDoS:Distributed Denial of Services) which the attacking agency is distributing on a network especially. An aggressor creates many step equipment on a network, and the attack origin used as step equipment publishes a processing demand to the same address simultaneously. For this reason, it was difficult to distinguish also quantitatively the processing demand which each of step equipment publishes from the thing at the time of normal.

[0005]

Fig.2 is an imaged figure of the network in the state where the DDoS attack was performed. In Fig.2, the aggressor 201 enters into apparatus, or infects apparatus with a virus, and creates many pieces of step equipment via the network 202. For example, as shown in Fig.2, the aggressor 201 creates the step equipment 203-206. The step equipment 203-206 sends out a processing demand simultaneously to the attack-airplane machine 207 according to the mechanism which the aggressor created, for example. Since the attack-airplane machine 207 will receive a processing demand from many step equipment (step equipment 203-206) simultaneously, normal employment will be barred.

[0006]

Conventionally, the following technology is proposed as a solution to a DoS attack or a DDoS attack. For example, the system which performs attack defense processing which detected offensive signs with the edge router of the attacking side, and was determined by the attack defense server with this edge router. (For example, Patent document 1) When the situation of the defense side network is monitored and an attack is detected, Instruct communications control to the apparatus of the unlawful access side

ERICSSON EXHIBIT 1005, Page 283

network, and it searches the inflow way of unlawful access to the system (for example, Patent document 2) which controls communication of step equipment, and the service currently exhibited by the network, The system (for example, Patent document 3) which prevents unlawful access with the router of an inflow way is proposed.

[0007]

Such a conventional system performs attack defense processing to a DoS attack or a DDoS attack by the simple substance processing of the routers 208-216 or cooperation processing which exists in a network.

[Patent document 1] JP,2004-328307,A

[Patent document 2] JP,2002-158660,A

[Patent document 3] JP,2004-280724,A

[Description of the Invention]

[Problem to be solved by the invention]

[0008]

conventionally, the system which performs attack defense processing as technology of coping with a DoS attack and a DDoS attack, to the signs which detected offensive signs and were detected in the edge router and network near the attack-airplane machine which receive an attack is proposed.

[0009]

For example, the system (Patent document 1) which detects an attack with an edge router and performs attack defense processing, and the defense side network detect an attack, The system (Patent document 2) which performs attack defense processing by the apparatus of the unlawful access side network, and the system which searches the inflow way of unlawful access and performs defense processing to unlawful access with the router of an inflow way are proposed.

[0010]

Cooperation can be taken among apparatus, such as a router which exists on a network, an attack-airplane machine can detect the DoS attack and that the DDoS attack was carried out, and these systems can carry out defense processing so that an attack-airplane machine may not carry out a system failure. However, in order to specify an attacking agency or to carry out defense processing near an attacking agency, it is necessary to search sequentially from the router near the attack-airplane machine, and to specify attacking agency apparatus, and the time and effort and load for search are applied. For this reason, to attacking agency apparatus, a security patch may be hit or management processing of performing attack defense processing to the router near attacking agency apparatus may not delay. The processing to which a security patch is hit is processing which corrects the software of the apparatus which received the attack. Attack defense processing is processing to which an abnormal packet and an abnormality message are made not to be sent out from a router.

[0011]

In the conventional system, about the attack packet which had the transmitting agency camouflaged, since the attack origin cannot be specified, the apparatus which became step equipment by the DoS attack or the DDoS attack cannot be specified.

[0012]

The conventional system may perform attack defense processing with the router near the attack-airplane machine, and cannot prevent an attack packet from consuming a network resource in this case.

[0013]

By the present invention, it is detected from the above thing whether apparatus and the system on a network are step equipment of the attack in response to the DoS attack or the DDoS attack, It aims at providing the attack detection device which instructs the maintenance processing to step equipment, and the attack defense processing to the router step equipment or near the step equipment.
[Means for solving problem]
[0014]
The attack detection device of the present invention collects the address log information which is transmitted from each of a plurality of apparatus and which shows the address to which each aforementioned apparatus transmitted information, When it detects that the number of the information transmitted to the same address is over a predetermined threshold value from said plurality of apparatus based on the address log information which the log collecting means which totals, and the aforementioned log collecting means totaled, It has an unlawful access determination means judged that unlawful access to the address occurred.
[0015]
The apparatus which has transmitted information to the address it was judged that it was accessed unlawfully to the attack detection device of the present invention among said plurality of [determination means / aforementioned / unlawful access] apparatus in the aforementioned attack detection device is specified from the aforementioned address log information which shows the address.
[0016]
The attack detection device of the present invention is a time of it being detected in the aforementioned attack detection device that unlawful access is performed by the aforementioned unlawful access determination means. It has a maintenance processing directing means which instructs the maintenance processing to a plurality of apparatus which transmitted the aforementioned address log information.
[0017]
The attack detection device of the present invention is a time of it being detected in the aforementioned attack detection device that unlawful access is performed by the aforementioned unlawful access determination means. It has an attack defense processing instruction means to instruct attack defense processing in which the router on the course from the address by which unlawful access is carried out [aforementioned] to a plurality of apparatus which transmitted the aforementioned address log information, or said plurality of apparatus is received.
[0018]
In the aforementioned attack detection device, the aforementioned log collecting means totals the aforementioned address log information for every classification of the aforementioned apparatus, and, as for the attack detection device of the present invention, the aforementioned threshold value is set up for every classification of the aforementioned apparatus.
[0019]
The address log collecting means which collects the address log information which shows the address to which the offensive and defensive systems of the present invention transmitted information, A plurality of apparatus which has respectively a log transmission means which transmits the address log information which the aforementioned address log collecting means collected, The aforementioned address log information transmitted from each aforementioned log transmission means of said plurality

ERICSSON EXHIBIT 1005, Page 285

of apparatus is collected, When it detects that the number of the information transmitted to the same address is over a predetermined threshold value from said plurality of apparatus based on the address log information which the log collecting means which totals, and the aforementioned log collecting means totaled, It has an attack detection device which has an unlawful access determination means judged that unlawful access to the address occurred.

[0020]

It is characterized by an attack detecting method of the present invention comprising the following.

A step which collects address log information which is transmitted from each of a plurality of apparatus, and which shows an address to which each aforementioned apparatus transmitted information.

A step which totals address log information which collected [aforementioned].

A step judged that unlawful access to the address occurred when it detects that the number of information transmitted to the same address is over a predetermined threshold value from said plurality of apparatus based on address log information which totaled [aforementioned].

[Effect of the Invention]

[0021]

According to the attack detection device of the present invention, the address log information which shows the address to which the aforementioned apparatus transmitted information from a plurality of apparatus decided preliminarily is collected, Total and it is detected from said plurality of apparatus whether the number of the information transmitted to the same address is over the threshold value set up preliminarily based on the aforementioned address log information, Since it judged whether it would be accessed unlawfully to the address, it is detectable whether said plurality of apparatus is accessing unlawfully by becoming a step of the attack in response to a DoS attack or a DDoS attack.

[0022]

In [according to the attack detection device of the present invention] the aforementioned attack detection device, From having had a means to instruct the maintenance processing to a plurality of apparatus which transmitted the aforementioned address log information, when unlawful access was detected, It can instruct so that maintenance processing of hitting a security patch to a means to perform maintenance processing to a plurality of apparatus, to the apparatus made a steppingstone by the DoS attack or a DDoS attack may be performed.

[0023]

In [according to the attack detection device of the present invention] the aforementioned attack detection device, A plurality of apparatus which transmitted the aforementioned address log information when unlawful access was detected, Or from having had a means to instruct the attack defense processing to the router on the course from the address which is an attack place of unlawful access to said plurality of apparatus, It can instruct so that attack defense processing in which a DoS attack and a DDoS attack restrict transmission of an abnormal packet or an abnormality message to a means to perform attack defense processing to apparatus or a router, to the router near the apparatus or it which was made a steppingstone may be performed. As a result, it can stop immediately in the place near consumption of resource of network by transmission of abnormal packet or abnormality message attack-origin.

[0024]

ERICSSON EXHIBIT 1005, Page 286

In [according to the attack detection device of the present invention] the aforementioned attack detection device, the aforementioned address log information is totaled for every classification of the aforementioned apparatus, and since the aforementioned threshold value used for judgment of unlawful access was managed for every classification of the aforementioned apparatus, according to the use and function of the aforementioned apparatus, the threshold value over the address of the aforementioned apparatus is set up easily -- things can be carried out.

[Best Mode of Carrying Out the Invention]

[0025]

Hereinafter, about an embodiment of the invention, while referring to Drawings, it describes.

(Embodiment 1)

Fig.1 is an imaged figure of the network to which the attack detection device concerning the embodiment 1 of the present invention is applied. As shown in Fig.1, the attack detection device 101 manages a plurality of registration machine machines, and it is detected whether the registration machine machine is a step of the attack from the aggressor 201 in response to the DoS attack or the DDoS attack. And if unlawful access with a registration machine machine is detected, it will instruct to the maintenance processing means 102 so that maintenance processing, such as hitting a security patch to a registration machine machine, may be performed. It instructs to the attack defense processing means 103 so that attack defense processing of restricting sending out of an abnormal packet or an abnormality message may be performed to the router near a registration machine machine or a registration machine machine.

[0026]

The configuration example of the network system containing the attack detection device 101 concerning this embodiment 1 and the attack detection device 101 is shown in Fig.3.

A system shown in Fig.3 is provided with the following.

Attack detection device 101.

The registration machine machines 104-107 which the attack detection device 101 manages.

Maintenance processing means 102.

Attack defense processing means 103.

Suppose that it is the registration machine machines 104-107 apparatus of an identical kind in Fig.3.

[0027]

The attack detection device 101 is provided with the following.

The log collecting means 301 which collects address log information which shows an address to which each apparatus transmitted information from the registration machine machines 104-107, and totals.

The unlawful access determination means 302 which judges whether the registration machine machines 104-107 have accessed unlawfully in an attack-airplane machine based on address log information.

The maintenance processing directing means 303 which instructs maintenance processing to the maintenance processing means 102 when the unlawful access determination means 302 detects unlawful access.

The attack defense processing instruction means 304 to instruct attack defense processing to the attack defense processing means 103 when the unlawful access determination means 302 detects unlawful access.

ERICSSON EXHIBIT 1005, Page 287

[0028]
The maintenance processing means 102 performs maintenance processing to all the registration machine machines of the identical kind registered preliminarily based on the instruction from the maintenance processing directing means 303. In Fig.3, since the registration machine machines 104-107 are apparatus of an identical kind, maintenance processing, such as hitting a security patch to the registration machine machines 104-107, is performed.
[0029]
The attack defense processing means 103 performs attack defense processing to the router which exists on the course from a registration machine machine or a registration machine machine to an attack-airplane machine based on the instruction from the attack defense processing instruction means 304. For example, as shown in Fig.1, when the registration machine machine 105 becomes step equipment, by asking the registration machine machine 105, on the course to the attack-airplane machine 207, the router 210 near the registration machine machine 105 is specified, and attack defense processing is performed to the router 210. When attack defense processing cannot be performed to the router 210, it is made to perform attack defense processing to other routers on a course, such as the router 209. Same attack defense processing is performed also to the router on the course from a registration machine machine (registration machine machine 104,106,107) to the attack-airplane machine 207 of the identical kind registered preliminarily. This restricts that an abnormal packet, an abnormality message, etc. are sent out from step equipment in a network in the place near an attacking agency, and it can avoid useless consumption of a network resource.
[0030]
The registration machine machines 104-107 are provided with the following.
The address log collecting means 305 which collects address log information which shows an address (for example, other apparatus, terminals, and servers) which transmitted information.
The log transmission means 306 which transmits address log information which the address log collecting means 305 collected to the log collecting means 301 of the attack detection device 101.

[0031]
Since the registration machine machines 104-107 can make 1 conclusion log information which the kind of log to collect is limited and overlaps even if it has the address log collecting means 305 and the log transmission means 306, Neither the load of the processing which collects address log information, nor the load which communicates address log information enlarges.
[0032]
It may be made for the registration machine machines 104-107 to be provided with a maintenance processing execution means. A maintenance processing execution means performs maintenance processing, such as hitting a security patch, based on the instruction from the maintenance processing means 102, further, upgrades software with application of a security patch, and copes with an attack.
[0033]
It may be made for the registration machine machines 104-107 to be provided with an attack defense processing performing means. Based on the instruction of the attack defense processing means 103, an attack defense processing performing means changes setting out of a firewall, or restricts sending out of an abnormal packet or an abnormality message. It may be made for each router shown in Fig.1 to be

ERICSSON EXHIBIT 1005, Page 288

provided with such an attack defense processing performing means.
[0034]
Next, it describes using Fig.4 - Fig.8 about operation of the attack detection device 101.
Fig.4 is a flow chart showing the contents of processing which the attack detection device 101 performs. Fig.5 and Fig.6 are the figures showing the address log information which the registration machine machine 104 and the registration machine machine 105 transmit, respectively. The address log information shown in Fig.5 and Fig.6 is the list which made the group the number of the destination IP addresses with which the registration machine machine 104 and the registration machine machine 105 transmitted information, and the information transmitted to each address, respectively. "AA.AA.AA.AA", "BB.BB.BB.BB", "XX.XX.XX.XX", "YY.YY.YY.YY", and "ZZ.ZZ.ZZ.ZZ" are character strings which show destination IP addresses, respectively. "Numbers" is a "transmitting packet number", the "number of outgoing messages", and a "session set number", for example, and which number is used determines preliminarily. Fig.7 is the list which carried out the group of destination IP addresses and the address summary value which is the totaled results of address log information. Fig.8 is the list which carried out the group of destination IP addresses and the threshold value which the attack detection device 101 has managed.
[0035]
First, the log collecting means 301 obtains address log information from the registration machine machines 104-107 every definite period of time (Step S401).
Next, the log collecting means 301 totals the collected address log information (Step S402). As shown in Fig.7, the log collecting means 301 totals a "number" for every same address IP. For example, about address IP "ZZ.ZZ.ZZ.ZZ", the number "1" with which the registration machine machine 104 transmitted information, and the number "1" with which the registration machine machine 105 transmitted information are added, and an address summary value is set to "2." It is similarly totaled about other address IP.
[0036]
Next, the unlawful access determination means 302 judges whether the address summary value of un-reference exists (Step S403), and performs comparison with an address summary value and a threshold value for every address IP sequentially (Step S404). Since the unlawful access determination means 302 is not over the threshold value about address IP "XX.XX.XX.XX", "AA.AA.AA.AA", and "BB.BB.BB.BB" among address summary values, it is judged that it is normal (Step S405). About address IP "YY.YY.YY.YY", since the threshold value is not set up, it is judged that it is normal. On the other hand, about address IP "ZZ.ZZ.ZZ.ZZ", since the address summary value is "2" and is over the threshold value "1", it is judged that unlawful access to address IP "ZZ.ZZ.ZZ.ZZ" occurred (Step S406).
[0037]
Next, if unlawful access is detected, as for the maintenance processing directing means 303, maintenance processing will be instructed to the maintenance processing means 102, and the attack defense processing instruction means 304 will instruct attack defense processing to the attack defense processing means 103. That is, the attack detection device 101 instructs unlawful access management processing to the maintenance processing means 102 and the attack defense processing means 103 (Step S407).
[0038]

ERICSSON EXHIBIT 1005, Page 289

After comparing an address summary value with a threshold value sequentially as mentioned above and completing all the comparison, a series of attack detecting operation is ended (Step S408). And same operation is again performed to the following log acquisition timing.

[0039]

Although Fig.5 and 6 showed the list with destination IP addresses and the information number transmitted to each address as an example of the address log information which the registration machine machines 104-107 transmit, the address log information should just be information which does not restrict to this and shows a transmission destination. For example, "address URL" and a "mail address" may be shown as an address.

[0040]

In Fig.5 - Fig.8, although the "number" is shown as one kind, a threshold value is not limited to one kind. For example, it is possible to set as a threshold value combining numbers, such as a "transmitting packet number", the "number of outgoing messages", and a "session set number."

[0041]

The list in which it does not restrict to the list shown in Fig.5 and Fig.6, and only an address is shown may be sufficient as the address log information which a registration machine machine transmits. Fig.9 is the figure showing an example of the address log information which shows only an address (address URL). The attack detection device 101 which received the address log information shown in Fig.9 will not be inspected about the number of the address which one set of a registration machine machine transmitted, but it will be inspected whether information is simultaneously transmitted to the same address from a plurality of registration machine machines. In the list which address log information shows to Fig.9, the log collecting means 301 will total "the number of registration machine machines", as shown in Fig.10. In this case, even if multiple information is transmitted to the same address from one registration machine machine, it totals by regarding it as 1. And a threshold value [summary value / determination means / 302 / unlawful access] turns into "a threshold value of the number of registration machine machines" set up for every address, as shown in Fig.11. In this case, it is judged that unlawful access to "http://www.bbbb" generated the unlawful access determination means 302 since the number of the registration machine machines which transmitted information to address URL of "http://www.bbbb" exceeded the threshold value.

[0042]

It may be made to set up for every classification of a registration machine machine about the threshold value managed with the attack detection device 101. In this case, total processing of address log information is performed for every classification of a registration machine machine. "The classification of a registration machine machine" here means the classification which specifies the use of apparatus, such as a "telephone", a "network camera", "PC", and a "DVD recorder", and its function, for example. If the use and function of a registration machine machine are specified, it will become possible to define the threshold value to the transmission destination easily. For example, if it is the "telephone" which has only the function to perform communication between 2 persons, any communication destinations other than the server which performs special processing of call control etc. will not overlap by a plurality of apparatus. For this reason, when information is transmitted to the same address from a plurality of apparatus, it can be judged as unlawful access. When exceeding the number of the limits transmitted on specification also about access to a server, a threshold value can also be set up as judging it as unlawful

ERICSSON EXHIBIT 1005, Page 290

access.
[0043]
As mentioned above, according to the attack detection device concerning this embodiment 1, each registration machine machine obtains the address log information which shows the address which transmitted information from a plurality of managed registration machine machines (registration machine machines 104-107), Since it judged whether the registration machine machine would access unlawfully based on the address log information, it is detectable whether the registration machine machine serves as a step of the attack in response to the DoS attack or the DDoS attack.
[0044]
When unlawful access is detected according to the attack detection device concerning this embodiment 1, Since it had the maintenance processing directing means 303 which instructs maintenance processing to the maintenance processing means 102, the maintenance processing to the registration machine machine which became the attacking agency in response to the DoS attack or the DDoS attack can be instructed.
[0045]
The attack detection device concerning this embodiment 1, Since it had the attack defense processing instruction means 304 to instruct attack defense processing to the attack defense processing means 103 when unlawful access was detected, the attack defense processing to the router near the registration machine machine which became the attacking agency in response to the DoS attack or the DDoS attack, or the registration machine machine can be instructed. As a result, it can hold down that an abnormal packet and an abnormality message consume a network resource in the place near the registration machine machine which became the attacking agency.
[0046]
(Embodiment 2)
The attack detection device concerning the embodiment 2 of the present invention specifies the registration machine machine in which it is accessing unlawfully.
By this embodiment 2, the attack detection device 101 processes first Step S401 - Step S406 which are shown in Fig.4. And when the unlawful access determination means 302 detects generating of unlawful access, it specifies the registration machine machine in which it is accessing unlawfully. Fig.12 is a flow chart showing the contents of processing which specify the registration machine machine in which the unlawful access determination means 302 is accessing unlawfully.
[0047]
First, it judges whether the unlawful access determination means 302 has a registration machine machine which is not referring to address log information (Step S1201), and refers to the address log information of the registration machine machine of un-reference (Step S1202). And it judges whether the address to which a number exceeding a threshold value of information was transmitted is contained in address log information (Step S1203), and it is judged whether the registration machine machine is accessing unlawfully (Step S1204, Step S1205). If the registration machine machine in which it is accessing unlawfully is detected, the unlawful access determination means 302 will notify the information on the registration machine machine to the maintenance processing directing means 303 and the attack defense processing instruction means 304. Then, the maintenance processing directing means 303 instructs maintenance processing to the maintenance processing means 102, and it notifies

ERICSSON EXHIBIT 1005, Page 291

the information on the registration machine machine in which it has accessed unlawfully. The attack defense processing instruction means 304 instructs attack defense processing to the attack defense processing means 103, and it notifies the information on the registration machine machine in which it has accessed unlawfully.

[0048]

For example, when transmitting the address log information the registration machine machine 105 indicates the address log information which the registration machine machine 104 shows to Fig.4 to be to Fig.5 to the attack detection device 101, as shown in Fig.7 and 8. Since the "number" of address IP "ZZ.ZZ.ZZ.ZZ" exceeds a threshold value, the unlawful access determination means 302, It judges that unlawful access is performed to address IP "ZZ.ZZ.ZZ.ZZ", and the registration machine machine 104 which has transmitted information to address IP "ZZ.ZZ.ZZ.ZZ", and the registration machine machine 105 specify that it is the registration machine machine in which it is accessing unlawfully.

[0049]

When transmitting the address log information containing only address URL as the registration machine machines 104-107 show to Fig.9 to the attack detection device 101, as shown in Fig.10 and Fig.11. Since the number of the registration machine machines which transmit information to address URL "http://wwww.bbbb" exceeds a threshold value, it specifies that it is the registration machine machine in which the registration machine machine which has transmitted information to this address URL is accessing unlawfully.

[0050]

As mentioned above, when it detects that the registration machine machine to manage is accessing unlawfully according to the attack detection device concerning this embodiment 2, From specifying the registration machine machine in which it has accessed unlawfully from address log information, and having notified the information on the registration machine machine to the maintenance processing means 102 and the attack defense processing means 103, The maintenance processing means 102 can carry out maintenance processing only to the registration machine machine in which it is accessing unlawfully, or can carry out maintenance processing to order from the registration machine machine in which it is accessing unlawfully. The attack defense processing means 103 carries out attack defense processing only to the router on the course from the registration machine machine in which it is accessing unlawfully, or the registration machine machine to an attack-airplane machine, or, Attack defense processing can be carried out to order from the router on the course from the registration machine machine in which it is accessing unlawfully, or the registration machine machine to an attack-airplane machine.

[Industrial applicability]

[0051]

The present invention is useful as an attack detection device which detects on a network that apparatus, such as a network connected home appliance and an IP phone, received the DoS attack and the DDoS attack, and prevents apparatus serving as step equipment of a DoS attack or a DDoS attack.

[Brief Description of the Drawings]

[0052]

[Drawing 1]It is an imaged figure of the network containing the attack detection device concerning the embodiment 1 of the present invention.

ERICSSON EXHIBIT 1005, Page 292

[Drawing 2]It is an imaged figure of the network in the state where the DDoS attack was performed.
[Drawing 3]It is the figure showing the configuration example of a network system which has an attack detection device concerning the embodiment 1 of the present invention.
[Drawing 4]It is a flow chart showing the contents of processing which the attack detection device concerning the embodiment 1 of the present invention performs.
[Drawing 5]The attack detection device concerning the embodiment 1 of the present invention is the figure showing an example of the address log information received from a registration machine machine.
[Drawing 6]The attack detection device concerning the embodiment 1 of the present invention is the figure showing an example of the address log information received from a registration machine machine.
[Drawing 7]The attack detection device concerning the embodiment 1 of the present invention is the figure showing an example of the result of having totaled the address log information received from the registration machine machine.
[Drawing 8]It is the figure showing an example of the threshold value which the attack detection device concerning the embodiment 1 of the present invention has managed.
[Drawing 9]The attack detection device concerning the embodiment 1 of the present invention is the figure showing an example of the address log information received from a registration machine machine.
[Drawing 10]The attack detection device concerning the embodiment 1 of the present invention is the figure showing an example of the result of having totaled the address log information received from the registration machine machine.
[Drawing 11]It is the figure showing an example of the threshold value which the attack detection device concerning the embodiment 1 of the present invention has managed.
[Drawing 12]It is a flow chart showing the contents of processing which the attack detection device concerning the embodiment 2 of the present invention performs.
[Explanations of letters or numerals]
[0053]
101 Attack detection device
102 Maintenance processing means
103 Attack defense processing means
104-107 Registration machine machine
201 Aggressor
202 Network
203 - 206 step equipment
207 Attack-airplane machine
208-216 Router
301 Log collecting means
302 Unlawful access determination means
303 Maintenance processing directing means
304 Attack defense processing instruction means

ERICSSON EXHIBIT 1005, Page 293

305 Address log collecting means
306 Log transmission means

ERICSSON EXHIBIT 1005, Page 294

CLAIMS

[Claim(s)]

[Claim 1]

A log collecting means which collects address log information which is transmitted from each of a plurality of apparatus, and which shows an address to which each aforementioned apparatus transmitted information, and totals,

An unlawful access determination means judged that unlawful access to the address occurred when it detects that the number of information transmitted to the same address is over a predetermined threshold value from said plurality of apparatus based on address log information which the aforementioned log collecting means totaled,

An attack detection device characterized by preparation ******.

[Claim 2]

In the attack detection device according to claim 1,

The aforementioned unlawful access determination means,

An attack detection device specifying apparatus which has transmitted information to an address it was judged that it was accessed unlawfully among said plurality of apparatus from the aforementioned address log information which shows the address.

[Claim 3]

In the attack detection device according to claim 1 or 2,

When it is detected that unlawful access is performed by the aforementioned unlawful access determination means, it has a maintenance processing directing means which instructs maintenance processing to a plurality of apparatus which transmitted the aforementioned address log information,

An attack detection device characterized by things.

[Claim 4]

In the attack detection device according to any one of claims 1 to 3,

When it is detected that unlawful access is performed by the aforementioned unlawful access determination means, It has an attack defense processing instruction means to instruct attack defense processing in which a router on a course from an address by which unlawful access is carried out [aforementioned] to a plurality of apparatus which transmitted the aforementioned address log information, or said plurality of apparatus is received,

An attack detection device characterized by things.

[Claim 5]

In the attack detection device according to claim 1,

The aforementioned log collecting means totals the aforementioned address log information for every classification of the aforementioned apparatus,

The aforementioned threshold value is set up for every classification of the aforementioned apparatus,

An attack detection device characterized by things.

[Claim 6]

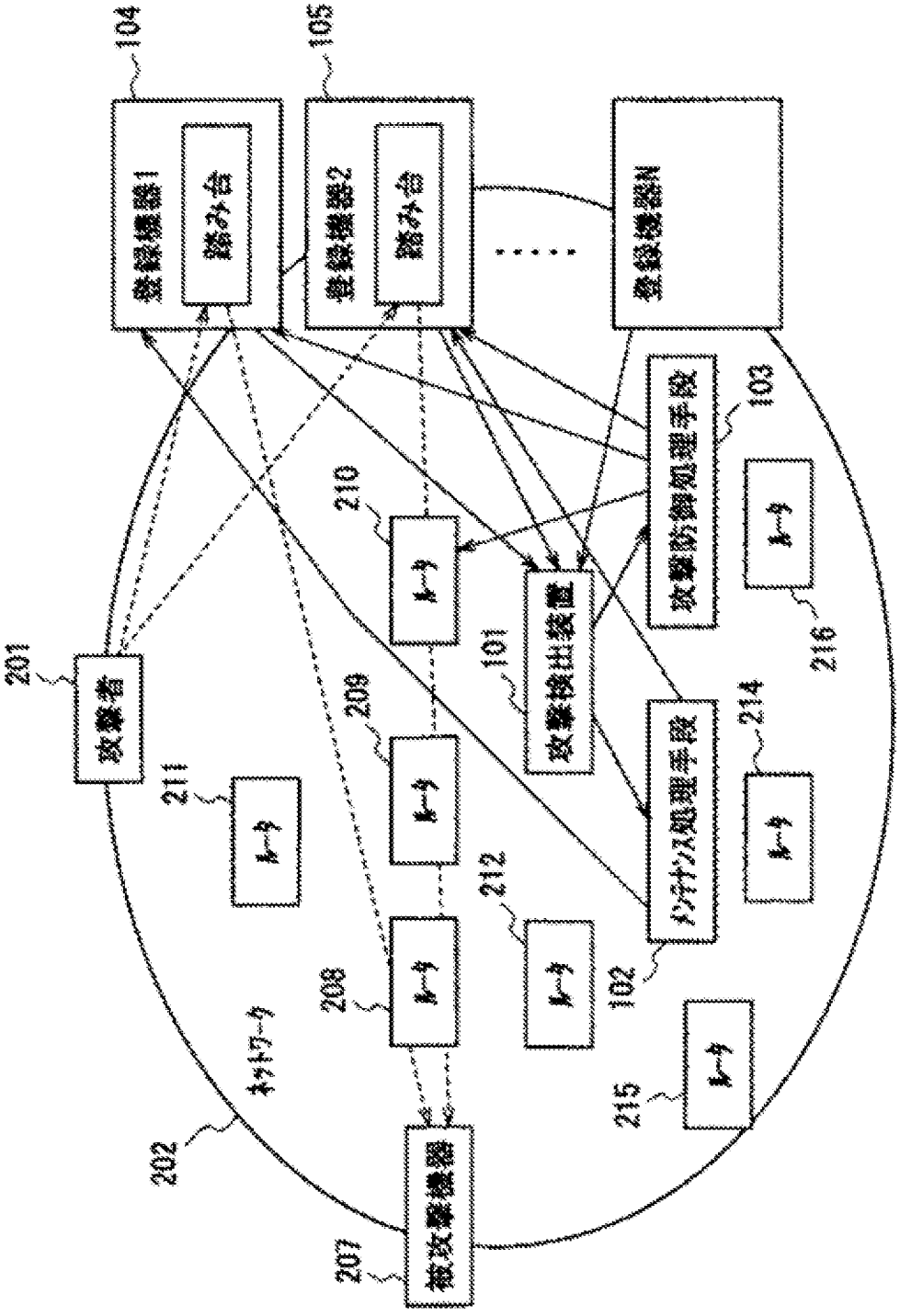
A plurality of apparatus which has respectively an address log collecting means which collects address log information which shows an address which transmitted information, and a log transmission means which transmits address log information which the aforementioned address log collecting means collected,

ERICSSON EXHIBIT 1005, Page 295

The aforementioned address log information transmitted from each aforementioned log transmission means of said plurality of apparatus is collected, When it detects that the number of information transmitted to the same address is over a predetermined threshold value from said plurality of apparatus based on address log information which a log collecting means which totals, and the aforementioned log collecting means totaled, An attack detection device which has an unlawful access determination means judged that unlawful access to the address occurred,
An attack detection system characterized by preparation ******.
[Claim 7]
A step which collects address log information which is transmitted from each of a plurality of apparatus, and which shows an address to which each aforementioned apparatus transmitted information,
A step which totals address log information which collected [aforementioned],
A step judged that unlawful access to the address occurred when it detects that the number of information transmitted to the same address is over a predetermined threshold value from said plurality of apparatus based on address log information which totaled [aforementioned],
****** -- an attack detecting method characterized by things.

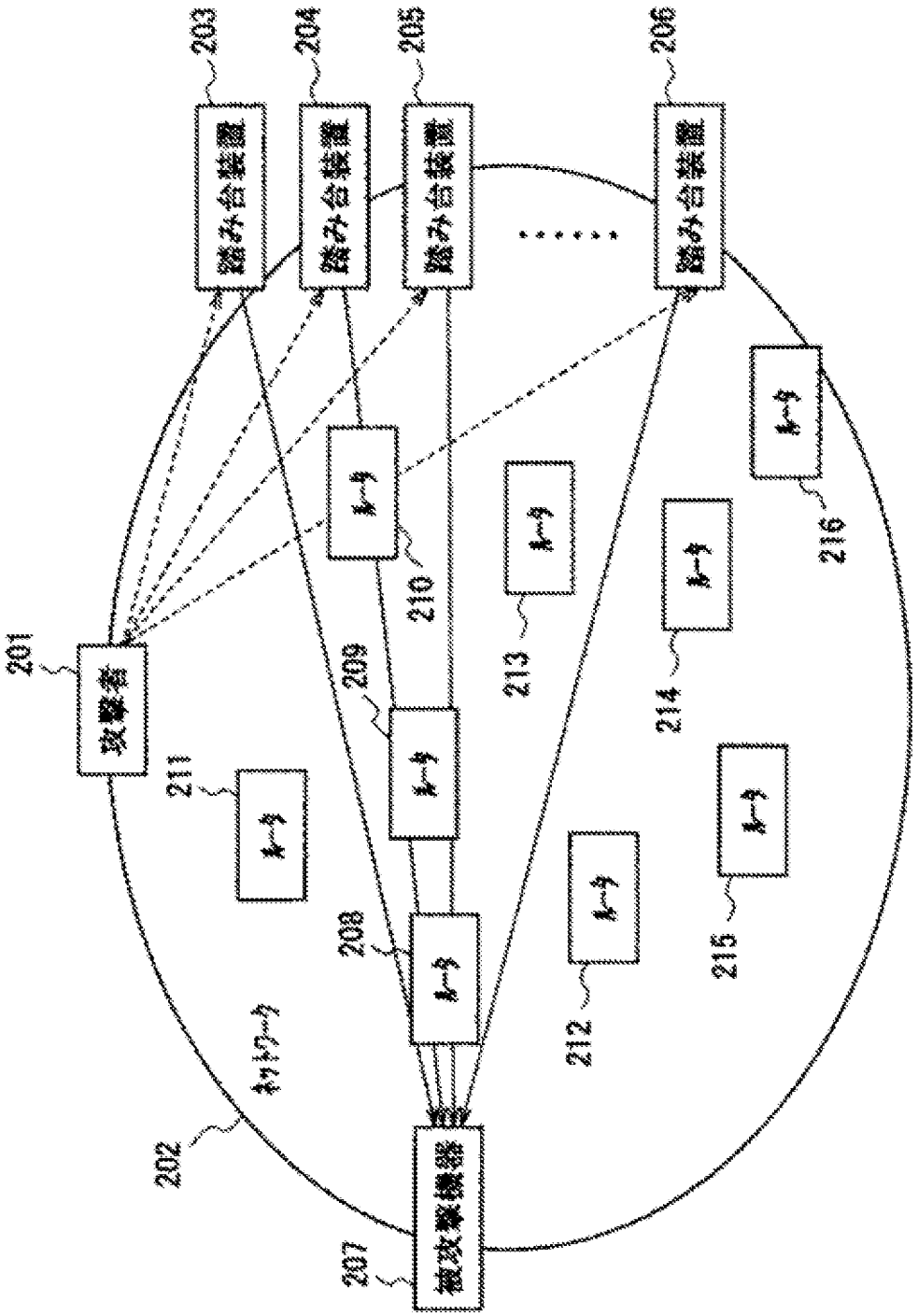
ERICSSON EXHIBIT 1005, Page 296

DRAWINGS



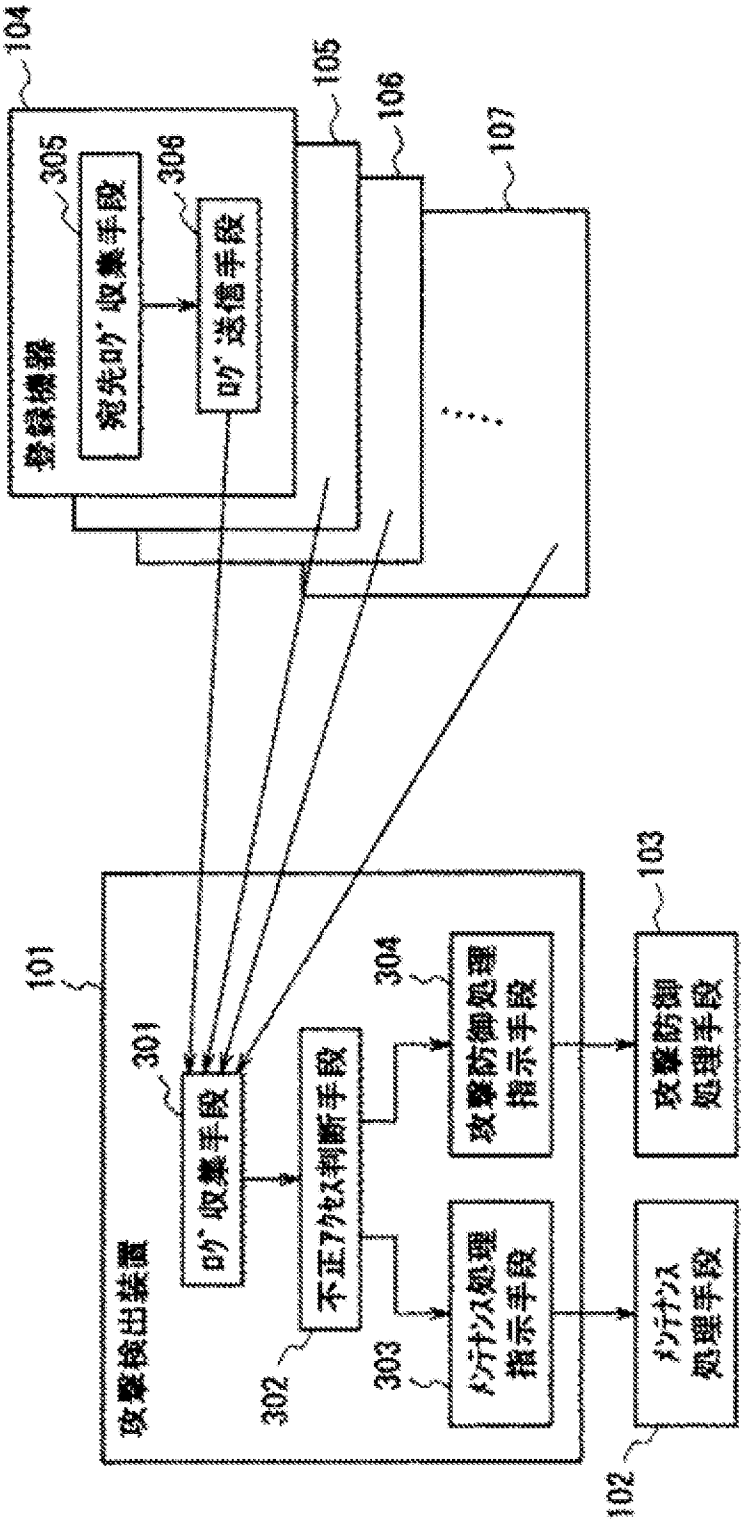
[Drawing 1]

ERICSSON EXHIBIT 1005, Page 297



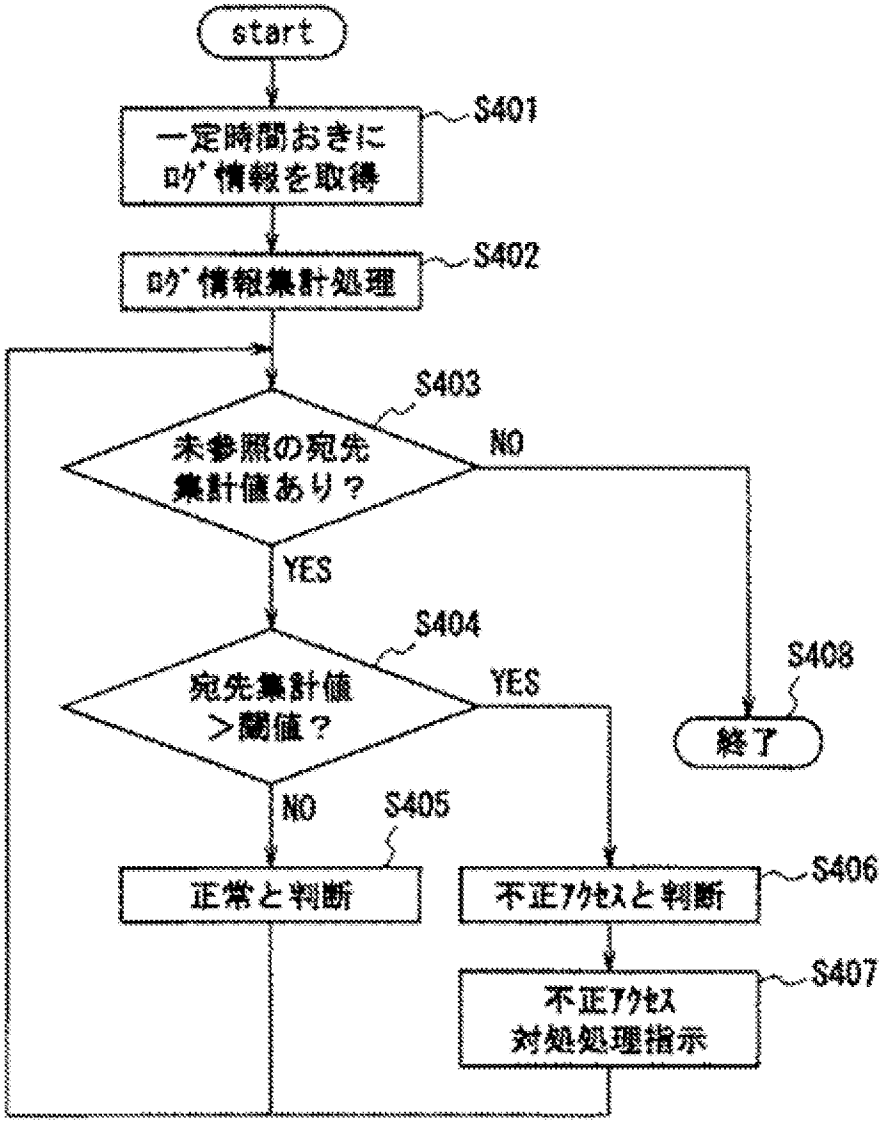
[Drawing 2]

ERICSSON EXHIBIT 1005, Page 298



[Drawing 3]

ERICSSON EXHIBIT 1005, Page 299



[Drawing 4]

ERICSSON EXHIBIT 1005, Page 300

宛先IP	数
XX.XX.XX.XX	1
YY.YY.YY.YY	5
ZZ.ZZ.ZZ.ZZ	1

[Drawing 5]

宛先IP	数
AA.AA.AA.AA	1
BB.BB.BB.BB	1
YY.YY.YY.YY	3
ZZ.ZZ.ZZ.ZZ	1

[Drawing 6]

宛先IP	宛先集計値
XX.XX.XX.XX	1
YY.YY.YY.YY	8
ZZ.ZZ.ZZ.ZZ	2
AA.AA.AA.AA	1
BB.BB.BB.BB	1

[Drawing 7]

宛先IP	閾値
YY.YY.YY.YY	設定なし
他	1

[Drawing 8]

ERICSSON EXHIBIT 1005, Page 301

宛先URL
http://www.aaa.aaa.aaa/
http://www.bbbb/
http://www.cccccc.cccccc/

[Drawing 9]

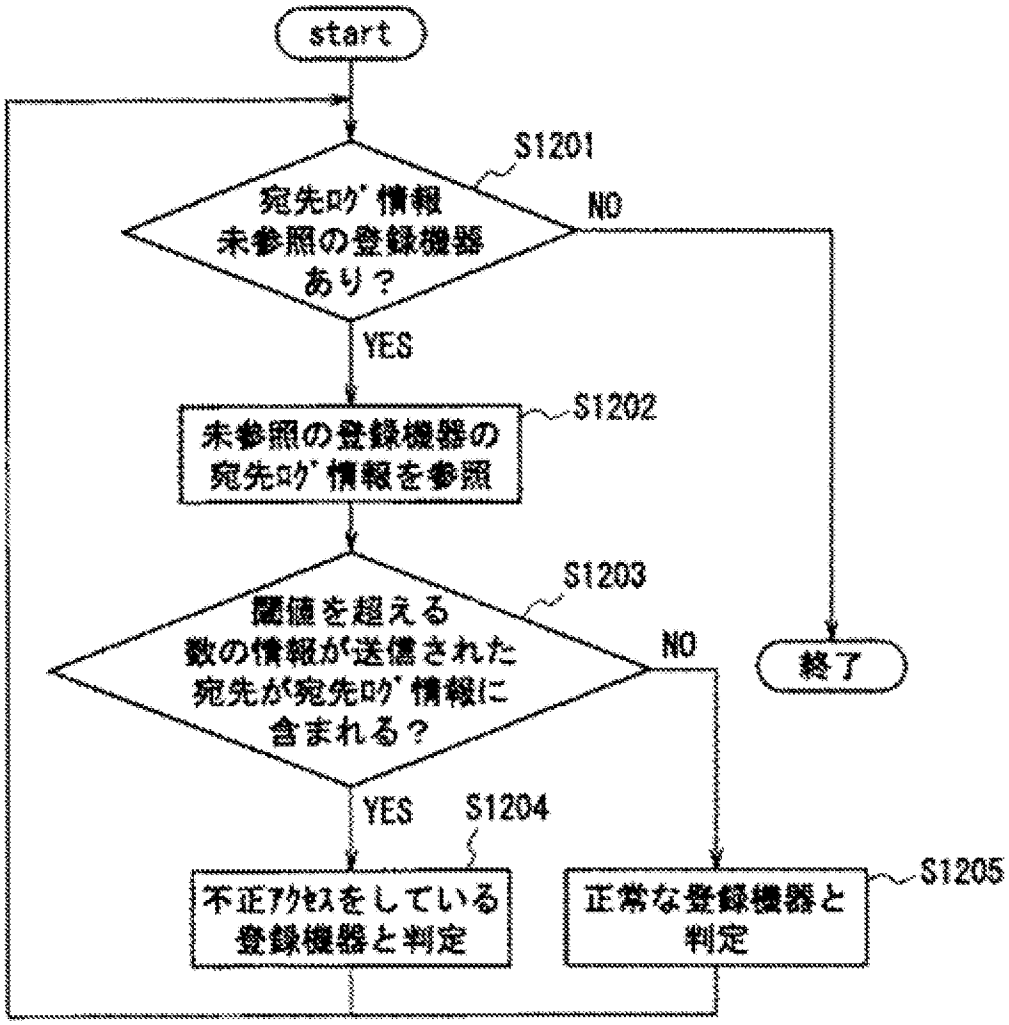
宛先URL	登録機器数
http://www.aaa.aaa.aaa/	1
http://www.bbbb/	2
http://www.cccccc.cccccc/	5

[Drawing 10]

宛先URL	登録機器数の閾値
http://www.cccccc.cccccc/	設定なし
他	1

[Drawing 11]

ERICSSON EXHIBIT 1005, Page 302


start
S1201
宛先ﾛｸﾞ情報
未参照の登録機器
あり？
NO
YES
S1202
未参照の登録機器の
宛先ﾛｸﾞ情報を参照
S1203
閾値を超える
数の情報が送信された
宛先が宛先ﾛｸﾞ情報に
含まれる？
NO
終了
YES
S1204
不正ｱｸｾｽをしている
登録機器と判定
正常な登録機器と
判定
S1205

[Drawing 12]

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 200
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

August 26, 2016 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**380**

Electronic Acknowledgement Receipt

EFS ID:	26763959
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	26-AUG-2016
Filing Date:	21-MAY-2015
Time Stamp:	16:39:19
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$380
RAM confirmation Number	2999
Deposit Account	132490
Authorized User	GRABELSKY, DAVID ANDREW

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

Charge any Additional Fees required under 37 CFR 1.492(a) (basic national fee only)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	15-686-WO-US_Response_10May16_OA.pdf	153566 73bff0b2f269548805c0351504591d2c5d6f5369	no	13
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	15_686_WO_US_Information_Disclosure_Statement_26Aug16.pdf	612415 c7c00f7dc96911fdf73adcc23a2e52fc03442798	no	4
Warnings:					
Information:					
3	Foreign Reference	JP2004-320636.pdf	612354 84e1f55604f16f56ed79f14898c2de2fc76df731	no	20
Warnings:					
Information:					
4	Foreign Reference	JP2006-295240.pdf	1192377 b4f499ff03cff65aeabf09a38c257edcee87944c	no	45
Warnings:					
Information:					
5	Foreign Reference	JP2009-520447_WO2007075423.pdf	434974 d9e52b25d2fc54db0f49fbb47f25f41fc00d7a17	no	9
Warnings:					
Information:					
6	Foreign Reference	JP2006-350561.pdf	642092 d82ae52726cb6cbe2652f7fab8648264906ab858	no	22
Warnings:					
Information:					

7	Extension of Time	15-686-WO-US_Petition_for_one-month_Extension_of_Time.pdf	188319 80aa7272bdeeab2ed4570ef4b6de9d7f2cf22d67	no	2
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	32387 621c90fc64cc799cadb94030e40b94934913b1a7	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	3868484	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **08/26/2016**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 16	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

SLIE
/BARBARA FRIESON/

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	2483
Examiner Name	Vu, Phy Anh Tran
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100064341	A1	2010-03-11	Carlo Aldera	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	KR100628329	KR	B1	2006-09-19	Korea Electronics Telecomm		X

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

	1	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2016-10-26
Name/Print	David A. Grabelsky	Registration Number	59,208

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Bibliotheek voor Ondernemend Nederland

Espacenet

Bibliografische gegevens: KR100628329 (B1) — 2006-09-19

GENERATION APPARATUS AND METHOD OF DETECTION RULES FOR ATTACK BEHAVIOR BASED ON INFORMATION OF NETWORK SESSION

Uitvinder(s):	CHEONG IL AHN [KR]; OH JIN TAE [KR]; JANG JONG SOO [KR] ± (CHEONG, IL AHN, ; OH, JIN TAE, ; JANG, JONG SOO)
Aanvrager(s):	KOREA ELECTRONICS TELECOMM [KR] ± (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE)
Classificatie:	**- internationaal:** ***H04L9/00***
	- cooperative:
Aanvraagnummer:	KR20050069968 20050730
Prioriteitsnummer (s):	KR20050069968 20050730

Er is geen samenvatting beschikbaar voor KR100628329 (B1)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Patent Translate
Powered by EPO and Google

Notice

This translation is machine - generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine - translation output.

DESCRIPTION KR100628329

Information sessions on the network characteristics of the attack behavior detection rule generating apparatus and method {Generation Apparatus and Method of detection rules for attack behavior based on information of network session}

Figure 1 is an overall configuration diagram of a method for automatic generation of rules tamjieul attack behavior based on the attribute information and updating the network session.

Figure 2 (a) is a general statistical information illustrated network session attribute information extraction unit in the session in Fig.

Figure 2 (b) is illustrated network session attribute information extraction unit in the network connection protocol information in FIG.

Figure 2 (c) is illustrated network session attribute information extraction unit in the network protocol header information in Fig.

ERICSSON EXHIBIT 1005, Page 317

Figure 2 (d) and 2 (e) is a connection between the information shown in Figure 1, the network session attribute information extraction unit in the two hosts.

3 is a flow chart for extracting characteristic information of the data collected from the network session attribute information extraction unit 130 of Fig.

Figure 4 is a flow chart for automatically generating a detection rule generating unit in the automatic detection rules shown in Fig.

Figure 5 is a flow diagram for verifying the detected rules created in the detection rule verification unit shown in the detected rule to verify and update the portions in FIG.

6 is a flow chart for updating the accuracy of the detection rule generating the auto detection rule update unit illustrated in Figure 1 to verify and update the detection rule in part.

7 is an overall flow chart for automatically generating a detection rule.

8 is a diagram showing the effect of the present invention as compared with the conventional one attack detection method.

9 is a diagram illustrating the improved accuracy of the detection rule by converting the continuous data into discrete data.

Figure 10 and Figure 11 shows the results of applying the detection rule formed in accordance with an embodiment of the present invention to the experimental data.

The present invention is the accuracy of the attack behavior detection rule automatic generation and automatic update method, and relates to a device, the network session specific characteristics automatically generating a detection rule for each attack behavior for the information, and generate rules for the network session attribute information through more accurate detection rules automatically updated through the

ERICSSON EXHIBIT 1005, Page 318

detection accuracy of calculation, known attacks and similar types of attacks, intended to detect the normal behavior and other types. In general, intrusion detection method is split into a rule - based feature detection and anomaly detection. Feature - based method is to analyze the already known attack packet patterned, and that for determining the attack by checking whether matching that pattern detection accuracy of the known attack is extremely high, transformation of attack behavior or the detection of new attacks unknown there is a limit. Anomaly detection method for overcoming this drawback is used to detect an unknown attack it is mainly that detects attacks by modeling data generated by the normal behavior according to the degree and out the top model. Task of finding the characteristics relating to the network intrusion from a large amount of data is there is analyzed by a knowledge of the most professional, such a method has a high accuracy is high but the cost analysis will drop the ability to respond to new forms of attack. On the other hand, anomaly detection method is effective to detect unknown attacks, characterized by difficult and less accurate than the upset - based features. In addition, the packet network to appear, or a situation with little or no study on the method of utilizing the characteristic information of the network session unit to extract the features of the types of attacks that can not be clearly distinguished from the normal network data flow. The object of the present invention is to produce a high detection accuracy than rule to automatically generate and update the detected attack behavior rules for the network session attribute information in order to solve the above problems.

In a preferred embodiment of the invention, the attack actions detection rule generating apparatus the session attribute information and the normal type, the attack and unknown types of the network data belongs characteristics of a network of data types of the classified network data by the session characteristics network session attribute information extraction unit for converting the input data types, including; and wherein in the end nodes of configuring the decision tree by applying a classification algorithm, on the input data format in the converted network data, the decision tree based on the error rate, It generates the accuracy of the decision tree, for generating the network data type of the attribute, the optimal condition and the patterned detection rules to the network data type on the basis of the accuracy for selecting the node having an information gain of the decision tree It includes; detection rules automatically generated part. In a preferred embodiment of the invention, the attack actions detection rule generating apparatus When matching the detection rule newly and the detection rules previously generated generation of the respective network data type error rate wherein each of the network to the error rate, generated by multiplying the error rate to a target data types, and detection rules to verify and update section for updating the accuracy of the decision tree based on the respective data type of the error rate of the generated; further comprises a. In a further preferred embodiment, the attack actions detection rule

ERICSSON EXHIBIT 1005, Page 319

generating method of the present invention comprises the steps of classifying the network session data by attribute information; Converting the session attribute of the classified data information, and the normal type, the attack type to the input image and data format including the features of the data network is a network belonging to the data type; The step of configuring a decision tree classification algorithm by applying to the input data converted to the data type; Generating a decision tree based on the accuracy of the error rate at the final node of the decision tree; ; And a step for generating the network data belongs to the network the data type of the attribute, the optimal condition and the detection rule patterned to the network data type on the basis of the accuracy for selecting the node having an information gain of the decision tree It included.

In a further preferred embodiment of the present invention, attack detection rule generating method acts comprising: determining that the detection rule is matched with the newly generated detection rules previously generated; When matching the detection rule generating an error rate by multiplying the respective type of network data error rate target for each of the data types in the network error rate; Updating the accuracy of the decision tree based on the respective data type of the error rate of the generated; Further it comprises a. Hereinafter will be described with reference to the accompanying drawings, a preferred embodiment of the present invention. Of the figures should be noted that although denoted by the displays on the different figures the same reference number as possible and even if the numbers refer to the same elements. It the following description, if a detailed description of known functions and configurations determines that unnecessarily obscure the subject matter of the present invention, a detailed description thereof will be omitted. 1 is a diagram showing an overall flow chart for automatically generating and updating an attack behavior detection rule based on the network session attribute information according to the present invention, the network data generating unit 110, network data acquisition unit 120, a network and a session attribute information extraction unit 130, a detection rule generating automatic unit 140, a detection rule database storage unit 150, a detection rule to verify and update the unit 180. Network data generating unit 110 performs a function of generating data. The data generated is optionally using a variety of attack tools by one and the administrator to optionally generate a normal care data in the normal network environment do not contain to receive the data on the actual network from the network card, the attack actions by the administrator It includes as data for generating the attack actions. Network data acquisition section 120 performs a function for processing the data generated from the network to the data generation unit configured to collect software or by hardware. Network data acquisition unit 120 to the network data normal behavior data according to the type of data generated by the generating unit 110 is "Normal (normal)" data, attack care data are in "Attack (attack)" data, and if that is not part of the normal attack and care data are all collected in a "unknown (unknown)" data.

ERICSSON EXHIBIT 1005, Page 320

There the collection of attack behavior data manager is the title name in each of the attack attack behavior data is stored in each file. If this type of file name includes the attack and attack the name and other information. File Name for addition to a preferred embodiment a, attack a DoS (Denial of Service) attack cases 'dos' notation, and the attack is a mail server attack to mailbomb the case 'mailbomb' notation and . In addition, other information, the test indicated a date or day of the week, such as the distinction between those who are denoted by '_'. That is, it is configured to facilitate that by generating a file name in the form 'dos_mailbomb_w2frii', extracts the characteristic information from the list file that manages the data generated. Network session attribute information extraction section 130 classifies the data collected from the network data collection unit 120 each session and perform a function for extracting the characteristic information. Thus among properties will be described in more detail in the description related to Fig. 2 and 3. Automatic detection rule generation unit 140 of each type of attack by using an algorithm which extend one of the C4.5 of the decision tree algorithm based on information theory based on the characteristic information extracted from the network session attribute information extraction unit 130 functions to create a detection rule to classify the data into. About this documentation will be described in more detail in Fig. Detection rule database storage 150 stores the detection rule in the detection rule generating automatic generation unit 140. The detection rules to verify and update section 180 includes a detection rule verification unit 160 and the detection rules automatically update section 170. Detection rule verification unit 160 verifies the detection rule stored in the detection rule automatically generating unit generates the detection rule storage database 150 at 140, and detection rule automatic updating unit 170 is a detection rule verification unit 160 updates from the accuracy of the detection rule verification. Detection rule to verify and update unit 180 that the earlier the detection rule newly generated and the detection rule resulting in the match to each of the error rate as a target for the respective network data types in the error rate for a network data type error rate It multiplying generated, and updates the accuracy of the decision tree based on the respective data type of the error rate of the generated.

Thus among properties will be described in more detail in FIGS. Figure 2 illustrates an embodiment to extract the network data collection unit data sorted by the session attributes and collected from the 120 information in a network session attribute information extraction unit 130. Network session attribute information extraction unit 130 is a network data acquisition unit 120 based on the destination and full point of view to analyze the collected data for the network session characteristics significantly session information from the statistical information (Fig. 2 - (a)), the network protocol connection information (Fig. 2 - (b)), the network protocol header information (FIG. 2

ERICSSON EXHIBIT 1005, Page 321

- (c)), the two hosts among the connection information (Fig. 2 - (d), FIG. 2 - (e)) as classified by defining and . Data are classified into a predetermined value after a continuous form of the form leading to the continuously within a range type (continuous) with a range or discrete form of distinct specific values are limited (discrete), depending on the type. Entire session statistics (Figure 2 - (a)) is the statistical information to be analyzed and all of the packets in the session. If the extracted attribute information in packets to the data extraction by hand is limited to the extracted characteristic information unit's session as a classification type is more effective. Network protocol connection information (Fig. 2 - (b)) is an information analysis of the information associated with the connection establishment of the TCP / IP protocol. Network protocol header information (Fig. 2 - (c)) is an information field of major interest in the TCP / IP protocol header. Connection of information between two hosts (Figure 2 - (d), Figure 2 - (e)) are the various statistical information regarding the direction between the two hosts. 3 is a flow chart for extracting characteristic information of the data collected from the network session attribute information extraction unit 130 of Fig. Network data collection unit accumulating the characteristic information for each session, as shown the data collected from the 120 in Fig. 2 classified by a session in a network session attribute information extraction unit 130, and extracts the attribute information (S310) (S320). The type of the data to extract the characteristic information for each network session is determined whether the continuous type or a discrete (S330).

If the type of the extracted data undergoes continuous type has a characteristic classification test (S340) for continuously or discrete jeokinji search at any interval, based on the threshold value (threshold) the range set by the administrator. Continuous data are classified according to have a major effect on the threshold determination method in the classification algorithm based on information theory, as compared to discrete. As a result, in the case of continuous data in order to apply a classification algorithm with the characteristics suitable for the characteristics undergoes a discrete classification test. If you type this type of data extracted and then classified as normal discrete, the type of attack (S370) to apply to the classification algorithm "Information session 1 and session information, 2, ..., session information, N, denominator" data formats as input It is converted (S380). Attribute classification (e.g., average value) test (S340) continuous data value is a specific value or a predetermined range of the representative value through a compartmentalized into discrete data values consisting of (partition) the optimum classification according to whether (S350) the and determines whether the. If when the optimum category convert the continuous data in discrete data (S360), and if not, to apply the continuous data to a classification algorithm to classify (370) the normal and each type of attack without changing the data " 1 the session information, session information, 2, ..., N and the session information, converting the input data into the same format as the denominator "(S380). The denominator as the

title indicating the characteristics of the network data type belongs to a network data, if the network data collection unit of normal behavior data, such as that used in the file names of 120 has referred to the 'Normal (normal) " , in the case of attack behavior data, with reference to the network data collection portion is denoted by the file name designation attack. Figure 4 is an algorithm using Expand C4.5 of one of the decision tree algorithm based on the automatic generation rules detection unit 140, the input data in a format converted from the data input session attribute information 3 on the information theory a flowchart to classify each type of attack.

C4.5 proposed by J. Ross Quinlan is an algorithm that calculates a gain value according to a decrease in entropy automatically configure the tree. C4.5 network is a type of data classification algorithm is adapted to this, since there have effectively classified the packets of high volume, continuous form and forms a discrete measure of the packet are at the same time. In addition, such classification algorithm is also advantageous for so easy to change a SQL statement in a query language for relational database than the neural networks and Bayesian classifier create a detection rule. C4.5 is a basic classification algorithm developed by J. Ross Quinlan ID3 algorithm is based on the year 1986. The algorithm Dodge separation (multiple split) is easily interpreted from a possible and the generated tree to allow the child node is separated from the at least two parent nodes. That is, the classification can be as many as the number of discrete for discrete, it is possible for the classification is continuous. However, the continuous type is categorized as compared to discrete can not be good. Due to an error rate in the last survey to the end node pruning to obtain a minimal error rate. The detection rule expansion C4.5 algorithm of the classification algorithm using the automatic generation unit facilitates the interpretation of the model tree, the selection of the scale for easy classification and configured automatically by the configuration tree. It is also the case for the combination of configuration parameters to be applied to the detection of the attack because it can easily see how it affects the algorithm appropriate for the target variable to investigate the link between attack and detection rules. Expansion C4.5 algorithm should be a process of converting the input data via said network session attribute information extraction unit in which characteristic classification test as adapted for the generation of rules detect the basic algorithm preceding C4.5. Making processes that make up the tree without performing the basic algorithm and C4.5, pruning process, but performed in the same way to calculate the error rate at the final node. Finally, by constructing a decision tree comprises a process of converting the decision tree into rules.

4 is extended by using the C4.5 algorithm in the automatically generated detection rules 140 to produce an automatic detection rule as follows: And calculates the frequency of

ERICSSON EXHIBIT 1005, Page 323

each class (or category) of the session attribute information input data (S380) (S410). It constitutes the nodes in the decision tree based on the calculated frequency (S420). Calculates a gain for each attribute - specific information, and select the properties with optimal gain information (S430) (S440). End (leaf) is performed by repeating the process of S410 to S440 in the case other than the node (S450). If the end node by calculating the error rate of each of the decision tree to determine the accuracy (S460). The error rate is calculated as the ratio of the case that does not satisfy the rule resulting in a data set as in the basic C4.5 algorithm, the accuracy is defined to consist of approval rating (support) and the reliability (confidence). Approval rating is frequently higher the approval rating to mean the frequency of the generated rule, which means that the rule is useful, and the reliability is high means that the accuracy is higher the reliability indicates just how reliable this rule. Approval rating is defined as the ratio of the size of the entry for the size of the entire data set, and the reliability is defined as a value obtained by subtracting the error rate at 100% confidence. That can be expressed as follows. Reliability = 1.0 error rate approval rating = if the size of the final node of the size / the complete set of data for the item after determining the accuracy by calculating the error rate of each of the decision tree (S460) each node constructs a decision tree has an accuracy (S470). In one embodiment, the following shows a portion of a decision tree configured for the case of an attack action (Attack) and the steady behavior (Normal) corresponding to the mailbomb attack. Configuring the format of the decision tree is a "level number value scale measures people symbol conditions: normal or attacking people (accuracy)" is represented by. Here, if the final node only [] entry is expressed, the accuracy and reliability include approval rating as defined the above step. L2 HAttl_length> 112: L3 HBidletime_max <= 988.7: L4 HBminseg_size> 23: mailbomb (1.000, 0.980) L4 HBminseg_size <= 23: L5 HBidletime_max <= 46.6: Normal (0.921, 0.752) for each node in the accuracy of having a decision tree for configuring after (S470) normal and each type of attack as a "rule number; attack people; the condition of; accuracy (approval rating, reliability)" format to represent the detection rules by converting (S480) the detection rules stored in the database 150 to store it.

When the mailbomb attack behavior for the attack (Attack) and one embodiment of a portion of a decision tree configured for the case of normal behavior (Normal) format described above, converted to the detection rule is expressed as .1; mailbomb; HAttl_length> 112 , HBidletime_max <= 988.7, HBminseg_size> 23; 1.000, 0.980 Figure 5 is a detailed configuration of the detection rule verification unit 160 in the detected rule to verify and update unit 180 shown in FIG. When starting the verification in the detection rule verification controller (S510), via the network data generating unit 110 generates the normal and attack data by collecting data over the network, the data collection unit 120, and also the collected data 3 extracts the session attribute

ERICSSON EXHIBIT 1005, Page 324

information data over a network session attribute information extractor 130, as shown in the process of (S511 - S514) "rule number; attack patients; the condition of; accuracy (approval rating, reliability)" the detected rules expressed in the format type It is converted to (S520). Transform the detection rule and the stored detection rule stored detection rule database 150 to verify that match with a query (query) (S530). Query to retrieve a one - to - one matching for determining whether or not the entire detection rule and stored in the database, and compares both the condition as contained in the form and order of the detection rule as step S480 of FIG. If they match, all the condition to update the accuracy of the detection rule update through the automatic detection rule group (170) (S540). If one or more of the condition do not match, and go back to step S613 again to repeat the steps of the process after that. Figure 6 is a detailed configuration of the detection rule automatic updating unit 170 in the detected rule to verify and update unit 180 shown in FIG. It is determined whether the detection rule verification unit 160, the session specific information about the data type is the normal input data detection rules (Normal) and verified by the act, the attack (Attack) Act, unknown (Unknown) Act (S610).

Here, the data type is determined by the denominator of the last hangin input data format conversion in FIG. 3, if that is not part of the normal attack, and both actions are determined by the unknown behavior (S380). Respectively calculate the error rate for each data type (normal, attacks, unknown) (S611, S612, S613). Error rate, reflecting the normal behavior of the error rate detection rules accuracy - error rate is calculated by multiplying by a target data set to conduct only normal (100% confidence in its reliability rules) (S611). Error rate, reflecting the attacks Act shall be calculated by multiplying the error rate target only one data set to conduct an attack error rate detection accuracy rules (S612). The error rate that reflects the behavior is unknown calculate the error rate that reflects the image acts by targeting only non - normal data set and attack behavior (S613). So depending on the data type (normal, attacks, unknown) for respectively reflecting the error rate is also the meaning improve the reliability of the detection rule accuracy. S611 - S613 granted in step weight based on the error rate calculated, respectively, perceptron rule, and calculates the precision of the detection rules by the fuzzy logic, etc. (S620). The accuracy and reliability include approval ratings, as in the automatic detection rule generating unit 140. For example, when applying the method to calculate the weighting in addition to the product of the weight and the calculated error rate for each data type defined by the administrator on the accuracy of the existing rules. After detection rule verification unit in converting the detection rules and detect the rule storage database 150, the stored detection rule queries (query) via correspondence if verified that step in the retrieved rule of accuracy and automatically updated after detection rules stored in the database is stored in the (150) (S630, S640). 7 is an overall flow chart for automatically generating a detection

ERICSSON EXHIBIT 1005, Page 325

rule. Collecting data generated by the network data generating unit 110 of Figure 1 according to the type of data generated from a network data collection unit 120. After that classifies the collected network data by the session attribute information (S700).

After that converts the segmented data as the input data type attribute comprising the session information and the normal type, the attack and the image type data network belonging to the attributes of the data type of the network (S710). For this in conjunction with the network session attribute information extracting section which describe in Figure 3 refer to the descriptions above. The input data applied to a classification algorithm to the data format conversion into the configuration tree to determine and generate the accuracy of the decision tree on the basis of (S720), the error rate in the final node of the decision tree (S730). Then, the name, to generate a conditional expression, and the patterned detection rules to the data network type on the basis of the accuracy for selecting the node with the best information gain of the decision tree (S740). For this also in relation to the detection rules automatically create wealth conifers described in Note 4 to the descriptions. It is prior to the detection of the detection rule and the newly created rule to the generation is determined to match (S750). For this in relation to the configuration of the detection rules also detected in the verification and validation rule updating unit described in Note 5 to the descriptions. When matching the detection rule and generates by multiplying the error rate for the respective network data type error rate target for the respective network data types to the error rate, the accuracy of the decision tree based on the respective data type of the error rate, the generated it updates the (S760). In respect with regard to detection rules automatically updated in the section which also detects verify and update the rules described in section 6, please refer to the descriptions. 8 is a diagram showing the effect of the present invention as compared with the conventional one attack detection method. It shows the detection rule and the method for forming the difference of the attack detection rate compared to the approach of the LERAD of Florida Institute of Technology of the present invention. In Figure 8 the horizontal axis will set forth the name of each attack, and the vertical axis represents the detection rate for each attack. The invention is illustrated by the solid line arrow portion shows the detection rate of the cited LERAD.

Improved detection results can be seen approximately 10% in the present invention than the results of LERAD As shown in the figure. Figure 9 (a) and (b) are views showing the accuracy improvement of the detection rule by converting the continuous data into discrete data. Figure 9 (a) shows the detection rate is high at the time when conversion to discrete data than the detection rate of the experimental data when the result of applying the DARPA peripheral data of the data, one continuous data. That is, as shown

ERICSSON EXHIBIT 1005, Page 326

in the figure, the result of applying the Tue, Wed data although not made a little improvement, the remaining data can be seen that the detection rate is improved. Figure 9 (b), if a data conversion into discrete than the case of continuous data which shows the O tamyul is more lowered. That is, when applied to a Mon, Fri data, but a significant change can be seen that the other data tamyul O (False Positive) is lowered. Figure 10 and Figure 11 shows the results of applying the detection rule formed in accordance with an embodiment of the present invention to the experimental data. Accumulated (S320) an attribute information for each session in Figure 3 and prior to the data type determination (S330) is the result of applying to the experimental data DARPA to ensure a good measure first selection from a variety of scales (measure). GRR is defined as follows. GRR (Good Rule Rate) =, (this time, α = 0.01) It is good GRR value every step of the selection (G), and ignore unnecessary thing, and (I), the bad test that does not select (X) equation . Results of the tests in the same way as above, when only select a good measure for each phase when applied to the Wed Thu data as in Figure 10, a high detection rate is lowered oh tamyul. RST in FIG. 11 indicates a test result and, SLT means selected. The present invention can also be embodied as computer readable code on a computer - readable recording medium. The computer - readable recording medium includes all kinds of recording devices storing data that can be read by a computer system.

Examples of the computer - readable recording medium are a ROM, RAM, CD - ROM, magnetic tapes, floppy disks, optical data storage devices, etc., and a carrier wave (such as data transmission through the Internet) also it included. The computer readable recording medium can also be distributed over network coupled computer systems may be that the computer readable code is stored and executed in a distributed fashion. Optimum embodiments have been disclosed herein and in the above drawing. Although specific terms are used here, this is not the only used to limit the scope of the invention as set forth in the claims or geotyiji means limited to use for the purpose of illustrating the invention. Thus, those of ordinary skill in the art will appreciate that various modifications and equivalent may be made from other embodiments. Therefore, the true technical protection scope of the present invention will be defined by the technical spirit of the appended claims.

In the present invention, by automatically processing the process of generating and, excluding and sorting the more accurate detection rules than to re - calculate the detected error rate, the accuracy is low detection rules each type of attack detection rules for the attribute information of the network session based makes it possible to automatically generate effective detection rules to detect known attacks or similar types of attacks without the help of a professional to perform a faster response. Thus, the

ERICSSON EXHIBIT 1005, Page 327

variants for the new activity or in the detection of unknown attack has a high accuracy and generates a detection rule with the ability to respond to new forms of attack. In addition, the effect occurs that the features extracted by the characteristic information of the network session for the unit of the attack can not be clearly distinguished from the normal or not the network packet network data stream.

ERICSSON EXHIBIT 1005, Page 328

Europäisches Patentamt
European Patent Office
Office européen des brevets

Patent Translate

Powered by EPO and Google

Notice

This translation is machine - generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine - translation output.

CLAIMS KR100628329

1.

The session attribute information and the normal type, the attack and unknown type of network session attribute information extraction unit for converting the input data type including the features of the data network is a network that belongs to type of data classified by the data network session attribute information; And Constitutes the decision tree by applying a classification algorithm, on the input data format in the converted network data and, based on the error rate at the final node of the decision tree generation accuracy of the decision tree, the network data type of the property, the crystal attack behavior detection rule comprising a; the condition and on the basis of the accuracy of detection rules automatically generating section for generating a patterned detection rules to the network data type for selecting the node with the best information gain of the tree generation device.

2.

According to claim 1, When matching the new detection rules and the rules generated detects a previously created The respective network data type error rate detection rule verification to update the accuracy of the decision tree based on the respective data

ERICSSON EXHIBIT 1005, Page 329

type error rate generated by multiplying the error rate target for the respective network data types, and wherein generating the error rate and attack behavior detection rule generating apparatus characterized in that it comprises a more; update unit.

3.

According to claim 1, Classified network characteristic data by the session information is divided into continuous and discrete, depending on whether the continuously within a predetermined range, If the continuous type, based on the predetermined threshold value range is partitioned into discrete data values within a predetermined range after conversion to discrete data Attack behavior detection rule generating apparatus characterized in that the conversion to the input data format of the algorithm classifying the data network to a normal behavior, and the behavior type of the unknown attack actions.

4.

According to claim 1, wherein the algorithm Calculating the frequency of the classified - network session data classified by the attribute information, It constitutes the nodes in the decision tree based on the calculated frequency, Calculating the gain information for each node to select a node with the best information and gain Attack behavior detection rule generating apparatus at the final node characterized in that for calculating the accuracy of the decision tree on the basis of the error rate.

5.

According to claim 1, wherein the session property information Entire session statistics, the network protocol connection information, network protocol header information, the attack actions detection rule generating apparatus characterized in that it comprises one or more of the connection information between two hosts.

6.

ERICSSON EXHIBIT 1005, Page 330

Classifying the network session data by attribute information; Converting the session attribute of the classified data information, and the normal type, the attack type to the input image and data format including the features of the data network is a network belonging to the data type; The step of configuring a decision tree classification algorithm by applying to the input data converted to the data type; Generating a decision tree based on the accuracy of the error rate at the final node of the decision tree; and The name, the condition for selecting the node with the best information gain of the decision tree, and generating the patterned detection rules to the network data type based on the accuracy; attack behavior comprising the how to create a detection rule.

7.

According to claim 6, Before said step of determining that the detected rules of the detection rule and the newly generated generation to match; When matching the detection rule generating an error rate by multiplying the respective type of network data error rate target for each of the data types in the network error rate; and Attack behavior detection rule generating method comprising the more; updating the accuracy of the decision tree based on the respective data type of the error rate of the generated.

8.

According to claim 6, Step classified network characteristic data by the session information is divided into continuous and discrete, depending on whether the continuously within a predetermined range; If continuous type if a predetermined threshold value based on a range partitioned into discrete data values within a predetermined range in discrete steps for converting data; and Attack behavior detection rule generating method comprising the more; the normal network data activity, and classified by type of attack actions unknown to the act of converting the input data type of the algorithm.

9.

According to claim 6, wherein the classification algorithm Calculating a frequency of the classified - network session data classified by the attribute information; The step of

ERICSSON EXHIBIT 1005, Page 331

configuring the nodes in the decision tree based on the calculated frequency; Selecting a node having the best gain information by calculating the gain information for each node, and Attack behavior detection rule generating method comprising the; calculating the accuracy of the decision tree on the basis of the error rate at the final node.

10.

According to claim 6 or claim 9, wherein the classification algorithm It characterized in that the extended algorithm C4.5 attack detection methods produce practices rules.

11.

The method of claim 6, wherein the characteristic information of the session Entire session statistics, the network protocol connection information, network protocol header information, the attack actions detection rule generating method characterized in that it comprises one or more of the connection information between two hosts.

ERICSSON EXHIBIT 1005, Page 332

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/00 (2006.01)

(45) 공고일자 2006년09월27일
(11) 등록번호 10-0628329
(24) 등록일자 2006년09월19일

(21) 출원번호 10-2005-0069968
(22) 출원일자 2005년07월30일

(65) 공개번호
(43) 공개일자

(73) 특허권자 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 정일안
대전 유성구 신성동 208-2

오진태
대전 유성구 전민동 엑스포아파트 209동 203호

장종수
대전 유성구 전민동 엑스포아파트 303동 903호

(74) 대리인 리엔목특허법인

(56) 선행기술조사문헌
KR1020020062071 A
KR1020050120875 A
KR1020060063606 A
KR1020050045500 A
KR1020060058179 A
* 심사관에 의하여 인용된 문헌

심사관 : 나용수

(54) 네트워크 세션 특성 정보에 대한 공격 행위 탐지규칙 생성장치 및 그 방법

요약

본 발명은 네트워크 세션 특성 정보에 대한 공격행위 탐지규칙 자동생성 및 자동갱신 방법 및 장치에 관한 것으로, 세션 특성 정보별로 분류된 네트워크 데이터를 세션 특성 정보 및 정상 유형, 공격 유형 및 미지 유형 중 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 포함하는 입력 데이터 형식으로 변환하는 네트워크 세션 특성정보 추출부 및 입력 데이터 형식으로 변환된 네트워크 데이터에 확장 C4.5 알고리즘을 적용하여 결정트리를 구성하고, 결정트리의 최종노드에서 오류율을 기초로 결정트리의 정확도를 생성하며, 네트워크 데이터 유형의 특성, 결정트리의 최적의 정보이득을 갖는 노드를 선택하기 위한 조건식 및 정확도를 기초로 네트워크 데이터 유형별로 패턴화된 탐지규칙을 생성하는 탐지규칙 자동 생성부를 포함하여 탐지규칙을 자동으로 생성하고 갱신한다.

대표도

도 1

ERICSSON EXHIBIT 1005, Page 333

색인어

네트워크 세션 특성 정보, 탐지규칙, 결정트리, 자동생성, 자동갱신

명세서

도면의 간단한 설명

도 1 은 네트워크 세션 특성정보를 기반으로 공격행위의 탐지을 규칙 자동생성하고 갱신하는 방법의 전체 구성도이다.

도 2(a)는 도 1 에 도시된 네트워크 세션 특성정보 추출부의 세션 전체 통계정보이다.

도 2(b)는 도 1 에 도시된 네트워크 세션 특성정보 추출부의 네트워크 프로토콜 연결정보이다.

도 2(c)는 도 1 에 도시된 네트워크 세션 특성정보 추출부의 네트워크 프로토콜 헤더정보이다.

도 2(d) 및 2(e)는 도 1 에 도시된 네트워크 세션 특성정보 추출부의 두 호스트 사이의 연결정보이다.

도 3 은 도 1 의 네트워크 세션 특성정보 추출부(130)에서 수집된 데이터의 특성정보를 추출하는 흐름도이다.

도 4 은 도 1 에 도시된 탐지규칙 자동생성부에서 탐지규칙을 자동으로 생성하는 흐름도이다.

도 5 는 도 1 에 도시된 탐지규칙 검증 및 갱신부 내의 탐지규칙 검증부에서 생성된 탐지규칙을 검증하기 위한 흐름도이다.

도 6 은 도 1 에 도시된 탐지규칙 검증 및 갱신부 내의 탐지규칙 자동갱신부에서 생성된 탐지규칙의 정확도를 갱신하기 위한 흐름도이다.

도 7 은 탐지규칙을 자동으로 생성하기 위한 전체 흐름도이다.

도 8 은 본 발명의 효과를 종래의 공격 탐지 방법 중의 하나와 비교하여 도시한 도면이다.

도 9 는 연속형 데이터를 이산형 데이터로 변환함으로써 탐지규칙의 정확도 향상을 나타내는 도면이다.

도 10 및 도 11 은 본 발명의 일 실시예에 따른 탐지규칙 형성을 실험 데이터에 적용한 결과를 도시한다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 세션 특성 정보에 대한 공격행위 탐지규칙 자동생성 및 자동갱신 방법 및 장치에 관한 것으로, 네트워크 세션별 특성정보에 대해 각 공격행위에 대한 탐지규칙들을 자동으로 생성하고, 생성된 규칙들의 정확성을 탐지 정확도 계산을 통해 자동으로 갱신하여 보다 정확한 탐지규칙들을 통해, 알려진 공격 및 유사한 공격유형, 정상 행위와 다른 유형을 탐지하기 위한 것이다.

일반적으로, 침입탐지 방법은 특징기반의 규칙 탐지와 비정상행위 탐지로 나뉜다. 특징기반 방법은 이미 알려진 공격패킷을 분석하여 패턴화하고 그 패턴과 일치하는지를 검사함으로써 공격을 판정하는 것으로, 알려진 공격에 대한 탐지 정확도는 상당히 높지만, 변형된 공격행위나 알려지지 않은 새로운 공격에 대한 탐지에는 한계가 있다.

이러한 단점을 극복하기 위한 비정상행위 탐지 방법은 정상적인 행위에 의해 생성된 데이터를 모델링하여 이 정상모델과 벗어난 정도에 따라 공격을 탐지하는 것으로 주로 알려지지 않은 공격을 탐지하는데 사용된다.

ERICSSON EXHIBIT 1005, Page 334

대량의 네트워크 데이터로부터 침입과 관련된 특징을 찾는 작업은 대부분 전문가의 지식에 의해 분석되는데, 이러한 방법은 정확성은 높으나 분석 비용이 높고 새로운 형태의 공격에 대한 대처 능력이 떨어지게 된다.

반면, 비정상행위 탐지 방법은 알려지지 않은 공격을 탐지하는데 효과적이지만, 특징화가 어렵고 특징 기반에 비해 정확성이 떨어진다. 또한, 네트워크 패킷에서는 나타나지 않거나 정상적인 네트워크 데이터 흐름과 명확하게 구별할 수 없는 공격유형에 대한 특징들을 추출하기 위해 네트워크 세션 단위의 특성정보를 이용하는 방법에 관한 연구가 거의 없는 실정이다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제점을 해결하기 위해 네트워크 세션 특성 정보에 대한 공격행위 탐지규칙을 자동으로 생성하고 갱신하여 보다 정확도가 높은 탐지규칙을 생성하는 것을 목적으로 한다.

발명의 구성 및 작용

본 발명의 바람직한 일 실시예에 있어서, 공격 행위 탐지 규칙 생성 장치는 세션 특성 정보별로 분류된 네트워크 데이터를 상기 세션 특성 정보 및 정상 유형, 공격 유형 및 미지 유형 중 상기 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 포함하는 입력 데이터 형식으로 변환하는 네트워크 세션 특성정보 추출부;및 상기 입력 데이터 형식으로 변환된 네트워크 데이터에 분류 알고리즘을 적용하여 결정트리를 구성하고, 상기 결정트리의 최종노드에서 오류율을 기초로 상기 결정트리의 정확도를 생성하며, 상기 네트워크 데이터 유형의 특성, 상기 결정트리의 최적의 정보이득을 갖는 노드를 선택하기 위한 조건식 및 상기 정확도를 기초로 상기 네트워크 데이터 유형별로 패턴화된 탐지규칙을 생성하는 탐지규칙 자동 생성부;를 포함한다.

본 발명의 바람직한 일 실시예에 있어서, 공격 행위 탐지 규칙 생성 장치는 이전에 생성된 상기 탐지규칙과 새롭게 생성된 상기 탐지 규칙이 일치하는 경우 상기 각각의 네트워크 데이터 유형별 오류율은 상기 오류율에 상기 각각의 네트워크 데이터 유형만을 대상으로 한 오류율을 곱하여 생성하고, 상기 생성된 각각의 데이터 유형별 오류율을 기초로 상기 결정 트리의 정확도를 갱신하는 탐지규칙 검증 및 갱신부;를 더 포함한다.

본 발명의 또 다른 바람직한 일 실시예에 있어서, 공격 행위 탐지 규칙 생성 방법은 네트워크 데이터를 세션 특성 정보별로 분류하는 단계; 상기 분류된 상기 데이터를 상기 세션 특성 정보 및 정상 유형, 공격 유형 및 미지 유형 중 상기 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 포함하는 입력 데이터 형식으로 변환하는 단계; 상기 입력 데이터 형식으로 변환된 상기 데이터에 분류 알고리즘을 적용하여 결정트리를 구성하는 단계; 상기 결정트리의 최종노드에서 오류율을 기초로 상기 결정트리의 정확도를 생성하는 단계; 및 상기 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성, 상기 결정트리의 최적의 정보이득을 갖는 노드를 선택하기 위한 조건식 및 상기 정확도를 기초로 상기 네트워크 데이터 유형별로 패턴화된 탐지규칙을 생성하는 단계;를 포함한다.

본 발명의 또 다른 바람직한 일 실시예에 있어서, 공격 행위 탐지 규칙 생성 방법은 이전에 생성된 상기 탐지규칙과 새롭게 생성된 상기 탐지 규칙이 일치하는지 판단하는 단계; 상기 탐지 규칙이 일치하는 경우 상기 각각의 네트워크 데이터 유형별 오류율을 상기 오류율에 상기 각각의 네트워크 데이터 유형만을 대상으로 한 오류율을 곱하여 생성하는 단계; 상기 생성된 각각의 데이터 유형별 오류율을 기초로 상기 결정 트리의 정확도를 갱신하는 단계; 를 더 포함한다.

이하 본 발명의 바람직한 실시예가 첨부된 도면들을 참조하여 설명될 것이다. 도면들 중 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 참조번호들 및 부호들로 나타내고 있음에 유의해야 한다. 하기에서 본 발명을 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

도 1 은 본 발명에 따른 네트워크 세션 특성정보를 기반으로 공격행위 탐지규칙을 자동으로 생성하고 갱신하는 전체 흐름을 도시하는 도면으로서, 네트워크 데이터 생성부(110), 네트워크 데이터 수집부(120), 네트워크 세션 특성정보 추출부(130), 탐지규칙 자동생성부(140), 탐지규칙 저장 데이터베이스부(150), 탐지규칙 검증 및 갱신부(180)를 포함한다.

ERICSSON EXHIBIT 1005, Page 335

네트워크 데이터 생성부(110)는 데이터를 생성하는 기능을 수행한다. 여기서 데이터 생성은 네트워크 카드로부터 실제 네트워크 상의 데이터를 수신하는 것, 관리자에 의하여 공격 행위가 포함되지 않는 정상적인 네트워크 사용환경에서 임의적으로 정상 행위 데이터를 생성하는 것 및 관리자에 의해 다양한 공격 도구를 사용하여 임의적으로 공격 행위 데이터를 생성하는 것을 포함한다.

네트워크 데이터 수집부(120)는 네트워크 데이터 생성부로부터 생성된 데이터들을 소프트웨어로 처리하거나 하드웨어적으로 구성하여 수집하는 기능을 수행한다.

네트워크 데이터 수집부(120)는 상기 네트워크 데이터 생성부(110)에서 생성된 데이터의 유형에 따라 정상 행위 데이터는 "Normal(정상)" 데이터로 , 공격 행위 데이터들은 "Attack(공격)" 데이터로, 그리고 정상 및 공격 행위 데이터에 속하지 않는 경우는 모두 "Unknown(미지)" 데이터로 수집한다.

공격 행위 데이터를 수집함에 있어 관리자는 공격 행위 데이터에 해당 공격 명칭을 각각 표기하여 각각의 파일 형태로 저장한다. 이 경우 파일 명칭의 형식은 공격 유형과 해당 공격명 및 기타 정보를 포함한다.

파일 명칭을 부가하는 바람직한 일 실시예로서, 공격유형이 서비스거부(Denial of Service) 공격의 경우에는 'dos'로 표기하고, 해당 공격이 메일 서버를 공격하는 mailbomb인 경우에는 'mailbomb'로 표기한다. 또한 기타 정보에는 시험한 날짜나 요일 등을 표기하고 이들간의 구별자는 '_'로 표기한다. 즉, 파일명을 'dos_mailbomb_w2frii' 형태로 생성함으로써, 생성된 데이터를 관리하는 목록 파일로부터 특성 정보를 추출하는 것이 용이하도록 구성한다.

네트워크 세션 특성정보 추출부(130)는 네트워크 데이터 수집부(120)에서 수집된 데이터를 세션별로 분류하고 특성정보를 추출하는 기능을 수행한다. 이에 대하여서는 도 2와 도 3 에 대한 관련 설명에서 보다 상세히 설명하기로 한다.

탐지규칙 자동생성부(140)는 네트워크 세션 특성정보 추출부(130)에서 추출한 특성 정보를 기초로 정보이론에 기반한 결정트리 알고리즘들중의 하나인 C4.5를 확장한 알고리즘을 사용하여 각 공격유형별로 데이터를 분류하도록 탐지규칙을 생성하는 기능을 한다. 이에 관하여서는 도 4에서 보다 상세히 설명하기로 한다.

탐지규칙 저장 데이터베이스(150)는 탐지규칙 자동생성부(140)에서 생성된 탐지규칙을 저장한다.

탐지규칙 검증 및 갱신부(180)는 탐지규칙 검증부(160)와 탐지규칙 자동갱신부(170)를 포함한다. 탐지규칙 검증부(160)는 탐지규칙 자동생성부(140)에서 생성되어 탐지규칙 저장 데이터베이스(150)에 저장된 탐지규칙들을 검증하고, 탐지규칙 자동갱신부(170)는 탐지규칙 검증부(160)에서 검증된 탐지규칙의 정확도를 갱신한다.

탐지규칙 검증 및 갱신부(180)는 이전에 생성된 상기 탐지규칙과 새롭게 생성된 상기 탐지 규칙이 일치하는지와 각각의 네트워크 데이터 유형별 오류율을 상기 오류율에 상기 각각의 네트워크 데이터 유형만을 대상으로 한 오류율을 곱하여 생성하고, 상기 생성된 각각의 데이터 유형별 오류율을 기초로 상기 결정 트리의 정확도를 갱신한다. 이에 대하여서는 도 5 및 도 6에서 보다 상세히 설명하기로 한다.

도 2 는 네트워크 세션 특성정보 추출부(130)에서 네트워크 데이터 수집부(120)로부터 수집한 데이터를 세션별로 분류하고 특성정보를 추출한 일 실시예를 도시한 것이다.

네트워크 세션 특성정보 추출부(130)는 네트워크 데이터 수집부(120)로부터 수집한 데이터를 분석할 대상 및 관점에 따라 네트워크 세션 특성 정보를 크게 세션 전체 통계정보(도 2-(a)), 네트워크 프로토콜 연결정보(도 2-(b)), 네트워크 프로토콜 헤더정보(도 2-(c)), 두 호스트 사이의 연결정보(도 2-(d), 도 2-(e))로 분류하여 정의한다.

데이터는 유형에 따라 소정의 범위 내에서 연속적으로 이어지는 형태로 나오는 값의 형태의 연속형(continuous)과 일정 범위나 특정 값이 한정되어 구별되는 형태의 이산형(discrete)으로 분류한다.

세션 전체 통계정보(도 2-(a))는 세션내에 있는 전체 패킷들에 대해서 분석되는 통계 정보이다. 패킷 단위로 특성 정보를 추출할 경우 데이터 추출이 제한됨에 반해 세션 단위로 특성 정보를 추출함으로서 유형을 분류함에 있어 보다 효과적이다.

ERICSSON EXHIBIT 1005, Page 336

네트워크 프로토콜 연결정보(도 2-(b))는 TCP/IP 프로토콜의 연결성립과 관련된 내용을 분석한 정보이다. 네트워크 프로토콜 헤더정보(도 2-(c))는 TCP/IP 프로토콜 헤더내의 주요 관심 필드들의 정보이다. 두 호스트 사이의 연결정보(도 2-(d), 도 2-(e))는 두 호스트 사이의 방향을 고려한 각종 통계 정보들이다.

도 3 은 도 1 의 네트워크 세션 특성정보 추출부(130)에서 수집된 데이터의 특성정보를 추출하는 흐름도이다.

네트워크 데이터 수집부(120)로부터 수집한 데이터를 네트워크 세션 특성정보 추출부(130)에서 세션별로 분류하고 특성정보를 추출하여(S310) 도 2에 도시된 바와 같이 각 세션별로 특성 정보를 누적한다(S320).

각 세션별로 네트워크 특성 정보를 추출한 데이터의 유형이 연속형인지 이산형인지를 판단한다(S330).

추출한 데이터의 유형이 연속형인 경우에는 관리자가 설정한 임계값(threshold) 범위를 기준으로 어느 구간에서 연속적 또는 이산적인지 검색하는 특성 분류 시험(S340)을 거친다.

연속형 데이터는 이산형에 비하여 정보이론에 기반한 분류 알고리즘에서 임계값 결정 방식에 따라 분류에 큰 영향을 미치게 된다. 그 결과, 이산형에 적합한 특성을 가진 분류 알고리즘에 적용하기 위하여 연속형 데이터의 경우 특성 분류 시험을 거친다.

추출한 데이터의 유형이 이산형인 경우에는 정상 및 공격 유형별로 분류(S370)한 후 분류 알고리즘에 적용하기 위해 "세션정보1, 세션정보2, ..., 세션정보N, 명명자" 와 같은 입력데이터 형식으로 변환(S380)한다.

특성 분류 시험(S340)을 거쳐 연속형 데이터 값이 특정 값이나 일정 범위의 대표값(예를 들어, 평균값)으로 이루어진 이산형 데이터 값들로 구획화(partition)가 되는지에 따라 최적의 분류(S350)가 되는지를 판단한다.

최적의 분류인 경우에는 연속형 데이터를 이산형 데이터로 변환(S360)하고, 그렇지 않은 경우에는 데이터의 변환없이 연속형 데이터를 정상 및 각 공격 유형별로 분류(370)하여 분류 알고리즘에 적용하기 위해 "세션정보1, 세션정보2, ..., 세션정보N, 명명자" 와 같은 입력 데이터 형식으로 변환(S380)한다.

여기서 명명자는 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 표시하는 명칭으로서, 상기 네트워크 데이터 수집부(120)의 파일명칭에 사용하는 방식과 같이 정상행위 데이터인 경우에는 'Normal(정상)'로 표기하고, 공격행위 데이터인 경우에는 상기 네트워크 데이터 수집부의 파일명칭을 참조하여 해당 공격명칭으로 표기한다.

도 4 는 탐지규칙 자동생성부(140)에서, 도 3에서 입력 데이터 형식으로 변환된 세션 특성 정보 입력 데이터를 정보이론에 기반한 결정트리 알고리즘들중의 하나인 C4.5를 확장한 알고리즘을 사용하여 각 공격유형별로 분류시키는 흐름도이다.

J. Ross Quinlan에 의해 제안된 C4.5는 엔트로피의 감소값에 따른 이득을 계산하여 트리를 자동으로 구성하는 알고리즘이다. C4.5 는 분류 알고리즘의 일종으로 네트워크 데이터는 대용량의 패킷들을 가지고 있고, 패킷내에 연속적인 형태와 이산적인 형태의 척도들이 동시에 존재하기 때문에 이를 효과적으로 분류하기에 적합하다.

또한, 이러한 분류 알고리즘은 신경망이나 베이지안 분류기에 비해 관계형 데이터베이스의 질의언어인 SQL문으로 바꾸기 쉬우므로 탐지규칙을 생성시키는데도 유리하다.

기본적인 C4.5는 J. Ross Quinlan이 1986년 ID3 알고리즘을 기초로 하여 개발한 분류 알고리즘이다. 이 알고리즘은 부모노드에서 자식노드가 2개 이상 분리되는 것을 허용하는 다지분리(multiple split)가 가능하고 생성된 트리로부터 해석이 용이하다.

즉, 이산형에 대해서는 이산의 수만큼 분류를 할 수 있고, 연속형에 대해서도 분류가 가능하다. 그러나 연속형인 경우에는 이산형에 비해 분류가 잘 되지 않을 수 있다. 마지막으로 끝 노드에서 오류율을 조사하여 최소한의 오류율을 얻기 위해 가지치기를 한다.

상기 탐지규칙 자동생성부에 사용하는 분류 알고리즘들 중 확장 C4.5 알고리즘은 트리를 자동으로 구성시킴으로써 분류를 위한 척도의 선택을 쉽게 하고, 구성된 트리 모형의 해석을 용이하게 해준다.

ERICSSON EXHIBIT 1005, Page 337

또한 구성되는 변수들의 결합이 목표변수에 어떤 영향을 주는지 쉽게 파악할 수 있기 때문에 공격탐지에 적용할 경우에는 탐지 규칙과 공격과의 연관성을 규명하기에도 적합한 알고리즘이다.

확장 C4.5 알고리즘은 상기 기본적인 C4.5 알고리즘을 탐지규칙의 생성을 위해 적합화시킨 것으로 상기 네트워크 세션 특성정보 추출부의 특성 분류 시험을 거쳐 입력데이터로 변환하는 과정이 선행되어야 한다.

결정트리를 구성하는 과정은 기본적인 C4.5 알고리즘과 같은 방식으로 수행되지만, 가지치기 과정을 수행하지 않고 최종 노드에서 오류율을 계산한다. 마지막으로 결정트리를 구성하여 결정트리 규칙으로 변환하는 과정을 포함한다.

도 4 는 탐지규칙 자동생성부(140)에서 확장 C4.5 알고리즘을 사용하여 다음과 같이 탐지규칙을 자동을 생성한다.

세션 특성 정보 입력 데이터(S380)의 각 클래스(또는 분류)별 빈도를 계산한다(S410). 계산된 빈도를 바탕으로 결정트리의 노드를 구성한다(S420). 각 속성별 정보이득을 계산하고(S430) 최적의 정보 이득을 갖는 속성을 선택한다(S440).

최종(leaf) 노드가 아닌 경우 S410 에서 S440까지의 과정을 반복하여 수행한다(S450).

최종 노드인 경우에는 각 결정트리의 오류율을 계산하여 정확도를 결정한다(S460). 여기서 오류율은 기본적인 C4.5 알고리즘에서와 같이 데이터 집합에서 생성된 규칙을 만족하지 않는 경우의 비율로 계산되고, 정확도는 지지도(support)와 신뢰도(confidence)로 구성하여 정의한다.

지지도는 빈번하게 발생하는 규칙의 빈도를 의미하는 것으로 지지도가 클수록 그 규칙이 유용함을 의미하고, 신뢰도는 규칙이 얼마나 믿을만한지를 나타내는 것으로 신뢰도가 클수록 정확성이 높다는 것을 의미한다.

지지도는 전체 데이터 집합의 크기에 대한 해당 항목의 크기의 비율로 정의하고, 신뢰도는 100% 신뢰도에서 오류율을 뺀 값으로 정의한다.

즉 다음과 같이 표현될 수 있다.

신뢰도 = 1.0 - 오류율

지지도 = 해당 항목의 크기 / 전체 데이터 집합의 크기

최종 노드인 경우에는 각 결정트리의 오류율을 계산하여 정확도를 결정한 후(S460) 각 노드들은 정확도를 갖는 결정트리를 구성한다(S470).

일 실시예로서, 다음은 mailbomb 공격에 해당하는 공격행위(Attack)와 정상행위(Normal)인 경우에 구성된 결정트리의 일부분을 나타낸 것이다.

결정트리의 구성형식은 "레벨번호 척도명 조건기호 척도값 : [정상 또는 공격명 (정확도)]"으로 표현된다. 여기서, 최종 노드인 경우에서만 []항목이 표현되고, 정확도는 상기 단계의 정의와 같이 지지도와 신뢰도를 포함한다.

L2 HAttl_length > 112 :

L3 HBidletime_max <= 988.7 :

L4 HBminseg_size > 23 : mailbomb (1.000, 0.980)

L4 HBminseg_size <= 23 :

L5 HBidletime_max <= 46.6 : Normal (0.921, 0.752)

각 노드에서 정확도를 갖는 결정트리를 구성한 후(S470) 정상 및 각 공격 유형별로 "규칙번호;공격명;조건식들;정확도(지지도, 신뢰도)" 형식으로 표현된 탐지규칙으로 변환(S480)하여 탐지규칙 저장 데이터베이스(150)에 저장한다.

ERICSSON EXHIBIT 1005, Page 338

위에서 설명한 mailbomb 공격에 해당하는 공격행위(Attack)와 정상행위(Normal)인 경우에 구성된 결정트리의 일부분의 일 실시예를 탐지규칙 형식으로 변환하면 다음과 같이 표현된다.

1;mailbomb;HAttl_length > 112, HBidletime_max <= 988.7, HBminseg_size > 23;1.000, 0.980

도 5는 도 1에 도시된 탐지규칙 검증 및 갱신부(180) 내의 탐지규칙 검증부(160)의 세부 구성도이다.

탐지규칙 검증제어기에서 검증을 시작하는 경우(S510), 네트워크 데이터 생성부(110)를 통해 정상 및 공격 데이터를 생성하여 네트워크 데이터 수집부(120)를 통해 데이터를 수집하고, 수집된 데이터를 도3의 과정과 같이 네트워크 세션 특성 정보 추출기(130)를 통해 세션 특성 정보 데이터를 추출하여(S511-S514) "규칙번호;공격명;조건식들;정확도(지지도, 신뢰도)" 형식으로 표현된 탐지규칙 형식으로 변환한다(S520).

변환된 탐지규칙과 탐지규칙 저장 데이터베이스(150)에 저장된 탐지규칙들을 질의(query)를 통해 일치하는지를 검증한다(S530). 질의는 데이터베이스에 저장되어 있는 전체 탐지규칙들과 일대일 일치여부를 검색하여 판단하기 위한 것으로, 도 4 의 S480 단계와 같은 탐지규칙의 형식에 포함된 조건식들과 순서대로 모두 비교한다.

모든 조건식들이 일치하는 경우에는 탐지규칙 자동 갱신기(170)를 통해 탐지규칙의 정확도를 갱신한다(S540). 하나 이상의 조건식이 일치하지 않는 경우에는 S613 단계로 돌아가서 다시 그 이후의 단계들을 반복하여 처리한다.

도 6은 도 1에 도시된 탐지규칙 검증 및 갱신부(180) 내의 탐지규칙 자동갱신부(170)의 세부 구성도이다.

탐지규칙 검증부(160)를 통해 검증된 세션 특성 정보 입력 데이터탐지규칙에 대하여 데이터 유형이 정상(Normal)행위, 공격(Attack)행위, 미지(Unknown)행위인지 판단한다(S610).

여기서 상기 데이터 유형은 도 3의 변환된 입력 데이터 형식의 마지막 항인 명명자에 의하여 판단하고, 정상 및 공격 행위에 속하지 않는 경우는 모두 미지 행위로 판단한다(S380).

각 데이터 유형(정상, 공격, 미지)에 따라 각각 오류율을 계산한다(S611, S612, S613).

정상 행위를 반영한 오류율은 탐지규칙 정확도의 오류율(100% 신뢰도 - 그 규칙의 신뢰도)에 정상 행위 데이터집합만을 대상으로 한 오류율을 곱한 값으로 계산한다(S611).

공격 행위를 반영한 오류율은 탐지규칙 정확도의 오류율에 공격 행위 데이터집합만을 대상으로 한 오류율을 곱한 값으로 계산한다(S612).

미지행위를 반영한 오류율은 정상 및 공격 행위가 아닌 데이터집합만을 대상으로 하여 미지 행위를 반영한 오류율을 계산한다(S613).

이렇게 각 데이터 유형(정상, 공격, 미지)에 따라 각각 오류율을 반영하는 것은 탐지규칙 정확도의 신뢰성을 높이는 의미를 지닌다.

S611- S613 단계에서 각각 계산된 오류율들을 바탕으로 가중치 부여, 퍼셉트론 규칙, 퍼지 이론 등을 이용하여 탐지규칙의 정확도를 계산한다(S620). 여기서 정확도는 상기 탐지규칙 자동생성부(140)에서와 마찬가지로 신뢰도와 지지도를 포함한다.

예를 들어, 가중치 부여 방법을 적용하는 경우에는 해당 규칙의 기존 정확도에 관리자가 정의한 각 데이터 유형에 대한 가중치와 계산된 오류율을 곱한 값을 더하여 계산한다.

그 후 탐지규칙 검증부에서 변환된 탐지규칙과 탐지규칙 저장 데이터베이스(150)에 저장된 탐지규칙들을 질의(query)를 통해 일치하는지를 검증하는 단계에서 검색된 규칙의 정확도를 자동으로 갱신한 후 탐지규칙 저장 데이터베이스(150)에 저장한다(S630, S640).

도 7 은 탐지규칙을 자동으로 생성하기 위한 전체 흐름도이다.

ERICSSON EXHIBIT 1005, Page 339

도 1 의 네트워크 데이터 생성부(110)에서 생성된 데이터를 네트워크 데이터 수집부(120)에서 생성된 데이터의 유형에 따라 수집한다. 그 후 상기 수집된 네트워크 데이터를 세션 특성 정보별로 분류한다(S700). 그 후 분류된 데이터를 세션 특성 정보 및 정상 유형, 공격 유형 및 미지 유형 중 상기 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 포함하는 입력 데이터 형식으로 변환한다(S710). 이에 대하여는 도 3에서 서술한 네트워크 세션 특성정보 추출부의 구성과 관련하여 서술한 내용을 참고한다.

상기 입력 데이터 형식으로 변환된 상기 데이터에 분류 알고리즘을 적용하여 결정트리를 구성하고(S720), 상기 결정트리의 최종노드에서 오류율을 기초로 상기 결정트리의 정확도를 생성한다(S730).

그 후, 상기 명칭, 상기 결정트리의 최적의 정보이득을 갖는 노드를 선택하기 위한 조건식, 및 상기 정확도를 기초로 상기 네트워크 데이터 유형별로 패턴화된 탐지규칙을 생성한다(S740). 이에 대하여는 도 4에서 서술한 탐지규칙 자동생성부의 구과 관련하여 서술한 내용을 참고한다.

이전에 생성된 상기 탐지규칙과 새롭게 생성된 상기 탐지 규칙이 일치하는지 판단한다(S750).이에 대하여는 도 5에서 서술한 탐지규칙 검증 및 갱신부 내의 탐지규칙 검증부의 구성과 관련하여 서술한 내용을 참고한다.

상기 탐지 규칙이 일치하는 경우 상기 각각의 네트워크 데이터 유형별 오류율을 상기 오류율에 상기 각각의 네트워크 데이터 유형만을 대상으로 한 오류율을 곱하여 생성하고, 상기 생성된 각각의 데이터 유형별 오류율을 기초로 상기 결정 트리의 정확도를 갱신한다(S760). 이에 대하여는 도 6에서 서술한 탐지규칙 검증 및 갱신부 내의 탐지규칙 자동갱신부의 구성과 관련하여 서술한 내용을 참고한다.

도 8 은 본 발명의 효과를 종래의 공격 탐지 방법 중의 하나와 비교하여 도시한 도면이다. 본 발명의 탐지규칙 형성 방법과 Florida Institute of Technology의 LERAD의 접근방법을 비교한 공격 탐지율의 차이를 도시하고 있다.

도 8 에서 가로축은 각 공격명을 명시한 것이고, 세로축은 각 공격에 대한 탐지율을 표시한다. 본 발명은 실선 화살표 부분으로 도시되고, 인용된 LERAD의 탐지율을 도시한다. 도면에 도시된 바와 같이 LERAD의 연구 결과보다 본 발명에서 10% 정도 향상된 탐지 결과를 볼 수 있다.

도 9 (a) 및(b)는 연속형 데이터를 이산형 데이터로 변환함으로써 탐지규칙의 정확도 향상을 나타내는 도면이다.

도 9(a)는 실험데이터인 DARPA 데이터의 주변 데이터에 적용한 결과, 연속형 데이터일 때의 탐지율보다 이산형 데이터로 변환하였을 때의 탐지율이 높음을 도시한다. 즉 도면에 도시된 바와 같이, Tue, Wed 데이터에 적용한 결과에서는 거의 향상이 이루어지지 않았으나, 나머지 데이터에서는 탐지율이 향상되고 있음을 볼 수 있다.

도 9(b) 는 연속형 데이터인 경우보다 이산형으로 변환한 데이터인 경우 오탐율이 더 낮아짐을 도시한다. 즉, Mon, Fri 데이터에 적용한 경우에는 큰 변화가 없으나, 그 외의 데이터에서는 오탐율(False Positive)이 낮아짐을 볼 수 있다.

도 10 및 도 11 은 본 발명의 일 실시예에 따른 탐지규칙 형성을 실험 데이터에 적용한 결과를 도시한다. 도 3 에서 각 세션별로 특성 정보를 누적(S320)하고 데이터 유형을 판단(S330)하기 전에 다양한 척도(measure)들 중에서 좋은 척도들을 우선 선택되도록 하여 DARPA 실험 데이터에 대해 적용한 결과이다.

GRR은 다음과 같이 정의한다.

$$\text{GRR(Good Rule Rate)} = \frac{RG\text{의 수}}{(RG+RB+\alpha)\text{의 수}}, \text{(이 때, } \alpha = 0.01\text{)}$$

매 단계마다 GRR값이 좋은 것은 선택(G)하고, 불필요한 것은 무시하고(I), 나쁜 것은 선택하지 않는(X) 식으로 시험한다. 위와 같은 방식으로 시험한 결과, 도 10에서와 같이 Wed와 Thu데이터에 적용했을 때 매 단계마다 좋은 척도만을 선택할 경우, 탐지율이 높고 오탐율이 낮아진다.

도 11에서 RST 는 시험 결과를 의미하고, SLT 는 선택을 의미한다.

ERICSSON EXHIBIT 1005, Page 340

본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플라피 디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

이상 도면과 명세서에서 최적 실시예들이 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다.

그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

본 발명에서는 네트워크 세션 기반의 특성 정보들에 대해 각 공격 유형별 탐지규칙들을 생성하고, 탐지 오류율을 계산하여 보다 더 정확한 탐지규칙들을 선별하고, 정확성이 낮은 탐지규칙들은 배제하는 과정을 자동으로 처리함으로써, 전문가의 도움 없이도 알려진 공격이나 유사한 공격 유형을 탐지하는데 효과적인 탐지규칙들을 자동으로 생성할 수 있어 보다 빠른 대응을 수행한다.

그에 따라, 변형된 공격행위나 알려지지 않은 새로운 공격에 대한 탐지에 있어 높은 정확성을 지니고 새로운 형태의 공격에 대한 대처 능력을 갖춘 탐지 규칙을 생성한다.

또한, 네트워크 패킷에서는 나타나지 않거나 정상적인 네트워크 데이터 흐름과 명확하게 구별할 수 없는 공격유형에 대한 특징들을 네트워크 세션 단위의 특성정보를 이용하여 추출하는 효과를 발생한다.

(57) 청구의 범위

청구항 1.

세션 특성 정보별로 분류된 네트워크 데이터를 상기 세션 특성 정보 및 정상 유형, 공격 유형 및 미지 유형 중 상기 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 포함하는 입력 데이터 형식으로 변환하는 네트워크 세션 특성정보 추출부; 및

상기 입력 데이터 형식으로 변환된 네트워크 데이터에 분류 알고리즘을 적용하여 결정트리를 구성하고, 상기 결정트리의 최종노드에서 오류율을 기초로 상기 결정트리의 정확도를 생성하며, 상기 네트워크 데이터 유형의 특성, 상기 결정트리의 최적의 정보이득을 갖는 노드를 선택하기 위한 조건식 및 상기 정확도를 기초로 상기 네트워크 데이터 유형별로 패턴화된 탐지규칙을 생성하는 탐지규칙 자동 생성부;를 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 장치.

청구항 2.

제 1 항에 있어서,

이전에 생성된 상기 탐지규칙과 새롭게 생성된 상기 탐지 규칙이 일치하는 경우

상기 각각의 네트워크 데이터 유형별 오류율은 상기 오류율에 상기 각각의 네트워크 데이터 유형만을 대상으로 한 오류율을 곱하여 생성하고, 상기 생성된 각각의 데이터 유형별 오류율을 기초로 상기 결정 트리의 정확도를 갱신하는 탐지규칙 검증 및 갱신부;를 더 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 장치.

ERICSSON EXHIBIT 1005, Page 341

청구항 3.

제 1 항에 있어서,

세션 특성정보별로 분류된 네트워크 데이터가 소정의 범위 내에서 연속적인지 여부에 따라 연속형과 이산형으로 나누고,

연속형인 경우 소정의 임계값 범위를 기준으로 소정의 범위 내에서 이산형 데이터 값으로 구획화가 되는 경우 이산형 데이터로 변환한 후

상기 네트워크 데이터를 정상 행위, 공격 행위 및 미지 행위의 유형별로 분류하여 상기 알고리즘의 상기 입력 데이터 형식으로 변환하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 장치.

청구항 4.

제 1 항에 있어서, 상기 알고리즘은

상기 세션 특성정보별로 분류된 네트워크 데이터의 분류별 빈도를 계산하고,

상기 계산된 빈도를 기초로 결정트리의 노드를 구성하며,

상기 각 노드별로 정보이득을 계산하여 최적의 정보이득을 갖는 노드를 선택하고

최종 노드에서 상기 오류율을 기초로 상기 결정트리의 정확도를 계산하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 장치.

청구항 5.

제 1 항에 있어서, 상기 세션 특성정보는

세션 전체 통계 정보, 네트워크 프로토콜 연결 정보, 네트워크 프로토콜 헤더정보, 두 호스트 사이의 연결 정보 중 하나 이상을 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 장치.

청구항 6.

네트워크 데이터를 세션 특성 정보별로 분류하는 단계;

상기 분류된 상기 데이터를 상기 세션 특성 정보 및 정상 유형, 공격 유형 및 미지 유형 중 상기 네트워크 데이터가 속하는 네트워크 데이터 유형의 특성을 포함하는 입력 데이터 형식으로 변환하는 단계;

상기 입력 데이터 형식으로 변환된 상기 데이터에 분류 알고리즘을 적용하여 결정트리를 구성하는 단계;

상기 결정트리의 최종노드에서 오류율을 기초로 상기 결정트리의 정확도를 생성하는 단계;및

상기 명칭, 상기 결정트리의 최적의 정보이득을 갖는 노드를 선택하기 위한 조건식, 및 상기 정확도를 기초로 상기 네트워크 데이터 유형별로 패턴화된 탐지규칙을 생성하는 단계;를 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 방법.

청구항 7.

ERICSSON EXHIBIT 1005, Page 342

제 6 항에 있어서,

이전에 생성된 상기 탐지규칙과 새롭게 생성된 상기 탐지 규칙이 일치하는지 판단하는 단계;

상기 탐지 규칙이 일치하는 경우 상기 각각의 네트워크 데이터 유형별 오류율을 상기 오류율에 상기 각각의 네트워크 데이터 유형만을 대상으로 한 오류율을 곱하여 생성하는 단계;및

상기 생성된 각각의 데이터 유형별 오류율을 기초로 상기 결정 트리의 정확도를 갱신하는 단계;를 더 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 방법.

청구항 8.

제 6 항에 있어서,

세션 특성정보별로 분류된 네트워크 데이터가 소정의 범위 내에서 연속적인지 여부에 따라 연속형과 이산형으로 나누는 단계;

연속형인 경우 소정의 임계값 범위를 기준으로 소정의 범위 내에서 이산형 데이터 값으로 구획화가 되는 경우 이산형 데이터로 변환하는 단계;및

상기 네트워크 데이터를 정상 행위, 공격 행위 및 미지 행위의 유형별로 분류하여 상기 알고리즘의 상기 입력 데이터 형식으로 변환하는 단계;를 더 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 방법.

청구항 9.

제 6 항에 있어서, 상기 분류 알고리즘은

상기 세션 특성정보별로 분류된 네트워크 데이터의 분류별 빈도를 계산하는 단계;

상기 계산된 빈도를 기초로 결정트리의 노드를 구성하는 단계;

상기 각 노드별로 정보이득을 계산하여 최적의 정보이득을 갖는 노드를 선택하는 단계;및

최종 노드에서 상기 오류율을 기초로 상기 결정트리의 정확도를 계산하는 단계;를 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 방법.

청구항 10.

제 6 항 또는 제 9 항에 있어서, 상기 분류 알고리즘은

확장된 C4.5 알고리즘인 것을 특징으로 하는 공격 행위 탐지 규칙 생성 방법.

청구항 11.

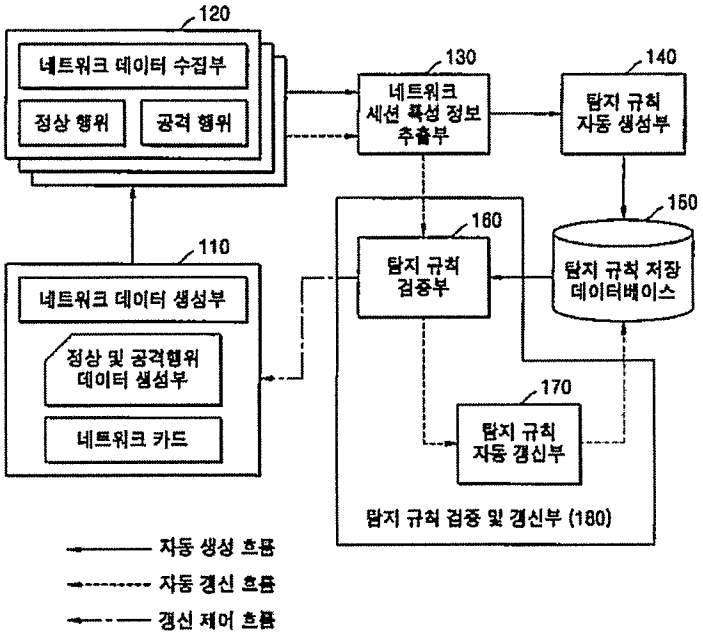
제 6 항에 있어서, 상기 세션 특성정보는

세션 전체 통계 정보, 네트워크 프로토콜 연결 정보, 네트워크 프로토콜 헤더정보, 두 호스트 사이의 연결 정보 중 하나 이상을 포함하는 것을 특징으로 하는 공격 행위 탐지 규칙 생성 방법.

ERICSSON EXHIBIT 1005, Page 343

도면

도면1



도면2a

정 보 명	설 명	유 형
Total packets	수집된 패킷의 총 개수	Continuous
TCP packets traced	각각 구별되는 TCP 연결 개수	Continuous
Elapsed wallclock time	패킷 수집의 전체 소요시간	Continuous
Packets/sec analyzed	분석 처리량	Continuous
Elasped time	첫 번째 패킷에서 마지막 패킷까지의 소요시간	Continuous
Traffic distribution	트래픽 분포 유형 (Local, Local-Remote, Remote-Local)	Discrete
Packets distribution	패킷 분포 유형 (unicast-broadcast-multicast, IP-nonIP)	Discrete
IP Multicast	멀티캐스트 패킷 개수	Continuous
Used bandwidth	평균 및 최대 대역폭량	Continuous
Packet sizes	최소, 평균, 최대, 초과(1500 bytes 이상) 패킷의 크기	Continuous

ERICSSON EXHIBIT 1005, Page 344

도면2b

정 보 명	설 명	유 형
TCP connections traced	각 TCP 연결 개수	Continuous
Host A	호스트 A의 IP 주소 또는 호스트 명	Discrete
Port of host A	호스트 A의 포트번호	Discrete
Host B	호스트 B의 IP 주소 또는 호스트 명	Discrete
Port of host B	호스트 B의 포트 번호	Discrete
Well-known ports	잘 알려진 각 서비스 포트들의 사용량 (사용자 정의된 포트들의 사용량)	Discrete
Complete connection	연결의 완료 여부(unidirectional, reset, complete, unknown)	Discrete
First packet	첫 번째 패킷의 시간	Continuous
Last packet	마지막 패킷의 시간	Continuous

도면2c

정 보 명	설 명	유 형
IP flags	단편화 정보항(0, DF, MF)	Discrete
TTL values	Time to Live 크기	Continuous
Header length	TCP 세그먼트 길이	Continuous
Code bits	코드 비트항(URG, ACK, PSH, RST, SYN, FIN)	Discrete

도면2d

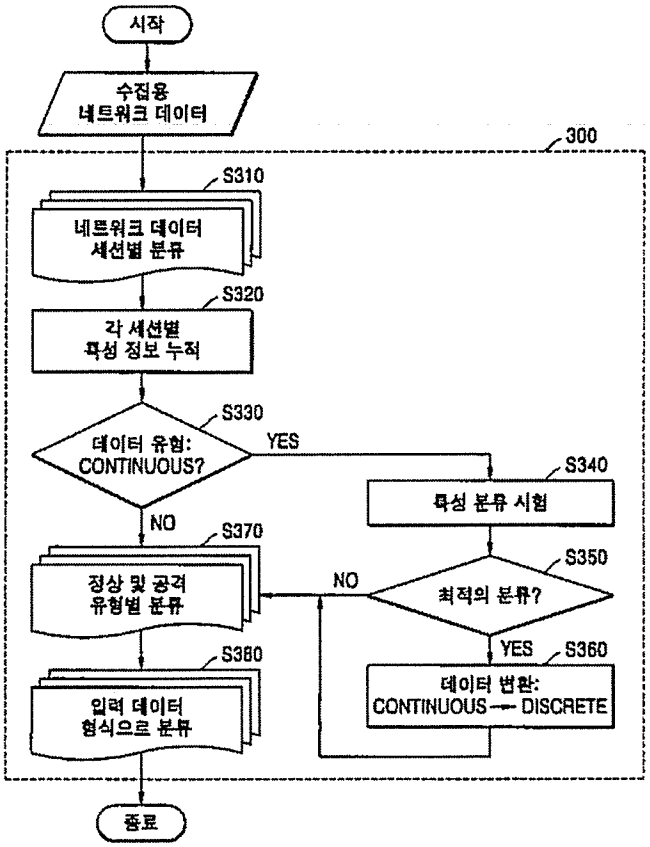
정 보 명	설 명	유 형
Packet counts	각 방향으로 보내진 패킷의 수	Continuous
ACK packets sent	유효 ACK에 포함된 패킷의 수	Continuous
Unique bytes sent	보내진 데이터 바이트의 양	Continuous
Actual data packets	데이터에 포함된 패킷의 양	Continuous
Actual data bytes	데이터 바이트의 양(재전송 포함)	Continuous
Retransmit data packets	재전송된 데이터 패킷의 양	Continuous
Retransmit data bytes	재전송된 데이터 바이트의 양	Continuous
Out of order packets	위배된 패킷의 양	Continuous
SYN/FIN packets sent	각 방향으로 보내진 SYN과 FIN의 개수	Discrete
mss requested	요청된 최대 세그먼트 크기	Continuous
Max segment size	가장 큰 세그먼트 크기	Continuous
Min segment size	가장 작은 세그먼트 크기	Continuous
Average segment size	평균 세그먼트 크기	Continuous
Max window adv	가장 큰 윈도우 공지(advertisement)	Continuous
Min window adv	가장 작은 윈도우 공지	Continuous
Zero window adv	크기 0인 윈도우 공지가 보내질 때 걸린 시간	Continuous
Average window adv	패킷이 보내지는 평균 윈도우 공지	Continuous
Bytes of initial window	첫 번째 윈도우의 바이트 양	Continuous
Packets of initial window	첫 번째 윈도우의 패킷의 양	Continuous
Throughput	초당 바이트 처리량	Continuous

ERICSSON EXHIBIT 1005, Page 345

도면2e

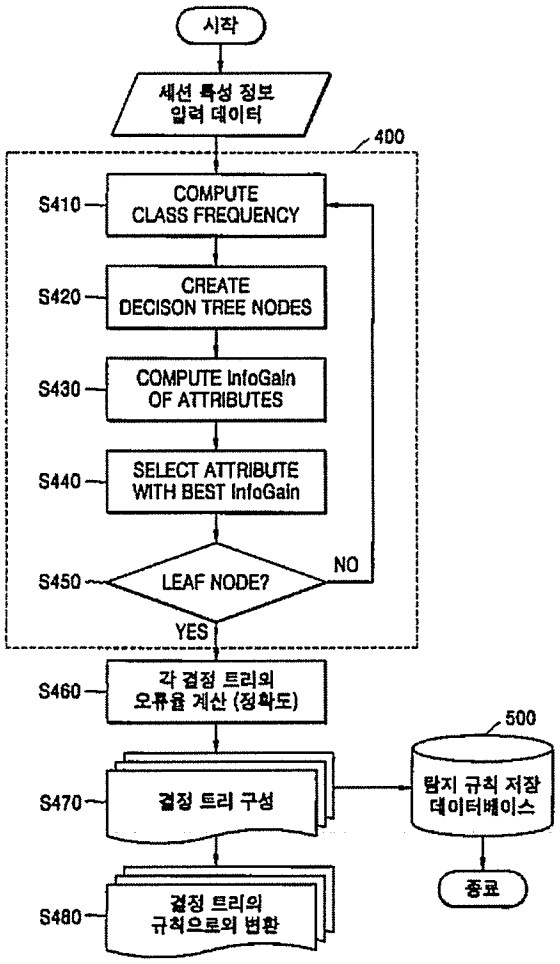
정 보 명	설 명	유 형
TTL stream length	FIN에서 SYN까지 스트림의 전체 길이	Continuous
Missed data	스트림에서 보이지 않았던 데이터의 바이트 양	Continuous
RTT samples	RTT(Round Trip Time) 샘플을 얻기 위해 사용된 ACK 개수	Discrete
RTT min	가장 작은 RTT	Discrete
RTT max	가장 큰 RTT	Discrete
RTT avg	평균 RTT	Discrete
RTT stdev	RTT의 표준편차(standard deviation)	Continuous
Segments cum ACKs	세그먼트에 누적된 ACK 개수	Discrete
Duplicate ACKs	중복된 ACK 개수	Discrete
Max # retransmit time	단일 세그먼트가 재전송되는 시간의 최대 수	Continuous
Min retransmit time	단일 세그먼트의 재전송 사이의 최소 시간	Continuous
Max retransmit time	단일 세그먼트의 재전송 사이의 최대 시간	Continuous
Average retransmit time	단일 세그먼트의 재전송 사이의 평균 시간	Continuous
Stdev retransmit time	재전송 시간의 표준편차(standard deviation)	Continuous
Urgent data packets	긴급 데이터 패킷의 수	Discrete
Urgent data bytes	긴급 데이터의 바이트 수	Continuous
Truncated data	잘린 데이터의 수	Continuous
Truncated packets	잘린 패킷의 수	Discrete
Data transmit time	데이터 전송 시간	Continuous
Max idle time	최대 지연 시간	Continuous

도면3

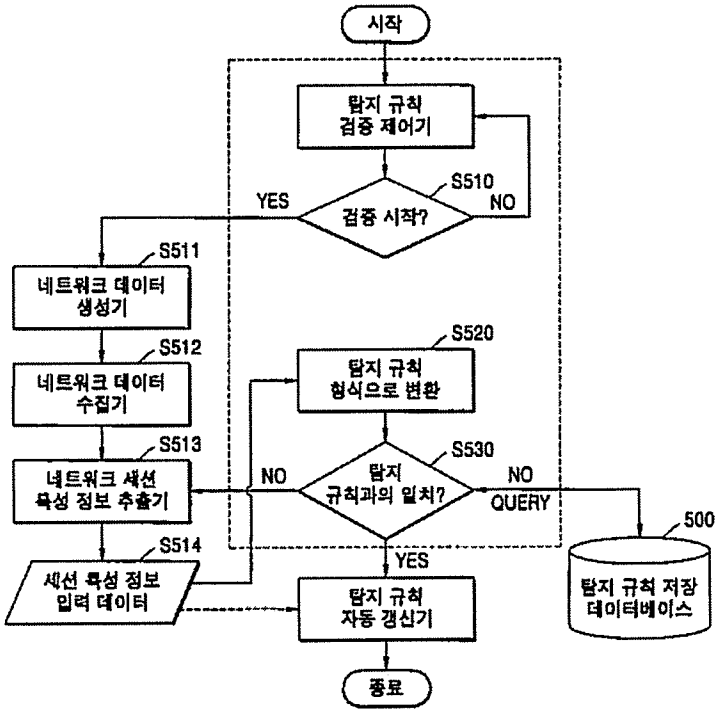


ERICSSON EXHIBIT 1005, Page 346

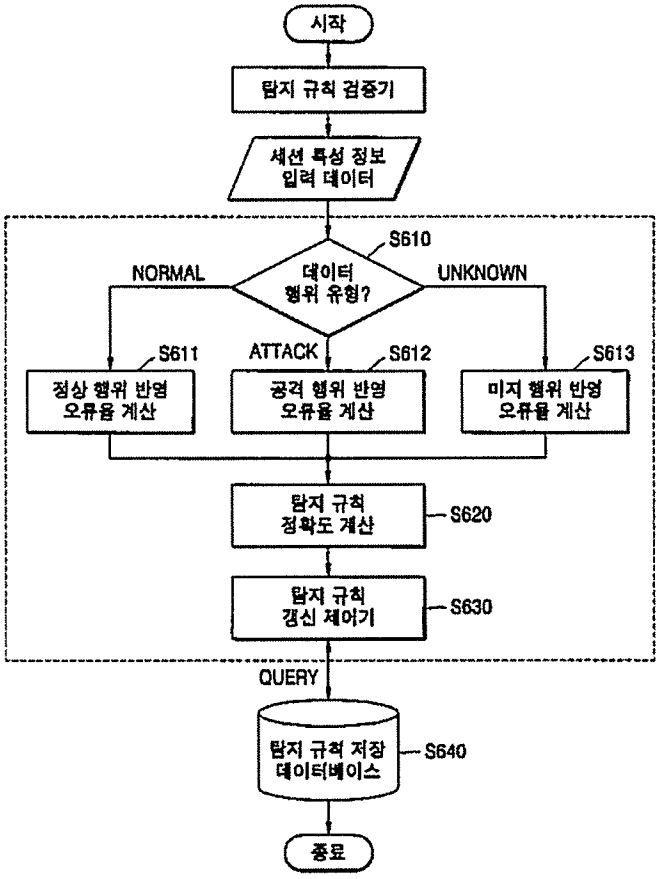
도면4


시작
세션 특성 정보
입력 데이터
400
S410
COMPUTE
CLASS FREQUENCY
S420
CREATE
DECISON TREE NODES
S430
COMPUTE InfoGain
OF ATTRIBUTES
S440
SELECT ATTRIBUTE
WITH BEST InfoGain
S450
LEAF NODE?
NO
YES
S460
각 결정 트리의
오류율 계산 (정확도)
500
S470
결정 트리 구성
탐지 규칙 저장
데이터베이스
종료
S480
결정 트리의
규칙으로의 변환

도면5

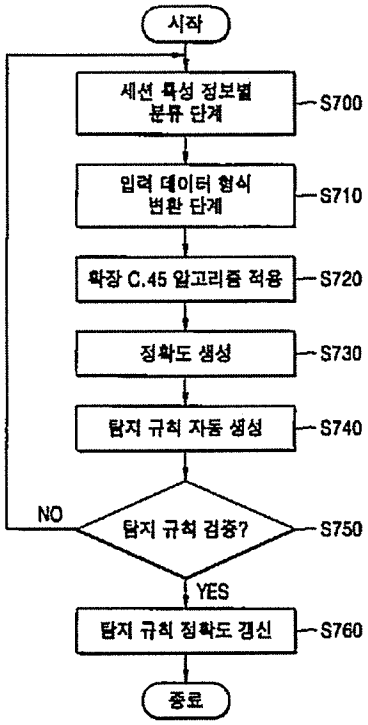

시작
탐지 규칙
검증 제어기
S510
검증 시작?
YES
NO
S511
네트워크 데이터
생성기
S512
네트워크 데이터
수집기
S513
네트워크 세션
특성 정보 추출기
S514
세션 특성 정보
입력 데이터
S520
탐지 규칙
형식으로 변환
S530
탐지
규칙과의 일치?
NO
NO
QUERY
YES
500
탐지 규칙 저장
데이터베이스
탐지 규칙
자동 갱신기
종료

도면6

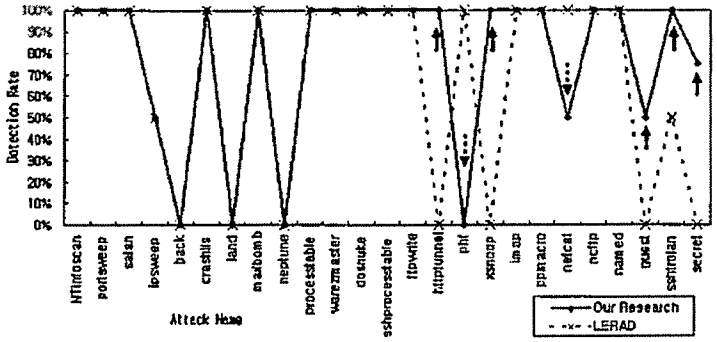


ERICSSON EXHIBIT 1005, Page 349

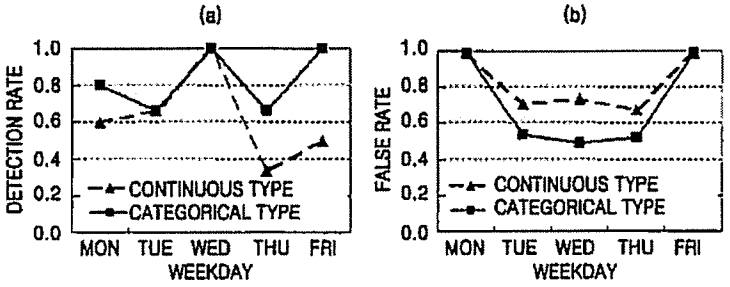
도면7


시작
세션 특성 정보별 분류 단계
S700
입력 데이터 형식 변환 단계
S710
확장 C.45 알고리즘 적용
S720
정확도 생성
S730
탐지 규칙 자동 생성
S740
NO
탐지 규칙 검증?
S750
YES
탐지 규칙 정확도 갱신
S760
종료

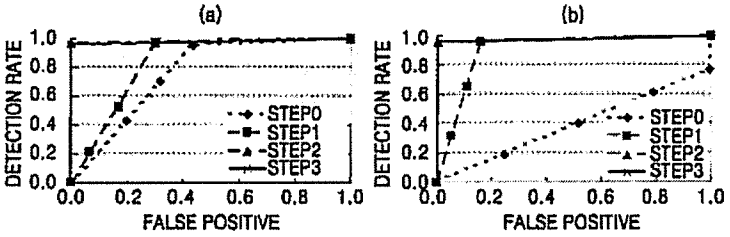
도면8


Detection Rate
Attack Name
Our Research
LERAD

도면9


(a)
(b)
DETECTION RATE
FALSE RATE
CONTINUOUS TYPE
CATEGORICAL TYPE
MON TUE WED THU FRI
WEEKDAY

도면10



도면11

No	Step0					Step1					Step2					Step3			
	RG	RB	GRR	RST	SLT	RG	RB	GRR	RST	SLT	RG	RB	GRR	RST	SLT	RG	RB	GRR	RST
1	0	0	0.00	I		3	1	0.75	G		11	1	0.92	G		11	1	0.92	G
3	0	0	0.00	I		0	0	0.00	I		7	7	0.50	B	X	0	0	0.00	I
4	7	28	0.20	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
5	10	5	0.67	G		18	10	0.64	G		19	11	0.63	G		19	9	0.68	G
6	6	7	0.46	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
8	0	0	0.00	I		30	20	0.60	G		38	14	0.73	G		38	12	0.76	G
10	3	0	1.00	G		8	4	0.67	G		6	1	0.86	G		6	1	0.86	G
13	0	0	0.00	I		0	0	0.00	I		61	15	0.80	G		61	13	0.82	G
20	37	30	0.55	G		35	39	0.47	B	X	0	0	0.00	I	X	0	0	0.00	I
21	0	0	0.00	I		2	0	1.00	G		10	0	1.00	G		10	0	1.00	G
22	0	0	0.00	I		0	0	0.00	I		5	0	1.00	G		5	0	1.00	G
24	0	0	0.00	I		5	1	0.83	G		55	14	0.80	G		55	12	0.82	G
26	17	11	0.61	G		23	14	0.62	G		34	13	0.72	G		34	11	0.76	G
27	10	5	0.67	G		20	10	0.67	G		34	13	0.72	G		34	11	0.76	G
28	0	0	0.00	I		0	0	0.00	I		2	0	1.00	G		2	0	1.00	G
38	4	0	1.00	G		3	1	0.75	G		3	2	0.60	G		3	2	0.60	G
39	4	1	0.80	G		4	1	0.80	G		0	0	0.00	I	X	0	0	0.00	I
41	19	26	0.42	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
43	0	0	0.00	I		2	3	0.40	B	X	0	0	0.00	I	X	0	0	0.00	I
45	21	18	0.54	G		2	0	1.00	G		13	0	1.00	G		13	0	1.00	G
46	0	0	0.00	I		6	4	0.60	G		9	4	0.69	G		9	4	0.69	G
47	10	5	0.67	G		20	10	0.67	G		22	11	0.67	G		22	9	0.71	G
48	3	3	0.50	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
49	0	0	0.00	I		0	0	0.00	I		6	0	1.00	G		6	0	1.00	G
50	27	26	0.51	G		20	37	0.35	B	X	0	0	0.00	I	X	0	0	0.00	I
51	10	8	0.56	G		7	13	0.35	B	X	0	0	0.00	I	X	0	0	0.00	I
52	0	0	0.00	I		2	0	1.00	G		0	0	0.00	I	X	0	0	0.00	I
53	0	0	0.00	I		0	0	0.00	I		26	12	0.68	G		26	10	0.72	G
54	49	48	0.51	G		49	52	0.49	B	X	0	0	0.00	I	X	0	0	0.00	I
55	11	4	0.73	G		21	9	0.70	G		12	1	0.92	G		12	1	0.92	G
56	7	12	0.37	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
60	4	1	0.80	G		9	3	0.75	G		64	17	0.79	G		64	15	0.81	G
61	3	0	1.00	G		0	0	0.00	I		8	5	0.61	G		8	5	0.61	G
62	0	0	0.00	I		10	3	0.77	G		25	2	0.93	G		25	2	0.93	G
63	0	0	0.00	I		2	0	1.00	G		5	0	1.00	G		5	0	1.00	G
64	0	0	0.00	I		5	2	0.71	G		3	0	1.00	G		10	5	0.67	G
65	12	12	0.50	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
66	6	5	0.54	G		8	17	0.32	B	X	0	0	0.00	I	X	0	0	0.00	I
67	2	0	1.00	G		3	8	0.27	B	X	0	0	0.00	I	X	0	0	0.00	I
68	18	29	0.38	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
75	1	2	0.33	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
76	4	1	0.80	G		46	51	0.47	B	X	0	0	0.00	I	X	0	0	0.00	I
77	46	48	0.49	B	X	0	0	0.00	I	X	0	0	0.00	I	X	0	0	0.00	I
78	0	0	0.00	I		13	26	0.33	B	X	0	0	0.00	I	X	0	0	0.00	I
79	17	11	0.61	G		25	14	0.64	G		32	13	0.71	G		32	11	0.74	G
80	6	0	1.00	G		13	10	0.56	G		14	5	0.74	G		14	5	0.74	G
Removed measure's numbers: 2, 7, 9, 11-12, 14-19, 23, 25, 29-37, 40, 43-44, 57-59, 69-74																			

ERICSSON EXHIBIT 1005, Page 351

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	27326654
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	26-OCT-2016
Filing Date:	21-MAY-2015
Time Stamp:	13:32:02
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$180
RAM confirmation Number	102616INTEFSW00014217132490
Deposit Account	132490
Authorized User	David Grabelsky

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.492 (National application filing, search, and examination fees)

37 CFR 1.492(a) (Basic national fee only)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	15-686-WO-US_Information_Disclosure_Statement_26Oct16.pdf	612290 a40bc19a7041a967c8cbf9ef32b5d50ac3a6b538	no	4
Warnings:					
Information:					
2	Foreign Reference	KR10-0628329.pdf	2114125 045511564653df6e8b06f70d826d42e537801942	no	36
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30472 c9eaf425dad925acae10206dad518ffae288eaef	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2756887		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 12/13/2016

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
12/13/2016	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) MULLER, FRANK	
	Examiner PHY ANH VU	Art Unit 2438	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/26/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☒ All b)☐ Some** c)☐ None of the:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *08/26/2016; 10/26/2016*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Amendment filed 08/26/2016.

Notice of Pre-AIA or AIA Status

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

Response to Arguments

Applicant's arguments filed 08/26/2016 have been fully considered but they are not persuasive.

On pages 11-12, Applicant argues that Bu does not teach “the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behavior of the mobile telecommunication device in the telecommunications network.

In response, Examiner respectfully disagrees and submits that first, the claim does not specify what “the data of the first type” comprises. Therefore, the recited "the data of the first type" is interpreted as any type of data flowing through the network. Second, Bu clearly discloses network traffic is monitored, because the network traffic flowing through the network of Bu will be identified as normal or suspicious *([0049]-[0053])*. For instance, when a packet from a specific sender is deemed suspicious, the specific sender and his packet will be flagged *([0057])*. Once the specific sender is flagged, the network of Bu continues to monitor network traffic from this specific sender, and when a sufficient number of packets have been flagged as suspicious from the

specific sender, then future traffic from the specific sender will be blocked *([0057])*. As such, contrasting to Applicant's argument, Bu discloses the limitations argues above.

Regarding 101 rejections, on page 10, Applicant argues that the new limitation "a base station…", which is added to the independent claims 1 and 14 are sufficient to overcome the 101 rejections.

In response, Examiner respectfully disagrees. A base station can be implemented using software, as such, the newly added limitation is not sufficient to over the 101 rejections. It is suggested that the claim be amended to recite "a hardware base station", in order to clarify that the base station is not a software.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claims 1 and 14, although the preamble of the claims recite "a system" and "device" respectively, the body of the claims do not positively recite any elements of hardware. Therefore, the nature of the subject matter claimed may reasonably be construed as non-tangible embodiments. The mere recitation of a system in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101.

Claims 2-13 and 15 depend on claims 1 and 14 respectively, as such, they also inherent the 101 rejections as their independent claims above.

Regarding claim 16, based upon consideration of all of the relevant factors with respect to the claim as a whole, claim 16 is determined to be directed to an abstract idea. The rationale for this determination is explained below:

Claim 16 is directed to method as recited. The method of claim 16 generally includes steps that receiving radio transmissions, identifying the mobile communications device, receiving the signals from the mobile communications device, monitoring for an occurrence in the data streams, and registering when the occurrence exceeds a level indicating acceptable behaviour of the mobile communications device. These steps correspond to a concept of comparing new and stored information and using rules to identify options (SmartGene). Although claim 16 recites that the steps in the method are carried out using a base station and a telecommunications network, these components do not add anything substantive to the performance of the methods, because the use of a base station and network to receiving radio transmissions, identifying the mobile communications device, receiving the signals from the mobile communications device, monitoring for an occurrence in the data streams, and registering when the occurrence exceeds a level indicating acceptable behaviour of the mobile communications device is well-established, and is therefore abstract without significant more. Therefore, claim 16 is rejected for the above reason.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-10 and 12-16 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu).

Regarding claim 1, Bu discloses a system for detecting behaviour of a mobile telecommunications device in a telecommunications network, the telecommunications network including a base station *([0023][0025], base station)*,

the system comprising:

the base station for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network *([0023][0025], base station)*;

the telecommunications network configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams *([0045]-[0047][0049]-[0053], signals from mobile/user is obtained and are processed into packets)*,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0060], normal/non-attack data)*, characterized in that,

the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network *([0049]-[0050][0057], if traffic ratio exceeds a certain threshold, signals as malicious)*.

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence of data of the first type by counting the number of occurrences data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of packets have been tagged as suspicious, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval *([0057], packets flagged have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer *(table 2; [0050]-[0057], packets are tracked and counted for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate *(table 2; [0054]-[0057], packets are tracked for predetermined threshold)*.

Regarding claim 6, Bu discloses the system according to claim 5. Bu further discloses the telecommunications network further includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate a rate as a ratio of counted detection of occurrence of data of the first type to time as measured by the timer *(table 2; [0054]-[0057], ratio of tracked packets is generated)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrence

exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network *([0019]-[0020][0027]-[0028], establishment data)*.

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates setting up of a bearer by the mobile telecommunications device *([0025], radio access bearer (RAB))*.

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicate handover of the mobile telecommunications device *(figure 5; [0037]-[0039])*.

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network *([0021], Serving Gateway Support Node (SGSN))*.

Regarding claim 13, Bu discloses the system according to claim 1. Bu further discloses the a telecommunications network is further configured to identify at least one additional mobile telecommunications device, to receive signals from the at least one additional device and to process these signals into additional data streams *([0045]-*

[0047][0049]-[0053], signals from another mobile/user is obtained and are processed into packets),

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if traffic ratio exceeds a certain threshold, signals as malicious)*,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Regarding claim 14, Bu discloses a device for detecting behaviour of a mobile telecommunications device in a telecommunications network wherein a base station of the telecommunications network converts radio transmissions received from the mobile telecommunications device into signals and wherein the signals are processed into data streams within the telecommunications network, and further wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0023][0025][0045]-[0047][0049]-[0053], base station converts radio transmission received from mobile/user and are processed into packets)*,

wherein the device is:

arranged to be coupled to the telecommunications network and arranged to receive the data streams and further wherein the device is arranged to monitor an occurrence in the data streams of the data of the first type and arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if traffic ratio exceeds a certain threshold, signals as malicious)*.

Regarding claim 15, Bu discloses a device according to claim 14. Bu further discloses the device is further arranged to operate within a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center *([0021], Serving Gateway Support Node (SGSN))*.

Claim 16 is rejected for the same rationale as claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin).

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0037]-[0039], handover to different BS)*.

Bu does not disclose monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on M-F 8:00-2:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH VU/
Examiner, Art Unit 2438
/TAGHI ARANI/
Supervisory Patent Examiner, Art Unit 2438

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	2483
Examiner Name	Vu, Phy Anh Tran
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/P.T.V/	1	20100064341	A1	2010-03-11	Carlo Aldera	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/P.T.V/	1	KR100628329	KR	B1	2006-09-19	Korea Electronics Telecomm		X

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

	1	

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

EXAMINER SIGNATURE

Examiner Signature	/PHY ANH T VU/	Date Considered	12/09/2016

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	2483
Examiner Name	Vu, Phy Anh Tran
Attorney Docket Number	15-686-WO-US

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2016-10-26
Name/Print	David A. Grabelsky	Registration Number	59,208

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank MULLER
Art Unit	2483
Examiner Name	Vu, Phy Anh Tran
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/P.T.V/	1	20120155274		2012-06-21	Wang et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/P.T.V/	1	JP2004-320636	JP		2004-11-11	NIPPON TELEGR & TELEPH CORP <NTT>		☒
/P.T.V/	2	JP2006-295240	JP		2006-10-26	MITSUBISHI ELECTRIC CORP		☒
/P.T.V/	3	WO2007075423	WO		2007-07-05	Lucent Technologies Inc.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

/P.T.V/	4	JP2006-350561	JP		2006-12-28	MATSUSHITA ELECTRIC IND CO LTD		☒

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

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

EXAMINER SIGNATURE

Examiner Signature	/PHY ANH T VU/	Date Considered	12/09/2016

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank MULLER
	Art Unit	2483
	Examiner Name	Vu, Phy Anh Tran
	Attorney Docket Number	15-686-WO-US

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2016-08-26
Name/Print	David A. Grabelsky	Registration Number	59,208

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
H04L 63/14	5/2/2016	PVU
H04L 63/1425	5/2/2016	PVU

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016; 12/09/2016	PVU

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	3	"20100064341".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:11
L2	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
L3	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13
L4	1342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
L5	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23
S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT;	OR	OFF	2016/05/02

			USOCR; DERWENT; IBM_TDB			09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:32
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33

S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16

12/9/2016 10:16:52 AM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	**Art Unit**
	PHY ANH VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16		✓							

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO FINAL OFFICE ACTION MAILED DECEMBER 13, 2016

In response to the Final Office Action mailed December 13, 2016, Applicant submits the following amendments and remarks. In addition, a request for consideration under the After Final Consideration Pilot 2.0 is included. Please charge any underpayment or credit any overpayment to Deposit Account No. 132490. Further, Applicants generally authorize the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system ~~for detecting behaviour of a mobile telecommunications device in a telecommunications network, the telecommunications network including a base station,~~ comprising:

~~the system comprising:~~

a telecommunications network; and

a hardware base station configured within the telecommunications network, wherein

the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,

~~characterized in that,~~

and wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type indicating the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

2. (Previously presented) The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence of data of the first type by

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

counting the number of occurrences data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Previously presented) The system according to claim 2 wherein the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Currently amended) The system according to claim 3 wherein the telecommunications network ~~further~~ includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

5. (Currently amended) The system according to claim 1 wherein the telecommunications network is <u>further</u> configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate.

6. (Currently amended) The system according to claim 5 wherein the telecommunications network ~~further~~ includes a counter and a timer, and wherein the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate a rate as a ratio of counted detection of occurrence of data of the first type to time as measured by the timer.

7. (Previously presented) The system according to claim 1 wherein the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Previously presented) The system according to claim 1 wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9. (Previously presented) The system according to claim 1 wherein the data of the first type indicates setting up of a bearer by the mobile telecommunications device.

10. (Previously presented) The system according to claim 1 wherein the data of the first type indicate handover of the mobile telecommunications device.

11. (Previously presented) The system according to claim 10 wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12. (Previously presented) The system according to claim 1 wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

13. (Previously presented) The system according to claim 1 wherein the a telecommunications network is further configured to

identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Canceled)

15. (Canceled)

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

16. (Currently amended) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network, the telecommunications network including a base station, the method comprising:

at the base station, ~~for~~ receiving radio transmissions from the mobile telecommunications device;

at the base station, converting the received radio transmissions into signals, and sending the signals into the telecommunications network;

in the telecommunications network, identifying the mobile telecommunications device;

in the telecommunications network, receiving the signals from the mobile telecommunications device by way of the base station, and processing the signals into data streams, wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network; and

in the telecommunications network, monitoring for an occurrence in the data streams of the data of the first type indicating the event of the first type and registering when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Final Office Action

In the Office Action mailed December 13, 2016 ("Current Final Office Action," hereinafter), the Examiner rejected claims 1-16 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. The Examiner rejected claims 1-10 and 12-16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). Finally, the Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-13 and 16, of which claims 1 and 16 are independent, and the remaining claims are dependent. Applicant has canceled claims 14 and 15 without prejudice, and amended various other claims as follows.

Applicant has amended claim 1 to clarify the structural components of the recited "system," including a "hardware base station" as suggested by the Examiner (Current Final Office Action, page 2). Applicant has also amended claim 1 to specify that the "occurrence in the data streams of the data of the first type" indicates "the event of the first type." Support for this amendment can be found generally throughout the original application, and specifically at least at page 3, lines 11-15, and page 7, lines 9-21, for example.

Applicant has amended claims 4, 5, and 6 to ensure consistency of antecedent basis.

Applicant has also amended claim 16 to identify structural elements that carry out steps of the recited method that involve physical actions, and to specify that the "occurrence in the data streams of the data of the first type" indicate "the event of the first type." Support for this amendment is generally the same as for the amendment to claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

No new matter has been introduced by way of any of the above amendments.

3. Response to Rejections under 35 U.S.C. § 101

The Examiner rejected claims 1-16 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Specifically, the Examiner asserted that the subject matter of claims 1 and 14 "may reasonably be construed as non-tangible embodiments. Without acquiescing to the Examiner's characterization of claims 1 and 14, Applicant has amended claim 1 to describe, *inter alia*, recited "system" in structural terms as comprising "a telecommunications network" and a "base station."

As also described above, Applicant has amended claim 16 to specifiy structural elements that carry out the recited method steps. Applicant submits that at least the recited steps of "receiving radio transmissions from the mobile telecommunications device" and "converting the received radio transmissions into signals" involve physical transformations that are integral to execution of the recited method, and that are not abstract.

In view of the above discussion, Applicant submits that these amendments overcome the rejections to claims 1 and 16 under 35 U.S.C. § 101, and respectfully requests the Examiner withdraw the rejections under 35 U.S.C. § 101 of claims 1 and 16, as well as of dependent claims 2-13. As noted above, Applicant has canceled claims 14 and 15, making the rejections of these claims moot.

4. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-10 and 12-16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. As noted above, Applicant has canceled claims 14 and 15, making these rejections of claims 14 and 15 moot. Regarding claims 1-10, 12-13, and 16, Applicant submits that Bu fails to teach each and every element set forth in any of claims 1-10, 12-13,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

or 16, and that these claims are allowable. Applicant first discusses claim 1, then subsequently addresses claims 2-10, 12-13, and 16.

Bu does not teach: "wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type indicating the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network"

In a "Response to Arguments" section of the Current Final Office Action (page 2), the Examiner asserted that "the data of the first type" could be interpreted broadly as "any type of data flowing through the network." Based on this broad interpretation, the Examiner maintained previous reliance on Bu's teachings in the anticipation rejection of claim 1.

Without acquiescing to the Examiner's characterization of "the data of the first type," Applicant has amended claim 1 (as described above) to specify that the "occurrence in the data streams of the data of the first type" indicates "the event of the first type." This amendment makes it is clear that "data of the first type" is indicative of "the event of the first type." As such, the Examiner's interpretation "the data of the first type" as "any type of data flowing through the network" is unambiguously excluded. That is, "data of the first type" *cannot* be "*any* type of data," but instead its occurrence in the data streams has explicit meaning: "indicating the event of the first type." Bu clearly does not teach this.

In the "Response to Arguments" section of the Current Final Office Action, the Examiner also asserted that Bu teaches monitoring of network traffic "because the network traffic flowing through the network of Bu will be identified as nor or suspicious." Applicant respectfully submits, however, that the teachings of Bu characterized by the Examiner as "monitoring" fall short of monitoring "an occurrence in the data streams of the data of the first type indicating the event of the first type," recited, *inter alia*, in claim 1.

Specifically, Bu teaches (paragraph [0049]):

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

> In accordance with the present invention, a statistical measure referred to as a *signaling cost to data ratio* is used as a metric. If the *ratio* exceeds a certain profiled threshold, a signaling attack is detected and malicious traffic/packets from the source of the attack are blocked. (Emphasis added.)

It is further clear from Table 2 in Bu that in determining the ratio "S/D," no distinction is made between possibly different types of data used in the computation. That is, the ratio "S/D" includes all signaling messages and all data packet arrivals related to a given user. There is no suggestion in Bu that the ratio "S/D," which forms the basis for the purported invention of Bu, could be determined using instead only "data of the first type indicating the event of the first type," as recited, *inter alia*, in claim 1. Accordingly, Applicant submits that Bu does not teach at least the above limitation of claim 1.

For at least the reasons above, Applicant respectfully submits that Bu does not anticipate claim 1, and that claim 1 is therefore allowable.

Claim 16 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 16 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 2-10 and 12-13 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claims 2-10 and 12-13 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with any of claims 2-10 or 12-13.

5. Response to Rejections under 35 U.S.C. § 103(a)

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

6. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: March 10, 2017

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
15-686-WO-US	14/646,554	May 22, 2015
First Named Inventor:	**Title:**	
Frank Muller	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
    - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
    - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
        - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
        - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
            - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
            - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/David A. Grabelsky/	March 10, 2017
Name (Print/Typed) David A. Grabelsky	**Practitioner Registration No.** 59,208

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

[✓] * Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	28592611
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	10-MAR-2017
Filing Date:	21-MAY-2015
Time Stamp:	11:45:25
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	15-686-WO-US_Response_13Dec16_FOA.pdf	150595 3be842a430c8d6e7fff50c950fea0928065f0bb8	no	11

Warnings:

Information:					
2	After Final Consideration Program Request	15-686-WO-US_AFCP_Request_13Dec16_FOA.pdf	226762 13b4ced35b0a53ed1837e5c15ceccf7dc3a4aadb	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	377357	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **03/10/2017**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

LIE
STEFANIE BRYCE

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 04/12/2017

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
04/12/2017	PAPER

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

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

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 14/646,554	**Applicant(s)** MULLER, FRANK	
	Examiner PHY ANH VU	**Art Unit** 2438	**AIA (First Inventor to File) Status** No

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

THE REPLY FILED 10 March 2017 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance;

(2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☐ The period for reply expires _____months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:

_____.

13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

14. ☒ Other: PTOL 2323 is attached.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: .
Claim(s) objected to: .
Claim(s) rejected: 1-16.
Claim(s) withdrawn from consideration: .

/TAGHI ARANI/ Supervisory Patent Examiner, Art Unit 2438	/PHY ANH VU/ Examiner, Art Unit 2438

The Applicant's request for entry into AFCP 2.0 is acknowledged and considered; however, the response with the amended features "..indicating event of the first type. " as amended in claims 1 & 16 cannot be fully reviewed and search conducted in the limited amount of time authorized for this pilot program and require further consideration and/or search.

AFCP 2.0 Decision	Application No.	Applicant(s)
	14/646,554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

This is in response to the After Final Consideration Pilot request filed 10 March 2017.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ A proper AFCP 2.0 request was submitted in response to the most recent final rejection.

   ☐ Other:

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☐ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☐ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action. See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☒ 5. Other: The Applicant's request for entry into AFCP 2.0 is acknowledged and considered; however, the response with the amended features "..indicating event of the first type. " as amended in claims 1 & 16 cannot be fully reviewed and search conducted in the limited amount of time authorized for this pilot program and require further consideration and/or search.

Examiner Note: Please attach an interview summary when necessary as described above.

DO NOT ENTER: /P.T.V/

04/06/2017

Doc Code: A.NE.AFCP

Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
15-686-WO-US	14/646,554	May 22, 2015
First Named Inventor:	**Title:**	
Frank Muller	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
   - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
   - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
     - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
     - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
       - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
       - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/David A. Grabelsky/	March 10, 2017
Name (Print/Typed) David A. Grabelsky	Practitioner Registration No. 59,208

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☑ * Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14/646,554	Filing Date	2015-05-22	Docket Number (if applicable)	15-686-WO-US	Art Unit	2438
First Named Inventor	Frank Muller			Examiner Name	Vu, Phy Anh Tran		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☒ Other After Final Response filed March 10, 2017

☐ Enclosed

☐ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132490

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2017-05-09
Name	David A. Grabelsky	Registration Number	59280

This collection of information is required by 37 CFR 1.114. 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 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.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

May 9, 2017 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
RCE- 1st Request	1801	1	1200	1200
		Total in USD ($)		**1800**

Electronic Acknowledgement Receipt

EFS ID:	29160098
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	09-MAY-2017
Filing Date:	21-MAY-2015
Time Stamp:	15:58:53
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1800
RAM confirmation Number	051017INTEFSW15595500
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	15-686-WO-US_Request_for_Continued_Examination_form_13Dec16_FOA.pdf	697834 69aa61dadf4b96c6ec034e88b876e985de6c3c26	no	3
Warnings:					
Information:					
2	Extension of Time	15-686-WO-US_Petition_for_one-month_Extension_of_Time.pdf	188321 0edd1d83402b878af9bfa897cc98ef45c419c69f	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32547 640944e729f4740f22304da6b95eedcfd86302bd	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	918702		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 06/27/2017

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
06/27/2017	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) MULLER, FRANK	
	Examiner PHY ANH VU	Art Unit 2438	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/09/2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-13 and 16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-13 and 16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *05/21/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☒ All b)☐ Some** c)☐ None of the:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/09/2017 has been entered.

Notice of Pre-AIA or AIA Status

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

Response to Amendment

Regarding claim 1, the amendments submitted are sufficient to overcome the previous 101 rejection with respect to the lack of hardware elements in the system claim. As such, the 101 rejections made in the previous Office Action pertaining to claims 1 and its dependent claims are hereby withdrawn.

Regarding claim 16, claim 16 was rejected under 101 as being an “abstract idea” in the previous Office Action. However, upon further considerations and consultation, claim 16 has been found statutory and thus not directed to an "abstract idea" as originally stated. Therefore, the 101 rejection made in the previous Office Action pertaining to claim 16 is hereby withdrawn.

Response to Arguments

Applicant's arguments with respect to claims 1 and 16 have been considered but are moot in view of the new interpretation of the reference.

Also, in an effort to clarify the Examiner's position, Applicant's arguments are addressed below:

Regarding claim 1, on pages 9-10, Applicant argues that Bu does not disclose 1) different types of data, therefore Bu does not teach "data of the first type indicating the event of the first type," and 2) wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type indicating the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

In response, Examiner respectfully disagrees, and submits that claim 1 as recited does not require different types of data. However, even if claim 1 recites the different types of data, Bu also teaches this limitation as detailed below:

1) Bu discloses all data packets arrived will be compared to a threshold to determine whether or not the data packets are part of an attack *([0050])*. The comparison identifies data packets with ratio that exceed the threshold ***(data of a first type),*** which indicates the likelihood of an attack ***(arranged to cause an event of a first type)****(table 2, [0054]-[0056])*. At the same time, since not all data packets related to the user exceed the threshold, the comparison also identifies data packets that do not

exceed the threshold, which indicates these data packets are not likely part of an attack, these data packets can be categorized as data of a second type.

2) Bu also discloses that the data packets that exceed the threshold ***(data of the first type indicating the event of the first type)*** are monitored and flagged (table 2, step 3), and when it is determined that a sufficient number of the data packets have been flagged, ***(monitored an occurrence in the data streams of the data of the first type indicating the event of the first type)*** filter may be applied to block future traffic ***(register the occurrence exceeds a level indicating acceptable behaviour)*** *(table 2, step 3, [0057]). As such, contrasting to the Applicant's arguments, Bu discloses all the limitations argue above.*

Claim Objections

Claims 2-13 are objected to because of the following informalities:

Claim 2 recites "'The' system according to claim 1 wherein..." which should be "'The' system according to claim 1**,** wherein..."

Claims 3-13 are also objected for the same rationale as claim 2 above.

Claim 3 also recites the limitation "..to count the occurrence of the data…" which should be "..to count the **number of** occurrence**s** of the data.."

Claim 13 recites in the preamble "wherein the a telecommunications network.." which should be ""wherein the ~~a~~ telecommunications network.." Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2-3 and 12-13 are rejected to because of the following:

Claim 2 recites the limitation ""..the number of occurrences data…" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 3 recites the limitation "..the time between a detected occurrence and the previously detected.." There is insufficient antecedent basis for this limitation in the claim.

Claim 12 recites the limitation "..the Mobility Management Entity.." There is insufficient antecedent basis for this limitation in the claim.

Claim 13 recites the limitation "..the registered data of the mobile communications device.." There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7-10, 12-13 and 16 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu).

Regarding claim 1, Bu discloses a system comprising:

a telecommunications network *(at least figures 4-5, 3G1x wireless network)*; and

a hardware base station configured within the telecommunications network *(figures 5-6, [0023][0029][0037][0040], base station)*, wherein the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network *([0023]-[0026], base station)*;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams *([0023]-[0026][0045]-[0047][0049]-[0053], signals from mobile/user are obtained and processed into data packets)*,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0056]-[0057], data packets with ratio that exceeds the threshold are flagged)*,

wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type indicating event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network

([0049]-[0050][0057]-[0057], data packets which have been flagged are monitored, and if a sufficient number of packets have been flagged, traffic will be blocked).

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence of data of the first type by counting the number of occurrences data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of packets have been tagged as suspicious, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the occurrence of the data of the first type in the data streams when the time between a detected occurrence and the previously detected occurrence is within a predetermined time interval *([0057], data packets that have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate *(table 2; [0054]-[0057], packets are tracked for predetermined threshold)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrence

exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates attachment of the mobile to telecommunications device to the telecommunications network *([0056][0060], data packets with ratio that exceed threshold indicates possible attack from the mobile to the network)*.

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates setting up of a bearer by the mobile telecommunications device *(table 2, [0050][0056]-[0057], the data packets with ratio that exceed the threshold indicates suspicious behavior by the mobile device)*.

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicate handover of the mobile telecommunications device *([0007][0023][0027], handoff)*.

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in the Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network *([0021][0056]-[0057], Serving Gateway Support Node (SGSN))*.

Regarding claim 13, Bu discloses the system according to claim 1. Bu further discloses the a telecommunications network is further configured to identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams *([0045]- [0047][0049]-[0053], signals from another mobile/user is obtained and are processed into packets)*,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if a sufficient number of packets have been flagged exceeds a certain threshold, signals as malicious)*,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Claim 16 is rejected for the same rationale as claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 6 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network includes a counter and a timer *(table 2, Flag*

++, and timer), and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs *(table 2, [0057] data packets which have been flagged are counted).*

Bu does not explicitly disclose increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

However, as another option for determining if the data packets are part of an attack, Bu also discloses a timer which times the suspicious behavior of traffic from a user, if the behaviour continues within a predetermined time interval T as measured by the timer, then the future traffic from the user will be blocked *(table 2; [0050]-[0057], packets are tracked and counted for a predetermined period of time)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine the timer and the counter as discloses by Bu to provide another way of determining suspicious data packets from users.

Claim 6 is rejected for the same rationale as claim 4 above.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin.)

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0007][0023][0027][0037]-[0039], handoff to different BS)*.

Bu does not disclose monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on M-F 8:00-2:00pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH VU/
Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/646,554	Applicant(s)/Patent Under Reexamination MULLER, FRANK	
	Examiner PHY ANH VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2004/0230834 A1	11-2004	McCallam, Dennis Hain	H04L41/046	726/23
*	B	US-2005/0198099 A1	09-2005	Motsinger, David Lee	G06F21/55	709/200
*	C	US-2005/0204169 A1	09-2005	Tonnesen, Steven D.	H04L63/1425	726/5
*	D	US-2006/0230450 A1	10-2006	Bu; Tian	H04L63/1416	726/22
*	E	US-2010/0199345 A1	08-2010	Nadir; Daniel O.	H04L63/02	726/11
*	F	US-2012/0124666 A1	05-2012	Kim; Jeong Hun	H04L63/14	726/23
*	G	US-2013/0291105 A1	10-2013	Yan; Zheng	G06Q10/06	726/22
*	H	US-2013/0304677 A1	11-2013	Gupta; Rajarshi	G06N5/043	706/12
*	I	US-2014/0031005 A1	01-2014	Sumcad; Anthony J.	H04W4/046	455/405
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 4961

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/646,554	05/21/2015	726	2438	15-686-WO-US

APPLICANTS

KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

INVENTORS

Frank Muller, Delft, NETHERLANDS;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/EP2013/074440 11/22/2013

**** FOREIGN APPLICATIONS ***************************

EUROPEAN PATENT OFFICE (EPO) 12193884.9 11/22/2012

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

07/07/2015

Foreign Priority claimed	☑ Yes ☐ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	☑ Yes ☐ No					
Verified and Acknowledged	/PHY ANH TRAN VU/ Examiner's Signature	Initials	NETHERLANDS	3	15	2

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

System to Detect Behaviour in a Telecommunications Network

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1480	No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	**Art Unit**
	PHY ANH VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016	06/23/2017						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	-						
	15	✓	✓	-						
	16		✓	✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		H04I63/14.cpc. and (excessive near5 (request occurrence traffic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
		"20060230450".pn. and nas	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:23
		(monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	1	H04I63/14.cpc. and (mobile and (excessive near5 occurrence))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:33
L2	1	H04I63/14.cpc. and (excessive near5 occurrence)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:34
L3	11	H04I63/14.cpc. and (excessive near5 (request occurrence traffic))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
L4	92	H04I63/14.cpc. and (excessive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:39
L5	48	l4 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:39
L6	237	H04I63/1425.cpc. and (mobile and excessive and (malicious attack suspicious))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:45
L7	71	l6 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:46
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19

S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23
S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28

S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:32
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16
S37	3	"20100064341".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:11
S38	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
S39	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13

S40	1342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S41	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S42	1121	(monitor$4 with (network with traffic) with event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S43	30	(monitor$4 with (network with traffic) with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S44	268	monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
S45	155	S44 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 11:54
S46	169	(network with indicat$4 near5 event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 12:55
S47	106	S46 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 12:55
S48	2	"20060230450".pn. and network	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:44
S49	1	"20060230450".pn. and bs	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:52
S50	1	"20060230450".pn. and pdsn	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:26
S51	2	"20150304345".pn. and (data near3 first near3 type)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:53
S52	13	"9684898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S53	2	"9684898".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S54	4	"9633208".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 18:00
S55	1	"20150304345".pn. and bearer	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2017/06/23 09:29

			EPO; DERWENT; IBM_TDB			
S56	0	"20060230450".pn. and handover	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:37
S57	0	"20060230450".pn. and hand$over	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S58	1	"20060230450".pn. and hand$off	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38

EAST Search History (Interference)

<This search history is empty>

6/23/2017 11:57:49 AM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
H04L 63/14	5/2/2016; 6/23/2017	PVU
H04L 63/1425	5/2/2016; 6/23/2017	PVU

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016; 12/09/2016; 6/23/2017	PVU
Consulted with WG SPE and QAS regarding 101 issues	06/23/2017	PVU

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO OFFICE ACTION MAILED JUNE 27, 2017

In response to the Office Action mailed June 27, 2017, Applicant submits the following amendments and remarks. Please charge any underpayment or credit any overpayment to Deposit Account No. 132490. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system comprising:

a telecommunications network; and

a hardware base station configured within the telecommunications network, wherein

the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams internal to the telecommunications network,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type representing an interaction in the telecommunications network between network devices,

and wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type, each occurrence indicating an occurrence of the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

2. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to monitor the occurrence of data of the first type by counting ~~the~~ a number of occurrences data of the first type is detected in the data streams when

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Currently amended) The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences of the data of the first type in the data streams when ~~the~~ a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Currently amended) The system according to claim 3, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

5. (Currently amended) The system according to claim 1, wherein the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate.

6. (Currently amended) The system according to claim 5, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate a rate as a ratio of counted detection of occurrence of data of the first type to time as measured by the timer.

7. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Currently amended) The system according to claim 1, wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9. (Currently amended) The system according to claim 1, wherein the data of the first type indicates setting up of a bearer by the mobile telecommunications device.

10. (Currently amended) The system according to claim 1, wherein the data of the first type indicate handover of the mobile telecommunications device.

11. (Currently amended) The system according to claim 10, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

12. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in ~~the~~ a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

13. (Currently amended) The system according to claim 1, wherein the [[a]] telecommunications network is further configured to

identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Canceled)

15. (Canceled)

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

16. (Currently amended) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network, the telecommunications network including a base station, the method comprising:

at the base station, receiving radio transmissions from the mobile telecommunications device;

at the base station, converting the received radio transmissions into signals, and sending the signals into the telecommunications network;

in the telecommunications network, identifying the mobile telecommunications device;

in the telecommunications network, receiving the signals from the mobile telecommunications device by way of the base station, and processing the signals into data streams internal to the telecommunications network, wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type representing an interaction in the telecommunications network between network devices; and

in the telecommunications network, monitoring for an occurrence in the data streams of the data of the first type, each occurrence indicating an occurrence of the event of the first type and registering when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Office Action

In the Action mailed June 27, 2017 ("Current Office Action," hereinafter), the Examiner objected to claims 2-13 for informalities. The Examiner rejected claims 2-3 and 12-13 under 35 U.S.C. § 112(b) or pre-AIA 35 U.S.C. § 112, second paragraph as allegedly being indefinite. directed to non-statutory subject matter. The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). Finally, the Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu, and rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-13 and 16, of which claims 1 and 16 are independent, and the remaining claims are dependent. Applicant has amended various other claims as follows.

Applicant has amended claim 1 described the recited "data streams" as being "internal to the telecommunications network." Applicant has further amended claim 1 to recite, *inter alia*, "the data of the first type representing an interaction in the telecommunications network between network devices." Applicant has also introduced clarifying language specifying "occurrences" of events. Support for this amendment can be found generally throughout the original application, and specifically at least at page 3, lines 20-23 and lines 32-34, and page 5, lines 13-16 and lines 23-24, for example.

Applicant has amended each of claims 2-13 to address informalities pointed out by the Examiner, and to ensure consistency of antecedent basis in each of the claims.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Applicant has amended claim 16 in a manner similar to that of claim 1. Support for this amendment is generally the same as for the amendment to claim 1.

No new matter has been introduced by way of any of the above amendments.

3. Response to Objections

The Examiner objected to claims 2-13 for informalities. Specifically, the Examiner pointed to what the Examiner appeared to consider minor grammatical errors and minor antecedent inconsistencies. Applicant submits that the amendments to these claims described above address the objections, and respectfully requests that the Examiner withdraw the objections.

4. Response to Rejections under 35 U.S.C. § 112

The Examiner rejected claims 2-3 and 12-13 under 35 U.S.C. § 112(b) or pre-AIA 35 U.S.C. § 112, second paragraph as allegedly being indefinite. Specifically, the Examiner asserted instances of lack of antecedent bases in these claims. Applicant submits that the amendments to these claims described above ensure consistency of antecedent basis in all of these claims, and respectfully requests that the Examiner withdraw the rejections of claims 2-3 and 12-13 under 35 U.S.C. § 112(b) or pre-AIA 35 U.S.C. § 112, second paragraph.

5. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. Applicant submits that Bu fails to teach each and every element set forth in any of claims 1-3, 5, 7-10, 12-13, or 16, and that these claims are allowable. Applicant first discusses claim 1, then subsequently addresses claims 2-3, 5, 7-10, 12-13, and 16.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Bu does not teach:

"wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type representing an interaction in the telecommunications network between network devices"

and

"wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type, each occurrence indicating an occurrence of the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network"

In a "Response to Arguments" section of the Current Office Action (pages 3-4), the Examiner, citing to paragraph [0050] in Bu, equated "the data of the first type" recited, *inter alia*, in claim 1, with data packets identified in Bu "with ratio that exceed the threshold." And the Examiner equated "an event of the first type," recited, *inter alia*, in claim 1, with "an attack," disclosed in Bu. The Examiner also equated "data of the first type indicating the event of the first type" recited, *inter alia*, in claim 1 with "data packets that exceed the threshold" that the Examiner asserted is disclosed in Bu, and further equated monitoring "an occurrence in the data streams of the data of the first type indicating the event of the first type" recited, *inter alia*, in a previous version of claim 1 with monitoring and flagging "data packets that exceed the threshold" that the Examiner asserted is disclosed in Bu. Finally, the Examiner equated registering "when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network" recited, *inter alia*, in claim 1 with applying a filter "to block future traffic" when "it is determined that a sufficient number of data packets have been flagged," that the Examiner asserted is disclosed in Bu. The Examiner largely reiterated these assertions on pages 6 and 7 of the Current Office Action in the anticipation rejection of claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Applicant respectfully submits that, as amended, claim 1 clearly distinguishes over Bu, and in particular, removes the bases for support for the Examiner's arguments as summarized above. Specifically, the data packets identified in Bu "with ratio that exceed the threshold," which the Examiner equated with "the data of the first type" in claim 1, refer to arriving packets for which it is determined that a "signaling cost to data ratio" exceeds a threshold for that ratio (paragraph [0056]). That is, Bu teaches that these packets are identified on the basis of an associated "signaling to data ratio" exceeding a threshold.

In contrast, claim 1 now recites, *inter alia*, "the data of the first type *representing an interaction in the telecommunications network between network devices*" (emphasis added). Applicant submits that data "representing an interaction in the telecommunications network between network devices" is clearly not the same as the data packets identified "with ratio that exceed the threshold," as taught in Bu.

As noted above, the Examiner equated "an event of the first type," recited, *inter alia*, in claim 1, with the "likelihood of an attack," disclosed in Bu. However, Applicant further submits that because "data of the first type" represents "an interaction in the telecommunications network between network devices," it follows that an "event of the first type" is "an interaction in the telecommunications network between network devices." Thus, as also recited, *inter alia*, in claim 1, "each occurrence [of data of the first type] indicating an occurrence of the event of the first type," means that each such occurrence is an indication of "an interaction in the telecommunications network between network devices." As such, even in an instance that "an interaction in the telecommunications network between network devices" is an attack, each monitored occurrence can be another occurrence of an attack. But in Bu, each packet "with ratio

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

that exceeds the threshold" is at best an indication of a possible ongoing attack, not an occurrence of *another* attack.

Applicant also submits that Bu does not teach monitoring and flagging "data packets that exceed the threshold," as characterized by the Examiner, but rather Bu teaches "[if] the derived ratio exceeds the threshold … *subsequent traffic from the sender 's' is flagged*" (paragraph [0056]; emphasis added). Thus, not only are arriving packets for which, in Bu, the "signaling cost to data ratio" exceeds the threshold not the same as "data of the first type" in claim 1, but the monitoring and flagging disclosed in Bu applies to "subsequent traffic from the sender 's'," *not* to the very data packets that the Examiner (incorrectly) equated with "data of the first type."

Finally, the disclosure in Bu of a filter "to block future traffic" from a sender teaches that the filter is applied in response to a threshold amount of flagged "subsequent traffic from the sender" (paragraph [0057]). That is, the filter is applied in response to monitoring and flagging "data packets that exceed the threshold," *not* to monitoring "an occurrence in the data streams of the data of the first type," as recited, *inter alia*, in claim 1. Thus, Bu teaches monitoring of different events than the "occurrence in the data streams of the data of the first type."

For at least the reasons above, Applicant respectfully submits that Bu does not anticipate claim 1, and that claim 1 is therefore allowable.

Claim 16 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 16 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 2-3, 5, 7-10, and 12-13 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claims 2-3, 5, 7-10, and 12-13 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

does not concede any the Examiner's specific assertions in connection with any of claims 2-3, 5, 7-10, or 12-13.

6. Response to Rejections under 35 U.S.C. § 103(a)

a. Claims 4 and 6

The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu. Each of claims 4 and 6 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that each of claims 4 and 6 is allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with either of claims 4 or 6.

b. Claim 11

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

7. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: September 25, 2017

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Electronic Acknowledgement Receipt

EFS ID:	30459435
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	25-SEP-2017
Filing Date:	21-MAY-2015
Time Stamp:	12:47:20
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	15-686-WO-US_Response_27Jun17_OA.pdf	158472 8d0c0c33c905b33bda1aec2a237cc021563 58231	no	13

Warnings:

Information:	
Total Files Size (in bytes):	158472

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	09/25/2017	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0		x $80 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	Ross W Brown
*** 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.	

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 11/29/2017

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
11/29/2017	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) MULLER, FRANK	
	Examiner PHY ANH VU	Art Unit 2438	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/25/2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-13 and 16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-13 and 16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *5/21/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☒ All b)☐ Some** c)☐ None of the:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Amendment filed 9/25/2017.

Notice of Pre-AIA or AIA Status

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

Claim Objections

Claims 1 and 16 are objected to because of the following informalities:

Claim 1 recites the limitation "..monitoring for an occurrence in the data streams of the data of the first type, each occurrence indicating an occurrence..." It is suggested that this limitation be changed to "..monitoring for ~~an~~ occurrence**s** in the data streams of the data of the first type, each occurrence indicating an occurrence..." in order to correctly conveys the inventive concept. Appropriate correction is required.

Claim 16 is objected for the same rationale.

Response to Arguments

Applicant's arguments filed 09/25/2017 have been fully considered but they are not persuasive.

Regarding claims 1 and 16 on pages 8-11, Applicant seems to argue that 1) the data packets that exceed the threshold and the subsequent traffic from the sender‘s’ as

disclose in Bu are not the very data packets that the Examiner incorrectly equated with 'data of the first type', 2) Bu teaches monitoring of different events than the 'occurrence in the data streams of the data of the first type'.

In response, Examiner respectfully disagrees, and submits that 1) all data packets transmitted from a particular sender is equivalent to the recited 'data streams'. The data packets from the sender can include data packets that do not have ratio that exceed the threshold, and data packets that do have ratio that exceed the threshold (table 2; [0054]-[0056]). The data packets that are determined to have ratio exceeding the threshold **(data of a first type)**, indicate the likelihood of an attack **(arranged to cause an event of a first type)** ([0054]-[0056]). The data packets having ratio exceeding the threshold **(data of a first type)** from the sender are tracked by the system, and when the number of the tracked data packets reaches a predetermined number, then future traffic **(including data packets with ratio that exceed the threshold)** from the particular sender will be blocked ([0057]). As such, the data packets that were determined to have ratio that exceed the threshold and the future traffic, which also include data packets with ratio exceeding the threshold are both from the same data streams of the particular user. 2) As discussed above, all data packets from a particular user is equivalent to the recited "data streams", and the same data packets from the particular user is monitored for data packets that have ratio exceeding the threshold (table 2; [0054]-[0056]). So, contrasting to the Applicant's argument, Bu clearly discloses the monitoring is for occurrence in the same data streams, and not for

different event as argue by the Applicant. As such, Applicant's argument is not persuasive for the above reasons.

Regarding claim 16, please see response for claim 1 above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7-10, 12-13 and 16 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu).

Regarding claim 1, Bu discloses a system comprising:

a telecommunications network *(at least figures 4-5, 3G1x wireless network)*; and

a hardware base station configured within the telecommunications network *(figures 5-6, [0023][0029][0037][0040], base station)*, wherein the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network *([0023]-[0026], base station)*;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the

signals into data streams, internal to the telecommunications network *([0023]-[0026][0045]-[0047][0049]-[0053], signals from mobile/user are obtained and processed into data packets with the network)*,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0056]-[0057], data packets with ratio that exceeds the threshold are flagged)*,

wherein the telecommunications network is arranged to monitor an occurrence in the data streams of the data of the first type indicating event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network *([0049]-[0050][0057]-[0057], data packets which have been flagged are monitored, and if a sufficient number of packets have been flagged, traffic will be blocked)*.

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence of data of the first type by counting a number of occurrences data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of packets have been tagged as suspicious, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the number of occurrences of the data of the first type in the data streams when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval *([0057], data packets that have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate *(table 2; [0054]-[0057], packets are tracked for predetermined threshold)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates attachment of the mobile to telecommunications device to the telecommunications network *([0056][0060], data packets with ratio that exceed threshold indicates possible attack from the mobile to the network)*.

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates setting up of a bearer by the mobile telecommunications device *(table 2, [0050][0056]-[0057], the data packets with ratio that exceed the threshold indicates suspicious behavior by the mobile device)*.

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicate handover of the mobile telecommunications device *([0007][0023][0027], handoff)*.

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network *([0021][0056]-[0057], Serving Gateway Support Node (SGSN))*.

Regarding claim 13, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is further configured to identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams *([0045]- [0047][0049]-[0053], signals from another mobile/user is obtained and are processed into packets)*,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if a sufficient number of packets have been flagged exceeds a certain threshold, signals as malicious)*,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Claim 16 is rejected for the same rationale as claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 6 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network includes a counter and a timer *(table 2, Flag ++, and timer)*, and wherein the telecommunications network is arranged to start the

counter upon detection of an occurrence of data of the first type, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs *(table 2, [0057] data packets which have been flagged are counted).*

Bu does not explicitly disclose increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

However, as another option for determining if the data packets are part of an attack, Bu also discloses a timer which times the suspicious behavior of traffic from a user, if the behaviour continues within a predetermined time interval T as measured by the timer, then the future traffic from the user will be blocked *(table 2; [0050]-[0057], packets are tracked and counted for a predetermined period of time).*

One of ordinary skill in the art at the time the invention was made would have been motivated to combine the timer and the counter as discloses by Bu to provide another way of determining suspicious data packets from users.

Claim 6 is rejected for the same rationale as claim 4 above.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin.)

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0007][0023][0027][0037]-[0039], handoff to different BS).*

Bu does not disclose monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on M-F 8:00-2:00pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH VU/
Examiner, Art Unit 2438

/TAGHI ARANI/

Supervisory Patent Examiner, Art Unit 2438

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	**Art Unit**
	PHY ANH VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016	06/23/2017	11/22/2017					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	-	-					
	15	✓	✓	-	-					
	16		✓	✓	✓					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		H04I63/14.cpc. and (excessive near5 (request occurrence traffic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
		"20060230450".pn. and nas	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:23
		(monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	1	H04I63/14.cpc. and (mobile and (excessive near5 occurrence))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:33
L2	1	H04I63/14.cpc. and (excessive near5 occurrence)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:34
L3	11	H04I63/14.cpc. and (excessive near5 (request occurrence traffic))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
L4	92	H04I63/14.cpc. and (excessive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:39
L5	48	l4 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:39
L6	237	H04I63/1425.cpc. and (mobile and excessive and (malicious attack suspicious))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:45
L7	71	l6 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:46
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19

S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23
S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28

S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:32
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16
S37	3	"20100064341".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:11
S38	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
S39	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13

S40	1342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S41	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S42	1121	(monitor$4 with (network with traffic) with event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S43	30	(monitor$4 with (network with traffic) with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S44	268	monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
S45	155	S44 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 11:54
S46	169	(network with indicat$4 near5 event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 12:55
S47	106	S46 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 12:55
S48	2	"20060230450".pn. and network	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:44
S49	1	"20060230450".pn. and bs	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:52
S50	1	"20060230450".pn. and pdsn	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:26
S51	2	"20150304345".pn. and (data near3 first near3 type)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:53
S52	13	"9684898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S53	2	"9684898".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S54	4	"9633208".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 18:00
S55	1	"20150304345".pn. and bearer	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2017/06/23 09:29

			EPO; DERWENT; IBM_TDB			
S56	0	"20060230450".pn. and handover	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:37
S57	0	"20060230450".pn. and hand$over	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S58	1	"20060230450".pn. and hand$off	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38

EAST Search History (Interference)

<This search history is empty>

6/23/2017 11:58:07 AM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14646554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
H04L 63/14	5/2/2016; 6/23/2017	PVU
H04L 63/1425	5/2/2016; 6/23/2017	PVU

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016; 12/09/2016; 6/23/2017; 11/22/2017	PVU
Consulted with WG SPE and QAS regarding 101 issues	06/23/2017	PVU

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO FINAL OFFICE ACTION MAILED NOVEMBER 29, 2017

In response to the Final Office Action mailed November 29, 2017, Applicant submits the following amendments and remarks. In addition, a request for consideration under the After Final Consideration Pilot 2.0 is included, as well as a Petition for Extension of Time under 37 C.F.R. § 1.136(a) (two-month), along with requisite fees. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system comprising:

a telecommunications network comprising a core network; and

a hardware base station configured within the telecommunications network, wherein

the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams internal to the telecommunications network,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type being a predetermined type representing an interaction between network devices in the ~~telecommunications~~ core network ~~between network devices~~,

wherein each event of the first type is an occurrence in the data streams of data of the first type,

and wherein the telecommunications network is arranged to monitor [[an]] the occurrence in the data streams of the data of the first type, ~~each~~ wherein the occurrence ~~indicating~~ indicates an ~~occurrence~~ incidence of the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

2. (Previously presented) The system according to claim 1, wherein the telecommunications network is arranged to monitor the occurrence of data of the first type by counting a number of occurrences data of the first type is detected in the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Previously presented) The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences of the data of the first type in the data streams when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Previously presented) The system according to claim 3, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

5. (Previously presented) The system according to claim 1, wherein the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

6. (Previously presented) The system according to claim 5, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate a rate as a ratio of counted detection of occurrence of data of the first type to time as measured by the timer.

7. (Previously presented) The system according to claim 1, wherein the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Previously presented) The system according to claim 1, wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9. (Previously presented) The system according to claim 1, wherein the data of the first type indicates setting up of a bearer by the mobile telecommunications device.

10. (Previously presented) The system according to claim 1, wherein the data of the first type indicate handover of the mobile telecommunications device.

11. (Previously presented) The system according to claim 10, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12. (Previously presented) The system according to claim 1, wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

13. (Previously presented) The system according to claim 1, wherein the telecommunications network is further configured to

identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Canceled)

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

15. (Canceled)

16. (Currently amended) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network comprising a core network, the telecommunications network including a base station, the method comprising:

at the base station, receiving radio transmissions from the mobile telecommunications device;

at the base station, converting the received radio transmissions into signals, and sending the signals into the telecommunications network;

in the telecommunications network, identifying the mobile telecommunications device;

in the telecommunications network, receiving the signals from the mobile telecommunications device by way of the base station, and processing the signals into data streams internal to the telecommunications network, wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type being a predetermined type representing an interaction between network devices in the ~~telecommunications~~ core network, wherein each event of the first type is an occurrence in the data streams of data of the first type ~~between network devices~~; and

in the telecommunications network, monitoring for an occurrence in the data streams of the data of the first type, ~~each~~ wherein the occurrence ~~indicating~~ indicates an ~~occurrence~~ instance of the event of the first type and registering when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Final Office Action

In the Final Action mailed November 29, 2017 ("Current Final Office Action," hereinafter), the Examiner objected to claims 1 and 16 for informalities. The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). Finally, the Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu, and rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-13 and 16, of which claims 1 and 16 are independent, and the remaining claims are dependent. Applicant has amended various other claims as follows.

Applicant has amended claim 1 to describe the recited "telecommunications network" as "comprising a core network." Applicant has further amended claim 1 to describe the recited "data of the first type" as "being a predetermined type" and to introduce clarifying rewording describing an "event of the first time" being "occurrence in the data streams of data of the first type," and describing the "occurrence in the data streams of data of the first type" as indicating "an incidence of the event of the first type." Support for this amendment can be found generally throughout the original application, and specifically at least at page 3, lines 32-34; page 5, lines 5-11; page 8, lines 1-6; and Figure 1, for example.

Applicant has amended claim 16 in a manner similar to that of claim 1. Support for this amendment is generally the same as for the amendment to claim 1.

No new matter has been introduced by way of any of the above amendments.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

3. Response to Objections

The Examiner objected to claims 1 and 16 for informalities. Specifically, the Examiner objected to the language "…monitor an occurrence in the data streams of the data of the first type, each occurrence indicating an occurrence…," and suggested a possible rewording to overcome the rejection. Applicant submits that the amendments to these claims described above, which adopt a somewhat different approach than the one suggested by the Examiner, address the objections, and respectfully requests that the Examiner withdraw the objections.

4. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. Applicant submits that Bu fails to teach each and every element set forth in any of claims 1-3, 5, 7-10, 12-13, or 16, and that these claims are allowable. Applicant first discusses claim 1, then subsequently addresses claims 2-3, 5, 7-10, 12-13, and 16.

Bu does not teach:

"wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type being a predetermined type representing an interaction between network devices in the core network"

and

"wherein each event of the first type is an occurrence in the data streams of data of the first type"

In a "Response to Arguments" section of the Current Final Office Action (pages 2-4), the Examiner, citing to paragraphs [0054]-[0056] in Bu, equated "the data of the first type" recited, *inter alia*, in claim 1, with data packets identified in Bu "that are determined to have ratio exceeding the threshold." And the Examiner equated "an event of the first type," recited, *inter alia*, in claim 1, with "an attack," disclosed in Bu. On page 5 of the Current Final Office Action, the Examiner, citing to paragraphs [0056]-[0057] in Bu, equated "wherein the data streams

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

include data of a first type arranged to cause an event of a first type within the telecommunications network" recited, *inter alia*, in claim 1 with "data packets with ratio that exceeds the threshold are flagged" disclosed in Bu. Applicant respectfully submits that, as amended, claim 1 clearly distinguishes over Bu, and in particular, removes the bases for support for the Examiner's arguments as summarized above.

Specifically, the Examiner, as noted, equated data packets having a "ratio exceeding the threshold" in Bu with "the data of the first type" recited, *inter alia*, in claim 1. However, as amended, claim 1 now describes "the data of the first type *being a predetermined type representing an interaction between network devices in the core network*." (Emphasis added.) That is, the "predetermined type" characterizes data that represents "an interaction between" devices in "the core network."

While it may be possible to consider an interpretation of Bu in which data packets having a "ratio exceeding the threshold" are involved in interactions "between network devices in the core network," Bu clearly does not teach a "predetermined type" that specifically characterizes data representing "an interaction between" devices in "the core network." Indeed, given the absence in Bu of any such teaching, an equally plausible interpretation of Bu could be that data packets having a ratio *smaller* than the threshold are also involved in interactions "between network devices in the core network." In other words, the teachings of Bu regarding data packets having a "ratio exceeding the threshold" provide no basis to distinguish between data that either do or do *not* represent "an interaction between" devices that in "the core network." Or simply put, Bu does not teach the "predetermined type" recited, *inter alia*, in claim 1.

Also as summarized above, the Examiner specifically equated "an event of the first type," recited, *inter alia*, in claim 1, with "an attack" disclosed in Bu. However, as amended, claim 1

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

describes "each event of the first type" as being "an occurrence in the data streams of data of the first type." Even if, for the sake of argument, Bu was interpreted as teaching "occurrence in the data streams of data of the first type" – i.e., data of the "predetermined type" – there is simply no teaching in Bu that such an occurrence is "an attack." And in any case, because Bu fails to even teach the "predetermined type" recited, *inter alia*, in claim 1 Bu necessarily cannot teach a "first type of event" that is "an occurrence" of data of the "predetermined type" to begin with.

Bu does not teach: "wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type, wherein the occurrence indicates an incidence of the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network"

For at least the reason that Bu fails to teach either "data of the first type" or the "event of the first type," Bu cannot teach "wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type, wherein the occurrence indicates an incidence of the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network." Even beyond this, while Bu teaches comparing a "signaling cost" to an amount of data transmitted as a result of the signaling in order to determining a "signaling cost to data ratio" (e.g., paragraph [0054]), Bu does not teach distinguishing between (i) data (signaling or otherwise) sent between a mobile device and a wireless network and (ii) data sent between network devices in a core network. Thus, in Bu, signaling messages between a base station and a mobile device may be included in determining signaling cost, along with signaling messages that may be generated only between network devices within the network – i.e., along with signaling messages exclusive of those between the mobile device and the base station.

In contrast, claim 1 recites, *inter alia*, that the "data of the first type" is of "a predetermined type representing an *interaction between network devices in the core network*."

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

(Emphasis added). In other words, "data of the first type" does not include data between "mobile telecommunications devices" and the base station. It only includes data "representing an interaction between network devices in the core network." Yet the signaling data disclosed in Bu may include both types of data, and Bu does not teach any way or need to distinguish between them. Accordingly, to the extent that it may be possible to interpret Bu as teaching "monitoring for an occurrence in the data streams of" signaling data, Bu clearly does not teach that such monitoring excludes possible signaling data between "mobile telecommunications devices" and the base station. Thus, Bu clearly fails to teach monitoring "the occurrence in the data streams of the data of the first type."

For at least the reasons above, Applicant submits that claim 1 distinguishes over Bu, and that claim 1 is therefore allowable.

Claim 16 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 16 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 2-3, 5, 7-10, and 12-13 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claims 2-3, 5, 7-10, and 12-13 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with any of claims 2-3, 5, 7-10, or 12-13.

5. Response to Rejections under 35 U.S.C. § 103(a)

a. Claims 4 and 6

The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu. Each of claims 4 and 6 depends from claim 1, which is

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

allowable for at least the reasons above. Applicant therefore submits that each of claims 4 and 6 is allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with either of claims 4 or 6.

b. Claim 11

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

6. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: April 30, 2018

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
15-686-WO-US	14/646,554	May 22, 2015
First Named Inventor:	**Title:**	
Frank Muller	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
    - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
    - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
        - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
        - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
            - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
            - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/David A. Grabelsky/	April 30, 2018
Name (Print/Typed) David A. Grabelsky	**Practitioner Registration No.** 59,208

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

[✓] * Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

April 30, 2018 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
			Total in USD ($)	**600**

Electronic Acknowledgement Receipt

EFS ID:	32480632
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	30-APR-2018
Filing Date:	21-MAY-2015
Time Stamp:	11:26:50
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	043018INTEFSW11273500
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	15-686-WO-US_Response_29Nov17_FOA.pdf	171665 fe577aacf731c5c778a6c3c60ce55cb7f4d5dfc0	no	12
Warnings:					
Information:					
2	After Final Consideration Program Request	15-686-WO-US_AFCP_Request_29Nov17_FOA.pdf	226763 7b351dc25ee03356910307b4bd4d48b9f8d2c056	no	2
Warnings:					
Information:					
3	Extension of Time	15-686-WO-US_Petition_for_two-month_Extension_of_Time.pdf	188332 4eebcace2eff098a93804e0bd8d6b752d71e9506	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30712 c408689269c938a69580e7ff9744f0a7c4c1db2c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	617472		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **04/30/2018**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0	X $100 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $460 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

LIE
JACQUELYN 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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 05/14/2018

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
05/14/2018	PAPER

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

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

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *14/646,554*	**Applicant(s)** MULLER, FRANK	
	Examiner PHY ANH VU	**Art Unit** 2438	**AIA (First Inventor to File) Status** No

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

THE REPLY FILED 30 April 2018 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance;

(2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☐ The period for reply expires _____months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See continuation sheet.

13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

14. ☒ Other: Form PTOL-2323 is attached.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: .
Claim(s) objected to: .
Claim(s) rejected: 1-13 and 16.
Claim(s) withdrawn from consideration: .

/PHY ANH VU/
Examiner, Art Unit 2438

The Applicant's request for entry into AFCP 2.0 is acknowledged and considered; however, the response with the amendments to claims 1 & 16 cannot be fully reviewed and search conducted in the limited amount of time authorized for this pilot program and require further consideration and/or search.

AFCP 2.0 Decision	Application No.	Applicant(s)
	14/646,554	MULLER, FRANK
	Examiner	Art Unit
	PHY ANH VU	2438

This is in response to the After Final Consideration Pilot request filed 30 April 2018.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ A proper AFCP 2.0 request was submitted in response to the most recent final rejection.

   ☐ Other:

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☐ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☐ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action. See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☒ 5. Other: The Applicant's request for entry into AFCP 2.0 is acknowledged and considered; however, the response with the amendments to claims 1 & 16 cannot be fully reviewed and search conducted in the limited amount of time authorized for this pilot program and require further consideration and/or search.

   Examiner Note: Please attach an interview summary when necessary as described above.

DO NOT ENTER: /P.T.V/

05/09/2018

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO FINAL OFFICE ACTION MAILED NOVEMBER 29, 2017

In response to the Final Office Action mailed November 29, 2017, Applicant submits the following amendments and remarks. In addition, a request for consideration under the After Final Consideration Pilot 2.0 is included, as well as a Petition for Extension of Time under 37 C.F.R. § 1.136(a) (two-month), along with requisite fees. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14/646,554	Filing Date	2015-05-22	Docket Number (if applicable)	15-686-WO-US	Art Unit	2438
First Named Inventor	Frank Muller			Examiner Name	Vu, Phy Anh Tran		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☒ Other After Final Response filed April 30, 2018

☐ Enclosed

☐ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132490

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2018-05-24
Name	David A. Grabelsky	Registration Number	59280

This collection of information is required by 37 CFR 1.114. 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 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.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1,400
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

May 24, 2018 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $600 paid	1253	1	800	800
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	1900	1900
		Total in USD ($)		**2700**

Electronic Acknowledgement Receipt

EFS ID:	32713296
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	24-MAY-2018
Filing Date:	21-MAY-2015
Time Stamp:	11:33:29
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2700
RAM confirmation Number	052418INTEFSW11342000
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	15-686-WO-US_Request_for_Continued_Examination_form_29Nov17_FOA.pdf	697833 c7d76fcc8ac731b239576858a102af0f2c88f56b	no	3
Warnings:					
Information:					
2	Extension of Time	15-686-WO-US_Petition_for_three-month_Extension_of_Time.pdf	188322 96e5ac9adbe8bab66135988c35b7356b3330299e	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32724 e80b3cda68b09fd8ed4a22c1799a512f221265c5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	918879		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 10/29/2018

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
VU, PHY ANH TRAN	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
10/29/2018	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 05/24/2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-13 and 16- is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-13 and 16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 05/21/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

1.☑ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☑ Interview Summary (PTO-413) Paper No(s)/Mail Date 10/23/2018.

4) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 05/24/2018 has been entered.

Notice of Pre-AIA or AIA Status

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

Response to Arguments

Applicant's arguments filed 04/30/2018 have been fully considered but they are not persuasive.

Regarding claims 1 & 16, on pages 8-11, Applicant seems to argue that due to the newly added limitations, Bu no longer anticipates claims 1 and 16.

In response, Examiner respectfully disagrees, and submits that due to the newly added limitations, a different interpretation of Bu is used, but Bu still anticipates all the limitations of claims 1 & 16 as detailed in the rejections below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7-10, 12-13 and 16 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu).

Regarding claim 1, Bu discloses a system comprising:

a telecommunications network comprising a core network *(at least figures 2, 4-5, core network)*; and

a hardware base station configured within the telecommunications network *(figures 5-6, [0023][0029][0037][0040], base station)*, wherein the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network *([0023]-[0026], base station)*;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive signals from the mobile telecommunications device by way of the base station, and further to process the signals into data streams, internal to the telecommunications network *([0023]-[0026][0045]-[0047][0049]-[0053], signals from mobile/user are obtained and processed into data packets with the network)*,

and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network *([0023]-[0027], messages exchange between Radio Network Controller (RNC) and components/devices in core network correspond to 'data of a first type' and cause signal cost to data ratio to increase)*, the data of the first type being a predetermined type representing an interaction between network devices in the core network *(figures 2 & 4,[0023]-[0027][0038]-[0040][0045]-[0047], messages exchanged between components/devices in the core network for the purposes of authentication and connection)*,

wherein each event of the first type is an occurrence in the data streams of data of the first type *(figures 2 & 4, [0023]-[0027][0038]-[0040][0045]-[0047][0056]-[0057], data packets with signaling cost to data ratio exceed threshold is flagged correspond to an occurrence*),

wherein the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type, wherein the occurrence indicates an incidence of the event of the first type and is arranged to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network *([0049]-[0050][0067]-[0057], data packets which have been flagged are monitored, and if a sufficient number of packets have been flagged, traffic will be blocked)*.

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence of data of the first type by counting a number of occurrences data of the first type is detected in

the data streams when the occurrence exceeds a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of packets have been flagged as suspicious, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the number of occurrences of the data of the first type in the data streams when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval *([0057], data packets that have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is configured to detect when the occurrence in the data stream of the data of a first type exceeds a predetermined rate *(table 2; [0054]-[0057], packets are tracked for predetermined threshold)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrence exceeds the level indicating acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates attachment of the mobile to telecommunications device to the telecommunications network *([0056][0060], data packets with ratio that exceed threshold indicates possible attack from the mobile to the network).*

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates setting up of a bearer by the mobile telecommunications device *([0023]-[0027], setting up RAB).*

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicate handover of the mobile telecommunications device *([0007][0023][0027], handoff).*

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrence in the data streams of the data of the first type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network *([0021][0056]-[0057], Serving Gateway Support Node (SGSN)).*

Regarding claim 13, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is further configured to identify at least one additional mobile telecommunications device,

to receive signals from the at least one additional device and to process these signals into additional data streams *([0045]- [0047][0049]-[0053], signals from another mobile/user is obtained and are processed into packets)*,

to monitor an occurrence in the additional data streams of the data of the first type and to register when the occurrence exceeds a level indicating acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if a sufficient number of packets have been flagged exceeds a certain threshold, signals as malicious)*,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Claim 16 is rejected for the same rationale as claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 6 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network includes a counter and a timer *(table 2, Flag ++, and timer)*, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs *(table 2, [0057] data packets which have been flagged are counted)*.

Bu does not explicitly disclose increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

However, as another option for determining if the data packets are part of an attack, Bu also discloses a timer which times the suspicious behavior of traffic from a user, if the behaviour continues within a predetermined time interval T as measured by the timer, then the future traffic from the user will be blocked *(table 2; [0050]-[0057], packets are tracked and counted for a predetermined period of time)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine the timer and the counter as discloses by Bu to provide another way of determining suspicious data packets from users.

Claim 6 is rejected for the same rationale as claim 4 above.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin.)

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0007][0023][0027][0037]-[0039], handoff to different BS)*.

Bu does not disclose monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH TRAN VU whose telephone number is (571)270-7317. The examiner can normally be reached on Monday-Friday 7 am-1 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an

interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571) 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH T VU/
Examiner, Art Unit 2438

Applicant-Initiated Interview Summary	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA Status No

All participants (applicant, applicants representative, PTO personnel):

(1) PHY ANH TRAN. VU.

(2) David Pearson.

(3) David Grabelsky (Applicant's representative).

(4) Daphne Creusen (Applicant's representative).

Date of Interview: 23 October 2018.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☑102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Bu et al. (US 2006/0230450 A1).

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

After a series of Examiner initiated interviews, Applicant's representative, Mr. Grabelsky requested to have another interview that includes a primary examiner. So, primary examiner David Pearson was joined. During the interview, claim 1 was analyzed, and all parties agreed that the claimd language needs to be further amended to distinguish over the cited art, Bu. Suggestions were given to the Applicant's representative to amend the claims..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/PHY ANH T VU/ Examiner, Art Unit 2438	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiners responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicants correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,-
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicants record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiners version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, Interview Record OK on the paper recording the substance of the interview along with the date and the examiners initials.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016	06/23/2017	11/22/2017	10/26/2018				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	✓				
	6	✓	✓	✓	✓	✓				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	-	-	-				
	15	✓	✓	-	-	-				
	16		✓	✓	✓	✓				

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L 63/14	5/2/2016; 6/23/2017	PVU
H04L 63/1425	5/2/2016; 6/23/2017	PVU

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016; 12/09/2016; 6/23/2017; 11/22/2017; 10/26/2018	PVU
Consulted with WG SPE and QAS regarding 101 issues	06/23/2017	PVU

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/PHY ANH T VU/ Examiner, Art Unit 2438	

ERICSSON EXHIBIT 1005, Page 521

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		H04l63/14.cpc. and (excessive near5 (request occurrence traffic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
		"20060230450".pn. and nas	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:23
		(monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:33
L2	7	g06f12/14.cpc. and (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:35
L3	1734	(detect$4 defend$4) with (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:38
L4	28	(detect$4 defend$4) with (signal$4 near3 attack$4) same (3g near10 wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:39
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23

S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28

S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:32
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16
S37	3	"20100064341".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:11
S38	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
S39	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13
S40	1342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S41	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14

S42	1121	(monitor$4 with (network with traffic) with event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S43	30	(monitor$4 with (network with traffic) with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S44	268	monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
S45	155	S44 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 11:54
S46	169	(network with indicat$4 near5 event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 12:55
S47	106	S46 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 12:55
S48	2	"20060230450".pn. and network	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:44
S49	1	"20060230450".pn. and bs	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:52
S50	1	"20060230450".pn. and pdsn	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:26
S51	2	"20150304345".pn. and (data near3 first near3 type)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:53
S52	13	"9684898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S53	2	"9684898".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S54	4	"9633208".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 18:00
S55	1	"20150304345".pn. and bearer	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:29
S56	0	"20060230450".pn. and handover	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:37
S57	0	"20060230450".pn. and hand$over	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2017/06/23 09:38

			EPO; DERWENT; IBM_TDB			
S58	1	"20060230450".pn. and hand$off	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S59	1	H04I63/14.cpc. and (mobile and (excessive near5 occurrence))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:33
S60	1	H04I63/14.cpc. and (excessive near5 occurrence)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:34
S61	11	H04I63/14.cpc. and (excessive near5 (request occurrence traffic))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
S62	92	H04I63/14.cpc. and (excessive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:39
S63	48	S62 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:39
S64	237	H04I63/1425.cpc. and (mobile and excessive and (malicious attack suspicious))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:45
S65	71	S64 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:46
S66	461	(telecommunication with (exceed$4) near5 threshold)	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S67	2	(telecommunication with (exceed$4) near5 threshold) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S68	0	(telecommunication with (exceed$4) near5 threshold) same behavior	US-PGPUB; USPAT	OR	ON	2017/11/22 07:12
S69	0	(monitor$4 with data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S70	0	(monitor$4 same data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S71	64	(monitor$4 with abnormal) with data near5 streams	US-PGPUB; USPAT	OR	ON	2017/11/22 07:14
S72	19559	monitor$4 with data near5 streams	US-PGPUB; USPAT	OR	ON	2018/05/09 17:15
S73	62	(monitor$4 with streams) same (data near5 abnormal$3)	US-PGPUB; USPAT	OR	ON	2018/05/09 17:20

EAST Search History (Interference)

< This search history is empty>

10/26/2018 12:42:59 PM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 4961

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/646,554	05/21/2015 RULE	726	2438	15-686-WO-US

APPLICANTS

KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

INVENTORS

Frank Muller, Delft, NETHERLANDS;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/EP2013/074440 11/22/2013

**** FOREIGN APPLICATIONS ***************************

EUROPEAN PATENT OFFICE (EPO) 12193884.9 11/22/2012

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

07/07/2015

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/PHY ANH TRAN VU/ Examiner's Signature	☐ Initials	NETHERLANDS	3	15	2

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

System to Detect Behaviour in a Telecommunications Network

FILING FEE RECEIVED		
1480	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

March 29, 2019 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
			Total in USD ($)	**600**

Electronic Acknowledgement Receipt

EFS ID:	35571086
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	29-MAR-2019
Filing Date:	21-MAY-2015
Time Stamp:	12:31:38
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	032919INTEFSW12321100
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	15-686-WO-US_Response_29Oct18_OA.pdf	184347 e2a072b94df79ae8c5bf9a2f0b91dcda67186980	no	21
Warnings:					
Information:					
2	Extension of Time	15-686-WO-US_Petition_for_two-month_Extension_of_Time.pdf	188331 096f646faa78f4207a166e1df8d9700494b36b27	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30713 9393c84e92ec5aba357d52ad2739ff953562f619	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	403391		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO OFFICE ACTION MAILED OCTOBER 29, 2018

In response to the Office Action mailed October 29, 2018, Applicant submits the following amendments and remarks. In addition, a Petition for Extension of Time under 37 C.F.R. § 1.136(a) (two-month) is included, along with requisite fees. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system comprising:

a telecommunications network comprising a core network; and

a hardware base station configured within the telecommunications network, wherein

the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive ~~signals~~ a request from the mobile telecommunications device by way of the base station, and further to process the ~~signals~~ request into data streams internal to the telecommunications network, wherein the request is associated with an event of the first type within the telecommunications network,

~~and wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network, the data of the first type being a predetermined type representing an interaction between network devices in the core network,~~

~~wherein each event of the first type is an occurrence in the data streams of data of the first type,~~

and wherein the telecommunications network is arranged to monitor, ~~the occurrence~~ in the data streams internal to the telecommunications network, occurrences of ~~the~~ data of ~~the~~ a first type, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type, and represents an interaction between network devices in the core telecommunications network, ~~wherein the occurrence indicates an incidence of the event of the first type~~

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

and [[is]] wherein the telecommunications network is further arranged to register when the ~~occurrence exceeds~~ occurrences of the data of the first type exceed a level ~~indicating~~ for acceptable behaviour of the mobile telecommunications device in the telecommunications network.

2. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to monitor the ~~occurrence~~ occurrences of data of the first type by counting that a number of occurrences data of the first type is detected in the data streams when the ~~occurrence exceeds~~ occurrences exceed a predetermined temporal rate, and ~~further~~ wherein the telecommunications network is further arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Previously presented) The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences of the data of the first type in the data streams when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Previously presented) The system according to claim 3, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

5. (Currently amended) The system according to claim 1, wherein the telecommunications network is further configured to detect when the ~~occurrence~~ occurrences in the data stream of the data of a first type exceeds a predetermined rate.

6. (Previously presented) The system according to claim 5, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type and further to start the timer and wherein the telecommunications network is further arranged to calculate a rate as a ratio of counted detection of occurrence of data of the first type to time as measured by the timer.

7. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to register when the ~~occurrence exceeds~~ occurrences of the data of the first type exceed the level ~~indicating~~ for acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Previously presented) The system according to claim 1, wherein the data of the first type indicates attachment of the mobile telecommunications device to the telecommunications network.

9. (Previously presented) The system according to claim 1, wherein the data of the first type indicates setting up of a bearer by the mobile telecommunications device.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

10. (Previously presented) The system according to claim 1, wherein the data of the first type indicate handover of the mobile telecommunications device.

11. (Previously presented) The system according to claim 10, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to monitor the ~~occurrence~~ occurrences in the data streams of the data of the first type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

13. (Currently amended) The system according to claim 1, wherein the telecommunications network is further configured to:

identify at least one additional mobile telecommunications device,

[[to]] receive signals from the at least one additional device and to process these signals into additional data streams,

[[to]] monitor ~~an occurrence~~ occurrences in the additional data streams of the data of the first type and to register when the ~~occurrence exceeds~~ occurrences exceed a level ~~indicating~~ for

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

acceptable behaviour of the mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Canceled)

15. (Canceled)

16. (Currently amended) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network comprising a core network, the telecommunications network including a base station, the method comprising:

at the base station, receiving radio transmissions from the mobile telecommunications device, the received radio transmissions including a request, wherein the request is associated with an event of the first type within the telecommunications network;

at the base station, ~~converting the received radio transmissions into signals, and~~ sending the ~~signals~~ request into the telecommunications network;

in the telecommunications network, identifying the mobile telecommunications device;

in the telecommunications network, receiving the ~~signals~~ request from the mobile telecommunications device by way of the base station, and processing the ~~signals~~ request into data streams internal to the telecommunications network~~, wherein the data streams include data of a first type arranged to cause an event of a first type within the telecommunications network,~~

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

~~the data of the first type being a predetermined type representing an interaction between network devices in the core network, wherein each event of the first type is an occurrence in the data streams of data of the first type~~; ~~and~~

in the telecommunications network, monitoring, ~~for an occurrence~~ in the data streams internal to the telecommunications network, occurrences of ~~the~~ data of ~~the~~ a first type, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type, and represents an interaction between network devices in the core telecommunications network ~~wherein the occurrence indicates an instance of the event of the first type~~; and

registering when the ~~occurrence exceeds~~ occurrences of the data of the first type exceed a level ~~indicating~~ for acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Office Action

In the Office Action mailed October 29, 2018 ("Current Office Action," hereinafter), the Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu, and rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-13 and 16, of which claims 1 and 16 are independent, and the remaining claims are dependent. Applicant has amended various other claims as follows.

Applicant has amended claim 1 to describe that the recited "telecommunications network" is: "configured to identify at least one mobile telecommunications device and to receive a request from the mobile telecommunications device by way of the base station, and further to process the request into data streams internal to the telecommunications network, wherein the request is associated with an event of the first type within the telecommunications network"; "arranged to monitor, in the data streams internal to the telecommunications network, occurrences of data of a first type, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type, and represents an interaction between network devices in the core telecommunications network"; and "further arranged to register when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network." This is a largely clarifying amendment, associating a "request" with "an event of the first type," emphasizing that the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

monitoring action is performed "in the data streams internal to the telecommunications network," and emphasizing that acceptable behaviour is evaluated in consideration only of occurrences of "data of the first type." Support for this amendment can be found generally throughout the original application, and specifically at least at page 2, lines 18-20; page 3, lines 3-17 and lines 32-34; page 5, lines 5-11; page 7, lines 9-11, line 17 and line 25; page 8, lines 1-6; and Figure 1, for example.

Applicant has amended claim 16 in a manner similar to that of claim 1. Support for this amendment is generally the same as for the amendment to claim 1.

Applicant has amended each of claims 2, 5, 7, 12, and 13 to ensure consistency of antecedent basis with base claim 1.

No new matter has been introduced by way of any of the above amendments.

3. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. Applicant submits that Bu fails to teach each and every element set forth in any of claims 1-3, 5, 7-10, 12-13, or 16, and that these claims are allowable. Applicant first discusses claim 1, then subsequently addresses claims 2-3, 5, 7-10, 12-13, and 16.

It is useful to first summarize at a high level the proposed approach to detecting and defending against signaling attacks taught by Bu, and to contrast, also at a high level, claim 1 to the proposed approach of Bu. Further detailed arguments then follow the summary.

Bu is concerned with a type of attack in which an attacker causes unwitting mobile stations to become "accomplices" in a signaling attack. The attacker does not itself actually send any signaling into the network. Rather, the attacker repeatedly sends just a single data packet to

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

an unwitting mobile station. Each sent packet may result in a page to the unwitting mobile station, causing the unwitting mobile station to then initiate a cascade of signaling messages for setting up a wireless connection. The signaling messages appear as normal and legitimate overhead to the network, and so are not recognized by the network as an attack.

The attacker knows that a mobile station must first establish a wireless connection to the network in order to send or receive data, and that an existing wireless connection will be released after a prescribed period of inactivity of the mobile station (e.g., no sending or receiving of data). The attacker also knows that it takes a large number of signaling messages for a mobile station to establish a wireless connection to the network (if it doesn't already have one), and only a slightly smaller number of signaling messages to release its wireless connection after the prescribed period of inactivity.

With this knowledge, the attacker's "game" is to send a single data packet to an unwitting mobile station. The single data packet itself is *not a signaling message*. But it triggers the large number of signaling messages required to establish a wireless connection to the network for the unwitting mobile station. The attacker then waits for the prescribed amount of time without sending any more data packets to the specific unwitting mobile station (though the attacker may target more than one unwitting mobile station, sending one packet at a time to each of them, for example), such that an inactivity timer expires and the unwitting mobile station's wireless connection is released. This triggers all the signaling messages associated with releasing the connection. The sum total of the signaling messages – for establishing and releasing the connection – are all transmitted in the service of just one data packet sent by the attacker. Since the single data packet itself is a negligible contribution to network traffic, it goes undetected as

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

an attack. And since the signaling messages for establishing and releasing the wireless connection are legitimate, the network does not detect them as an attack either.

By carrying out this sending-and-waiting repeatedly and to multiple unwitting mobile stations, the attacker causes many useless cascades of signaling messages without ever transmitting more than small, unsuspicious numbers of data packets into the network. The harm done to the network is the large number of signaling messages that consume network resources, but that don't actually support any real use to any of the unwitting mobile stations. Bu's purported solution is to introduce a metric of estimated activity that supposedly detects when this sort of low-level-data-but-high-level-signaling attack is being attempted by a would-be attacker.

Bu's disclosed metric is a "signaling cost to data ratio" that is tracked for each pair of sender and mobile station, where the sender might be an attacker. It is sufficient to consider just one sender and one mobile station to understand how Bu's proposed technique is supposed work. By way of background, Bu catalogs the signaling messages for establishing a wireless connection (a "radio access bearer" or "RAB" in Bu), and similarly catalogs the signaling messages for releasing a wireless connection. The technique depends on knowledge of signaling protocols for this purpose, *but does not entail ever actually monitoring or detecting signaling messages in the network*.

If a packet arrives for a mobile station, the signaling cost for that mobile station is the number of signaling messages required for re-establishing the connection – if the idle timer for that mobile station had previously expired – plus the number of signaling messages required for the prior release of the previous connection. *This cost is estimated without ever actually monitoring or detecting any signaling messages*. Rather, the cost estimate is inferred from (a) an assumed absence of an established connection if the data packet arrives after expiration of the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

idle timer (as also inferred from the packet's arrival time relative to the last previous RAB setup), and (b) knowledge of the signaling protocols (i.e., the number of signaling messages required to establish/release a connection). By correlating the signaling costs for the mobile station with the actual amount of data sent (e.g., numbers and sizes of packets), Bu teaches that a signaling cost to data ratio can be estimated for the mobile station. If the estimated cost exceeds a threshold – i.e., if there is voluminous signaling but very little actual data received using the established wireless connections – then an attack is suspected and the sender is blocked.

Two key aspects of the teachings Bu are: (1) there is no actual monitoring or detecting of transmitted signaling messages in the network, but just an inferred estimate based on knowledge of signaling protocols, and (2) to the extent that signaling messages are implicitly "tracked" by inference, *all* of the known signaling messages associated with connection establishment/release must be counted in order to estimate the signaling costs. The estimated signaling cost cannot be inferred, for example, by counting just one or a subset of the total number of signaling messages specified by the protocol.

Claim 1 is directed to a system in which unacceptable behavior of a mobile telecommunications device in a telecommunications network may be detected. In contrast to Bu, the operations described, *inter alia*, in claim 1 involve *actually monitoring* data streams that are internal to a telecommunications network for occurrences of a particular type of data that is known to cause a particular type of event in the telecommunications network, and is also known to represent an interaction between network devices in the core network. Further, the particular type of event is one that is associated with a request sent by the mobile telecommunications device. In addition to *actual monitoring*, the approach described, *inter alia*, in claim 1 monitors

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

for occurrences of *just the particular type of data*, unlike Bu, which tracks (by inference) *all* signaling messages associated with connection establishment/release.

With the above summary as context, Applicant now demonstrates specifically how and why Bu fails to anticipate claim 1.

Bu does not teach: "wherein the telecommunications network is arranged to monitor, in the data streams internal to the telecommunications network, occurrences of data of a first type, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type, and represents an interaction between network devices in the core telecommunications network"

In the Current Office Action, the Examiner equated "messages exchange between Radio Network Controller (RNC) and components/devices in core network" disclosed (according to the Examiner) in Bu with "data of a first type" recited, *inter alia*, in claim 1. The Examiner further equated causing "signal to cost ratio to increase" also disclosed (according to the Examiner) in Bu with causing "an event of the first type" also recited, *inter alia*, in claim 1. And still further, the Examiner asserted that flagged "data packets with signaling cost to data ratio" exceeding a threshold corresponds to "an occurrence in the data streams of data of the first type." (Current Office Action, page 4.). Applicant respectfully submits that the Examiner's analysis of Bu in connection with at least the cited elements of claim 1 is factually incorrect and fundamentally, technically flawed, and that the rejection is not supported by what Bu actually teaches.

Specifically, in order to support the rejection based on the Examiner's assertion that "messages exchange[d] between Radio Network Controller (RNC) and components/devices in core network correspond to 'data of a first type'," Bu would necessarily *have to* teach or disclose monitoring "*in the data streams* internal to the telecommunications network, occurrences of" "messages exchange[d] between Radio Network Controller (RNC) and components/devices in core network." Applicant submits that Bu clearly and unambiguously teaches no such thing. Rather, Bu teaches a method that purports to *estimate* a signaling cost by effectively *inferring* the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

occurrence of the types of messages cited by the Examiner, but without ever actually *monitoring* any communications for the presence of those messages.

In paragraphs [0025]-[0028] and related Figure 2, Bu catalogs various "Radio Resource Control (RRC)" messages associated with different phases and/or different scenarios of establishment and release of radio channels associated with a "radio access bearer (RAB)" for mobile device operation in a UMTS network. For example, Bu teaches that: "a total of 24 messages to establish a single RAB with the RNC"; a soft handoff "requires a total of 11 messages exchanged at the RNC"; and

> If there is no data exchanged between a mobile and its core network, the mobile is placed in a suspended state. In such a state, air link resources are released and assigned to other active mobiles, which requires 4 messages (2 with its core network and 2 with a base station). However, the context is still maintained at the RNC, and the mobile retains its IP address obtained during RRC/RAB establishment. A mobile can be reactivated (2 messages exchanged with RNC) using a packet call context resumption message (additional 2 messages with its core network) as long as an idle timeout period of 5 seconds has not occurred.

These messages correspond to the "signaling cost" for the establishment/release (among other) operations involved in RRC in a UMTS network, as taught by Bu.

In paragraphs [0038]-[0042] and related Figure 4, Bu similarly catalogs various "Radio Resource Control (RRC)" messages associated with different phases and/or different scenarios of establishment and release of radio channels associated with a "fundamental channel (FCH)" for mobile device operation in a 3G1x network. Further examples cited in Bu of the message counts corresponding to "signaling cost" in a 3G1x network are omitted here for the sake of brevity. But Bu's intent in tallying up the message counts is the same in either case: to provide a basis for estimating signaling cost *without ever actually monitoring for the occurrence of any of these messages*. Indeed, the term "monitor" does not appear even once in Bu. And the conceivably similar term "detect" (or the like) is used only in connection with detection of signaling attacks

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

or "signaling cost" (e.g., paragraphs [0048] and [0049]), but never in connection with detection (or monitoring) signaling messages.

In paragraph [0045], it is clear why Bu teaches estimating signaling costs. Namely, there is no other practical way, according to Bu, to directly determine signaling cost:

> To prevent and defend against an attack, the present inventors recognized that *knowledge of so-called wireless states, in particular the signaling cost(s) as traffic traverses through a wireless network was needed.* … Ideally, an exact signaling cost can be obtained by querying wireless elements, such as an RNC and base station, when these elements provide an interface for such queries. *However, current 3G wireless networks do not have such an interface*, thus requiring modifications in order to support such queries. Changing an existing infrastructure, however, *is not a viable solution* given the amount of investment already expended by network owners/operators. (Emphasis added.)

Bu's purported solution to the identified problem – the lack of interfaces for querying signaling costs – is estimation based on prior knowledge of the cataloged message counts. As Bu states in paragraph [0046], "[t]he present inventions provide for methods and devices for detecting an attack using the so *estimated signaling cost*" (emphasis added).

As Bu then teaches in paragraph [0047], "the signaling cost is estimated from traffic arrival patterns" and "*requires knowledge of the signaling protocols inside wireless elements*" (emphasis added). Table 1 illustrates the principle behind Bu's estimation approach in a UMTS network. The basic idea is that if a data packet (not signaling data) arrives for a given user more than a threshold time after the last previous packet, where the threshold time corresponds to an "IdleTimeout," then according to the known signaling protocols, any previously existing RAB will have to have been released, and a new one will have to be established in order to transmit the arrived packet. Thus, the signaling cost associated with the arrived packet may be estimated as the cost of the previous RAB release plus that of re-establishing a new RAB. Both of these costs are added to whatever prior costs exist. And the costs for each of these operations – release and re-establishment – are determined according to the cataloged signal message counts. Bu

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

teaches that a similar estimation technique may be used for other known protocol operations. The results of these techniques are signaling cost estimates that *do not rely on or entail ever monitoring* "in the data streams internal to the telecommunications network, occurrences of" signaling messages.

Thus, the only possible direct determination of the occurrence of signaling messages in Bu is one that Bu teaches is not available, and even if it was, it would not amount to monitoring occurrences of signaling messages "in the data streams internal to the telecommunications network," but rather to "querying wireless elements" of the network for *signaling cost*.

The remaining aspects of the methods taught by Bu involve estimating a signaling cost to data ratio for data packets received for a given user from a given sender. This estimate is used as a purported way to distinguish legitimate signaling costs associated with data packets from those which appear to be part of a signaling attack. The basic idea, illustrated in Table 2 and paragraphs [0054]-[0058] in Bu, is to compare the signaling cost to data ratio to a threshold cost value for the given user, and to increment a flag counter for packets from the given sender to the given receiver if the threshold is exceeded. Then, if the flag counter exceeds another counter threshold, or if the suspicious behavior lasts for too long, the given sender is suspected of attempting to carry out an attack, and future traffic from the given sender is blocked.

Neither the estimation of signaling cost to data ratio, nor its application to determining if an attack is underway, involves monitoring signaling messages "in the data streams internal to the telecommunications network." More particularly, estimation of signaling cost to data ratio relies on estimation of the signaling cost, which, as already described, is estimated based on prior knowledge of the signaling protocols, but *not* on monitoring signaling messages.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Even beyond the absence in Bu of any teaching of monitoring signaling messages "in the data streams internal to the telecommunications network," the Examiner's assertion that a flagged data packet "with signaling cost to data ratio" exceeding a threshold corresponds to "an occurrence in the data streams of data of the first type" is also contradicted by what Bu actually teaches. Specifically, Bu teaches that for each packet, an *estimated* signaling cost is used to determine an *estimated* signaling cost to data ratio, which is then compared with a threshold. Only when the cost threshold is exceeded is a packet flagged as such. But not every packet will necessarily be flagged, otherwise there would be no need or purpose to comparing the estimated signaling cost to data ratio to the threshold (step 2 in Table 2). Thus, following the Examiner's reasoning, every *un*flagged packet would *also* correspond to "an occurrence in the data streams of data of the first type." As such, there would be no distinction between flagged and unflagged packets, or to whether or not an event of the first type has occurred.

Bu does not teach: "wherein the telecommunications network is further arranged to register when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network"

As described above, Bu teaches determining when the number packets having an estimated signaling cost to data ratio greater than a cost threshold exceeds a count threshold, and taking protective action when it does. Making this estimate requires tallying *all* the signaling messages associated with establishing and releasing a RAB for each data transfer, whether the data transfer involves one packet or many. Thus, even if it were possible to obtain "an exact signaling cost" by "querying wireless elements" via an "interface" that Bu teaches *does not exist*, such an "exact cost" would *necessarily* have to count all the signaling messages specified by the signaling protocols. The signaling cost could not be obtained, for example, by only counting some of the messages Bu discloses are needed to establish a radio resource control (RRC) connection, or only some of the messages Bu discloses are needed for RAB assignment. Bu's

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

estimation requires that all of the 24 messages Bu discloses are needed for RAB establishment must be counted, without distinction. And this is the case whether an "exact" signaling cost that Bu teaches is not available is considered, or if an estimated signaling cost is inferred using Bu's disclosed method that does not ever actually monitor for signaling messages.

In contrast, claim 1 recites, *inter alia*, registering "when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network." Thus, "data of the first type" are distinguished from other types of data that may occur in the monitoring of "the data streams internal to the telecommunications network." If only "data of the first type" were considered in Bu's technique, the whole basis for estimating signaling cost would be undermined. On this basis alone, Applicant submits that Bu does not teach "wherein the telecommunications network is further arranged to register when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network."

What about the Examiner's interpretation of "messages exchange between Radio Network Controller (RNC) and components/devices in core network" in Bu as "data of a first type"? Applicant submits that this interpretation is logically inconsistent with Bu's teachings.

Specifically, Bu's estimate of signaling cost requires that all signaling messages be counted, including those between the mobile station and the base station. Thus, by considering only "messages exchange between Radio Network Controller (RNC) and components/devices in core network," the Examiner would impose a contradictory teaching on Bu. That is, the Examiner's interpretation would cause Bu to omit some of the signaling messages that are required by Bu to be counted toward the estimate of signaling cost.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Further, in paragraphs [0050]-[0058], Bu teaches determining "user profiles" in order to supposedly distinguish instances of apparent high signaling cost to data ratios that are legitimate from those that are likely attacks. That is, Bu teaches that while detected high signaling cost to data ratio transfers may be suspected as attacks, they are not necessarily so. Bu teaches using user profiles to describe statistical traffic patterns of individual users, applications, and servers (e.g., that may act as senders of data packets), which may then be used to set thresholds for signaling cost to data ratios for given users on a per-sender basis. This means that for a given user (mobile station), some senders of high signaling cost to data ratio data transfers will be blocked as attackers, while some others will not. Thus, not all excessive high signaling cost to data ratio signaling involving a given user would necessarily be flagged as unacceptable behaviour. So Bu does not even "register" all instances of high signaling cost to data ratio transfers.

Finally, the "signaling cost to data ratio" taught by Bu is an estimated quantity that is *derived* from both inferred numbers of signaling messages and measured amounts of data transferred. As such, even adopting the Examiner's interpretation of "messages exchange between Radio Network Controller (RNC) and components/devices in core network" in Bu as "data of a first type" for the sake of argument, a high value of "signaling cost to data ratio" does not necessarily correspond to "occurrences of the data of the first type" that would "exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network." That is, signaling cost to data *ratio* depends on values of a numerator and denominator. Thus, its value alone does not determine signaling cost.

For at least the reasons above, Applicant submits that claim 1 distinguishes over Bu, and that claim 1 is therefore allowable.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Claim 16 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 16 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 2-3, 5, 7-10, and 12-13 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claims 2-3, 5, 7-10, and 12-13 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with any of claims 2-3, 5, 7-10, or 12-13.

4. Response to Rejections under 35 U.S.C. § 103(a)

a. Claims 4 and 6

The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu. Each of claims 4 and 6 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that each of claims 4 and 6 is allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with either of claims 4 or 6.

b. Claim 11

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

5. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: March 29, 2019

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	03/29/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/PEGGY S YARBOROUGH/
*** 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.	

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 07/05/2019

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
VU, PHY ANH TRAN	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
07/05/2019	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA (FITF) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 03/29/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-13 and 16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-13 and 16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 05/21/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

1.☑ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Amendment filed 03/29/2019.

Notice of Pre-AIA or AIA Status

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

Response to Arguments

Applicant's arguments with respect to claims 1, 16 and all dependent claims have been considered but are moot in view of the new interpretation of the reference.

In addition, to clarify the Examiner's position, Applicant's arguments are addressed below:

Regarding claim 1, on pages 9-20, Applicant argues that Bu fails to teach:

1) **"wherein the telecommunication network is arranged to monitor, in the data streams internal to the telecommunication network, occurrences of data of a first type, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type, and represents an interaction between network devices in the core network telecommunications network"**

2) **"where in telecommunications network is further arranged to register when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network"**

In response, Examiner respectfully disagrees and submits that:

1) As discloses in Bu, in order to enable data transmission from/to a mobile, a few steps will need to be carried out between network devices in the core network for the purposes of at least authentication and assignment of IP address ([0024] [0026] [0039]). Bu also discloses that data packets transmitted via the network are monitored, as all the data packets passing through the network will be compared to a threshold, but only data packets that exceeding the threshold ***(occurrences of data of a first type)*** ([0056]) will be marked/flagged ***(cause the event of the first type)*** ([0056]).

2) Bu further discloses, data packets that are flagged for a particular sender will be monitored, and when a sufficient number of data packets from the particular sender exceeds a threshold have been flagged, then the sender will be listed/registered, and subsequent data packets from the sender will be blocked ([0057]).

As such, contrasting to the Applicant's arguments, Bu discloses all the limitations argue above.

Regarding claim 16 and all other dependent claims, please see respond to argument for claim 1 above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7-10, 12-13 and 16 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 1, Bu discloses a system comprising:

a telecommunications network *(figure s 1 & 5)* comprising

a core network *(figures 2 & 4, core network)*; and

a hardware base station configured within the telecommunications network *(figures 1, 5 & 6, base station)*, wherein the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for receiving the signals into the telecommunications network *([0023]-[0026], base station)*;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive a request from the mobile telecommunications device by way of the base station, and further to process the request into data streams internal to the telecommunications network *([0023]-[0026][0039][0045]-[0047][0049]-[0053], a subsequent request to transmit packet is received from the mobile)*, wherein the request is associated with an event of the first type within the telecommunications network *([0053]-[0056], i.e.: the request to transmit subsequent packet is associated with user whose packets are flagged)*, and

wherein the telecommunications network is arranged to monitor, in the data streams internal to the telecommunications network, occurrences of data of a first type *(table 2, [0056]-[0057], packets that have are determined to exceed threshold are monitored)*, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type *([0056]-[0057], data packets exceeding threshold are*

flagged), and represents an interaction between network devices in the core telecommunications network *([0053]-[0056], transmission of packets between receiver and user in the core network)*,

and wherein the telecommunications network is further arranged to register when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network *([0057], packets that have been flagged are monitored, and if a sufficient number of packets have been flagged, then traffic will be blocked.)*

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrences of data of the first type by counting that a number of occurrences data of the first type is detected in the data streams when the occurrences exceed a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of packets have been flagged as suspicious, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the number of occurrences of the data of the first type in the data streams when a time between a detected occurrence and the previously detected occurrence is within a predetermined

time interval *([0057], data packets that have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is further configured to detect when the occurrences in the data stream of the data of a first type exceeds a predetermined rate *(table 2; [0054]-[0057], packets are tracked for predetermined threshold)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrences of data of the first type exceed the level for acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates attachment of the mobile to telecommunications device to the telecommunications network *([0056][0060], data packets with ratio that exceed threshold indicates possible attack from the mobile to the network)*.

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicates setting up of a bearer by the mobile telecommunications device *([0023]-[0027], setting up RAB)*.

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the data of the first type indicate handover of the mobile telecommunications device *([0007][0023][0027], handoff)*.

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrences in the data streams of the data of the first type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network *([0021][0056]-[0057], Serving Gateway Support Node (SGSN))*.

Regarding claim 13, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is further configured to identify at least one additional mobile telecommunications device,

receive signals from the at least one additional device and to process these signals into additional data streams *([0045]- [0047][0049]-[0053], signals from another mobile/user is obtained and are processed into packets)*,

monitor occurrences in the additional data streams of the data of the first type and to register when the occurrences exceed a level for acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0057], if a sufficient number of packets have been flagged exceeds a certain threshold, signals as malicious)*,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one

additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Claim 16 is rejected for the same rationale as claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 6 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network includes a counter and a timer *(table 2, Flag ++, and timer)*, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of data of the first type, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of data of the first type occurs *(table 2, [0057] data packets which have been flagged are counted)*.

Bu does not explicitly disclose increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

However, as another option for determining if the data packets are part of an attack, Bu also discloses a timer which times the suspicious behavior of traffic from a user, if the behaviour continues within a predetermined time interval T as measured by the timer, then the future traffic from the user will be blocked *(table 2; [0050]-[0057], packets are tracked and counted for a predetermined period of time)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine the timer and the counter as discloses by Bu to provide another way of determining suspicious data packets from users.

Claim 6 is rejected for the same rationale as claim 4 above.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin.)

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0007][0023][0027][0037]-[0039], handoff to different BS)*.

Bu does not disclose monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a

single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement).*

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH TRAN VU whose telephone number is (571)270-7317. The examiner can normally be reached on Monday-Friday 7 am-1 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571) 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH T VU/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/646,554	Applicant(s)/Patent Under Reexamination Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20120124666-A1	05-2012	Kim; Jeong Hun	H04L63/1458	726/23
*	B	US-20150033322-A1	01-2015	Wang; Wei David	H04L63/1425	726/13
*	C	US-20190028479-A1	01-2019	MORI; Shunsuke	H04L63/101	1/1
*	D	US-20040054925-A1	03-2004	Etheridge, James K.	H04L63/1425	726/22
*	E	US-20040250124-A1	12-2004	Chesla, Avi	G06F21/552	726/13
*	F	US-20060140127-A1	06-2006	Lee; Hee-Jo	H04L43/18	370/241
*	G	US-20100064368-A1	03-2010	Stolfo; Salvatore J	G06F21/564	726/24
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016	06/23/2017	11/22/2017	10/26/2018	07/04/2019			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓			
	4	✓	✓	✓	✓	✓	✓			
	5	✓	✓	✓	✓	✓	✓			
	6	✓	✓	✓	✓	✓	✓			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓			
	11	✓	✓	✓	✓	✓	✓			
	12	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓			
	14	✓	✓	-	-	-	-			
	15	✓	✓	-	-	-	-			
	16		✓	✓	✓	✓	✓			

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L 63/14	5/2/2016; 6/23/2017; 7/4/2019	PVU
H04L 63/1425	5/2/2016; 6/23/2017; 7/4/2019	PVU

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016; 12/09/2016; 6/23/2017; 11/22/2017; 10/26/2018; 7/4/2019	PVU
Consulted with WG SPE and QAS regarding 101 issues	06/23/2017	PVU

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

ERICSSON EXHIBIT 1005, Page 571

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		H04l63/14.cpc. and (excessive near5 (request occurrence traffic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
		"20060230450".pn. and nas	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:23
		(monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	0	H04l63/14.cpc. and (excessive near5 occurrence) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:26
L2	14	H04l63/14.cpc. and (attack$4) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:26
L3	69	H04l63/1425.cpc. and (attack$4) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:33
L4	24	l3 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2019/07/04 12:33
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23
S8	1	(2006/0104752)	US-PGPUB; USPAT;	OR	OFF	2016/05/02

			USOCR; DERWENT; IBM_TDB			09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2016/05/02 11:32

			EPO; DERWENT; IBM_TDB			
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16
S37	3	"20100064341".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:11
S38	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
S39	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13
S40	1342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S41	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S42	1121	(monitor$4 with (network with traffic) with event)	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2017/04/05 11:52

			EPO; DERWENT; IBM_TDB			
S43	30	(monitor$4 with (network with traffic) with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S44	268	monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
S45	155	S44 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 11:54
S46	169	(network with indicat$4 near5 event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 12:55
S47	106	S46 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 12:55
S48	2	"20060230450".pn. and network	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:44
S49	1	"20060230450".pn. and bs	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:52
S50	1	"20060230450".pn. and pdsn	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:26
S51	2	"20150304345".pn. and (data near3 first near3 type)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:53
S52	13	"9684898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S53	2	"9684898".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S54	4	"9633208".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 18:00
S55	1	"20150304345".pn. and bearer	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:29
S56	0	"20060230450".pn. and handover	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:37
S57	0	"20060230450".pn. and hand$over	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38

S58	1	"20060230450".pn. and hand$off	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S59	1	H04l63/14.cpc. and (mobile and (excessive near5 occurrence))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:33
S60	1	H04l63/14.cpc. and (excessive near5 occurrence)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:34
S61	11	H04l63/14.cpc. and (excessive near5 (request occurrence traffic))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
S62	92	H04l63/14.cpc. and (excessive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:39
S63	48	S62 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:39
S64	237	H04l63/1425.cpc. and (mobile and excessive and (malicious attack suspicious))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:45
S65	71	S64 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:46
S66	461	(telecommunication with (exceed$4) near5 threshold)	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S67	2	(telecommunication with (exceed$4) near5 threshold) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S68	0	(telecommunication with (exceed$4) near5 threshold) same behavior	US-PGPUB; USPAT	OR	ON	2017/11/22 07:12
S69	0	(monitor$4 with data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S70	0	(monitor$4 same data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S71	64	(monitor$4 with abnormal) with data near5 streams	US-PGPUB; USPAT	OR	ON	2017/11/22 07:14
S72	19559	monitor$4 with data near5 streams	US-PGPUB; USPAT	OR	ON	2018/05/09 17:15
S73	62	(monitor$4 with streams) same (data near5 abnormal$3)	US-PGPUB; USPAT	OR	ON	2018/05/09 17:20
S74	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:33
S75	7	g06f12/14.cpc. and (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:35
S76	1734	(detect$4 defend$4) with (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2018/10/26 12:38

			EPO; DERWENT; IBM_TDB			
S77	28	(detect$4 defend$4) with (signal$4 near3 attack$4) same (3g near10 wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:39
S78	3	"20060230450"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2019/07/03 08:38

EAST Search History (Interference)

< This search history is empty>

7/ 4/ 2019 12:52:29 PM
C:\ Users\ pvu3\ Documents\ EAST\ Workspaces\ 14646554.wsp

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
15-686-WO-US	14/646,554	May 22, 2015
First Named Inventor:	**Title:**	
Frank Muller	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:

- Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
- The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
  - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
  - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
    - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
    - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/David A. Grabelsky/	December 12, 2019
Name (Print/Typed) David A. Grabelsky	**Practitioner Registration No.** 59,208

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

[✓] * Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1,400
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

December 12, 2019 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
			Total in USD ($)	**1400**

Electronic Acknowledgement Receipt

EFS ID:	38007167
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	12-DEC-2019
Filing Date:	21-MAY-2015
Time Stamp:	10:22:13
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1400
RAM confirmation Number	E2019BBA22450616
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	15-686-WO-US_Response_05Ju19_FOA.pdf	168994 26f9fc15e1cc74336cf1b5242e86a989fbaef72c	no	15
Warnings:					
Information:					
2	After Final Consideration Program Request	15-686-WO-US_AFCP_Request_05Jul19_FOA.pdf	226770 30169bb39cbb4416fb71e501e3b770278f614eee	no	2
Warnings:					
Information:					
3	Extension of Time	15-686-WO-US_Petition_for_three-month_Extension_of_Time.pdf	188329 225924e4384bba5cdb1e7796fe74ad44d3b4d7f2	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30758 3b5e2506b5a8066228367ba621a3699a04f02c3c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	614851		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO FINAL OFFICE ACTION MAILED JULY 5, 2019

In response to the Final Office Action mailed July 5, 2019, Applicant submits the following amendments and remarks. In addition, a request for consideration under the After Final Consideration Pilot 2.0 is included, as well as a Petition for Extension of Time under 37 C.F.R. § 1.136(a) (three-month), along with requisite fees. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system comprising:

a telecommunications network comprising a core network; and

a hardware base station configured within the telecommunications network, wherein

the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for ~~receiving~~ transmitting the signals into the telecommunications network;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive a request from the mobile telecommunications device by way of the base station, and further to process the request into ~~data streams~~ signaling internal to the telecommunications network~~, wherein the request is associated with an event of the first type within the telecommunications network~~,

~~and~~ wherein the telecommunications network is arranged to monitor, in the ~~data streams~~ signaling internal to the telecommunications network, for an occurrence[[s]] of a predetermined data ~~of a first~~ type~~, wherein the data of the first type is a predetermined type of data arranged to cause the event of the first type, and represents an~~ associated with the mobile telecommunications device, and representing an interaction between network devices in the core ~~telecommunications~~ network,

and wherein the telecommunications network is further arranged to register when the occurrence[[s]] ~~of the data of the first type exceed~~ exceeds a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

2. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to monitor for the occurrence[[s]] of predetermined data ~~of the first~~ type by counting that a number of occurrences ~~data of the first~~ of the predetermined data type is detected in the ~~data streams~~ signaling when the occurrences exceed a predetermined temporal rate, and wherein the telecommunications network is further arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Currently amended) The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences of the ~~data of the first~~ predetermined data type in the ~~data streams~~ signaling when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Currently amended) The system according to claim 3, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of ~~data of the first~~ the predetermined data type and further to start the timer and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of ~~data of the first~~ the predetermined data type occurs within the predetermined time interval T as measured by the timer.

5. (Currently amended) The system according to claim 1, wherein the telecommunications network is further configured to detect when the occurrences in the ~~data streams~~ signaling of ~~the data of a first~~ the predetermined data type exceeds a predetermined rate.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

6. (Currently amended) The system according to claim 5, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of ~~data of the first~~ the predetermined data type and further to start the timer and wherein the telecommunications network is further arranged to calculate a rate as a ratio of counted detection of occurrence of ~~data of the first~~ the predetermined data type to time as measured by the timer.

7. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to register when the occurrences of the ~~data of the first~~ predetermined data type exceed the level for acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Currently amended) The system according to claim 1, wherein the ~~data of the first~~ predetermined data type indicates attachment of the mobile telecommunications device to the telecommunications network.

9. (Currently amended) The system according to claim 1, wherein the ~~data of the first~~ predetermined data type indicates setting up of a bearer by the mobile telecommunications device.

10. (Currently amended) The system according to claim 1, wherein the ~~data of the first~~ predetermined data type indicates handover of the mobile telecommunications device.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

11. (Previously presented) The system according to claim 10, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to monitor the occurrences in the ~~data streams~~ signaling of the ~~data of the first~~ predetermined data type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

13. (Currently amended) The system according to claim 1, wherein the telecommunications network is further configured to:

identify at least one additional mobile telecommunications device,

receive signals from the at least one additional device and to process these signals into additional ~~data streams~~ signaling internal to the telecommunications network,

monitor for an occurrence[[s]] in the additional ~~data streams~~ signaling internal to the telecommunications network of the ~~data of the first~~ predetermined data type and to register when the occurrences exceed a level for acceptable behaviour of the mobile telecommunications device within the telecommunications network,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Canceled)

15. (Canceled)

16. (Currently amended) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network comprising a core network, the telecommunications network including a base station, the method comprising:

at the base station, receiving radio transmissions from the mobile telecommunications device, the received radio transmissions including a request~~, wherein the request is associated with an event of the first type within the telecommunications network~~;

at the base station, ~~sending the request~~ converting the received radio transmissions into signals, and transmitting the signals into the telecommunications network;

in the telecommunications network, identifying the mobile telecommunications device;

in the telecommunications network, receiving the request from the mobile telecommunications device by way of the base station, and processing the request into ~~data streams~~ signaling internal to the telecommunications network;

in the telecommunications network, monitoring, in the ~~data streams~~ signaling internal to the telecommunications network, for an occurrence[[s]] of a predetermined data ~~of a first~~ type~~, wherein the data of the first type is a predetermined type of data arranged to cause the event of~~

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

~~the first type, and represents an~~ associated with the mobile telecommunications device, and representing an interaction between network devices in the core ~~telecommunications~~ network; and

registering when the occurrence[[s]] of the ~~data of the first~~ predetermined data type ~~exceed~~ exceeds a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Final Office Action

In the Final Office Action mailed July 5, 2019 ("Current Final Office Action," hereinafter), the Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu, and rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-13 and 16, of which claims 1 and 16 are independent, and the remaining claims are dependent. Applicant has amended various other claims as follows.

Applicant has amended claim 1 to describe that the recited "base station" as "transmitting the signals into the telecommunications network." Applicant has further amended claim 1 to replace "data streams internal to the telecommunications network" with "signaling internal to the telecommunications network," and to remove recitations of "data of a first type" and "event of a first type." Applicant has also amended claim 1 to recite, *inter alia*, "a predetermined data associated with the mobile telecommunications device, and representing an interaction between network devices in the core network." Support for this amendment can be found generally throughout the original application, and specifically at least at page 2, lines 17-21; page 3, lines 28-30 and lines 32-34; page 5; page 8, lines 1-6; and Figure 1, for example.

Applicant has amended claim 16 in a manner similar to that of claim 1. Support for this amendment is generally the same as for the amendment to claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Applicant has amended each of claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, and 13 to ensure consistency of antecedent basis with base claim 1.

No new matter has been introduced by way of any of the above amendments.

3. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. Applicant submits that Bu fails to teach each and every element set forth in any of claims 1-3, 5, 7-10, 12-13, or 16, and that these claims are allowable. Applicant first discusses claim 1, then subsequently addresses claims 2-3, 5, 7-10, 12-13, and 16.

In response to a previous Office Action mailed October 29, 2018 ("Previous Office Action," hereinafter), Applicant filed a response on March 29, 2019 ("Previous Response," hereinafter). In the Previous Response, Applicant summarized the teachings of Bu with respect to what Bu does and does not teach in regard to the monitoring of signaling in a network. In particular, Applicant provided a technical analysis demonstrating that Bu does *not* teach monitoring of signaling in a network, but rather teaches only *inferring* signaling messages in a network by counting data packets in the network and applying known signaling protocols to the data packet counts in order to estimate what signals may have been sent to facilitate transmission of the observed data packets. Applicant stands by this analysis of Bu, as it is relevant to arguments herein rebutting the rejections of the Current Final Office Action. Rather than reiterate the analysis here, Applicant refers to pages 9-13 of the Previous Response for details of the analysis of the teaching of Bu.

In the present submission, as described above, Applicant has amended claim 1 to replace "data streams internal to the telecommunications network" with "signaling internal to the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

telecommunications network." Further, the monitoring described, *inter alia*, in claim 1 is now carried out on the "signaling internal to the telecommunications network" in order to detect occurrences *in the signaling* of "a predetermined data associated with the mobile telecommunications device, and representing an interaction between network devices in the core network." As such, claim 1 distinguishes over Bu for at least the reason that *Bu simply does not teach monitoring of signaling*. Rather, as described in the Previous Response, Bu teaches counting *data packets* that are only able to be transmitted in the network at all because prior signaling – *signaling that Bu does not monitor* – has presumably taken place to establish a radio access bearer to carry the transmitted data packets. Stated again, Bu counts data packets and does not monitor signaling; claim 1 recites, *inter alia*, monitoring "*in the signaling* internal to the telecommunications network" for "an occurrence of a predetermined data type." On this basis alone, without considering additional details of claim 1 that are omitted from this condensed description for the sake of brevity, Bu fails to anticipate claim 1. Applicant considers additional details below.

Certain aspects of the Current Final Office Action refer to terminology of claim 1 that has been removed by way of the amendments described above. Specifically, as described above, Applicant has removed references to "data of a first type" and "event of a first type." While these amendments render certain aspects of the rejection of claim 1 moot, these aspects are nevertheless addressed below, because they are still relevant to demonstrating how and why the teachings of Bu fail to anticipate claim 1.

In the Current Final Office Action, page 3, the Examiner asserted that "Bu also discloses that data packets transmitted via the network are monitored, as all the data packets passing through the network will be compared to a threshold, but only data packets that [exceed] the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

threshold (**occurrences of data of a first type**) ([0056]) will be marked/flagged **(cause the event of the first type)** ([0056])." (Emphasis in original.) Thus, the Examiner equated "only data packets that [exceed] the threshold" disclosed in Bu with "data of the first type" previously recited, *inter alia*, in claim 1; and the Examiner equated the detection (via what the Examiner characterized as "monitoring") of "only data packets that [exceed] the threshold" disclosed in Bu with "occurrences of data of a first type" previously recited, *inter alia*, in claim 1. The Examiner thus also equated the marking/flagging of "only data packets that [exceed] the threshold" in Bu with "the event of the first type" previously recited, *inter alia*, in claim 1.

On page 4 of the Current Final Office Action, the Examiner interpreted "a subsequent request to transmit packet is received from the mobile" disclosed (according to the Examiner) in Bu as equivalent to "a request from the mobile telecommunications device by way of the base station" recited, *inter alia*, in claim 1. And the Examiner interpreted "the request to transmit subsequent packet is associated with user whose packets are flagged" disclosed (according to the Examiner) in Bu as equivalent to "wherein the request is associated with an event of the first type within the telecommunications network" previously recited, *inter alia*, in claim 1.

For purposes of clarity and emphasis, Applicant summarizes the Examiner's assertions in the Current Final Office Action in list form:

- "only data packets that [exceed] the threshold" disclosed in Bu asserted to be equivalent to "data of the first type" previously recited, *inter alia*, in claim 1.
- detection of "only data packets that [exceed] the threshold" disclosed in Bu asserted to be equivalent to "occurrences of data of a first type" previously recited, *inter alia*, in claim 1.
- marking/flagging of "only data packets that [exceed] the threshold" disclosed in Bu asserted to be equivalent to "the event of the first type" previously recited, *inter alia*, in claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

- "the request to transmit subsequent packet is associated with user whose packets are flagged" disclosed in Bu asserted to be equivalent to "wherein the request is associated with an event of the first type within the telecommunications network" previously recited, *inter alia*, in claim 1.

- "a subsequent request to transmit packet is received from the mobile" disclosed in Bu asserted to be equivalent to "a request from the mobile telecommunications device by way of the base station" recited, *inter alia*, in claim 1.

- "the request to transmit subsequent packet is associated with user whose packets are flagged" disclosed in Bu asserted to be equivalent to "wherein the request is associated with an event of the first type within the telecommunications network" previously recited, *inter alia*, in claim 1.

As amended, claim 1 no longer recites "the request is associated with an event of the first type within the telecommunications network, the event of the first type being associated with an interaction between network devices in the core network." As such, this aspect of the rejection is moot.

Bu does not teach: "wherein the telecommunications network is arranged to monitor, in the signaling internal to the telecommunications network, for an occurrence of a predetermined data type associated with the mobile telecommunications device, and representing an interaction between network devices in the core network"

As described above and in the Previous Response, Bu does not teach monitoring "signaling internal to the telecommunications network." At most, Bu teaches counting data packets. Thus, claim 1 distinguishes over Bu on at least the basis that claim 1 recites, *inter alia*, monitoring "*in the signaling* internal to the telecommunications network, for an occurrence of a predetermined data type associated with the mobile telecommunications device, and representing an interaction between network devices in the core network."

Further, as summarized above, the Examiner has interpreted "data of a first type" as equivalent to "only data packets that [exceed] the threshold" disclosed in Bu. However, since the "predetermined data type" is monitored for *in the signaling*, it cannot be considered data packets in the sense taught by Bu, let alone "only data packets that [exceed] the threshold."

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Still further, the Examiner interpreted "the event of the first type" as being equivalent to marking/flagging of "only data packets that [exceed] the threshold" disclosed in Bu. The removal from claim 1 by amendment of "the event of the first type" renders this aspect of the rejection moot. However, the description of the "predetermined data type" as "representing an interaction between network devices in the core network" makes clear that its occurrence in the "signaling" has a meaning quite distinct from marking or flagging of any type of data packets, let alone "only data packets that [exceed] the threshold."

Bu does not teach: "wherein the telecommunications network is further arranged to register when the occurrence exceeds a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network"

On page 5 of the Current Final Office Action, the Examiner interpreted "packets that have been flagged are monitored, and if a sufficient number of packets have been flagged, then traffic will be blocked" disclosed (according to the Examiner) in Bu as being equivalent to "wherein the telecommunications network is further arranged to register when the occurrences of the data of the first type exceed a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network" recited, *inter alia*, in claim 1. Again, the removal of "data of the first type" renders this assertion by the Examiner strictly moot. However, the "occurrence" that exceeds "a level for acceptable behaviour" referred to in this limitation represents an excess of "an interaction between network devices in the core network," not "a sufficient number of packets [that] have been flagged." Accordingly, this limitation also distinguishes over Bu.

For at least the reasons above, Applicant submits that claim 1 distinguishes over Bu, and that claim 1 is therefore allowable.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Claim 16 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 16 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 2-3, 5, 7-10, and 12-13 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claims 2-3, 5, 7-10, and 12-13 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with any of claims 2-3, 5, 7-10, or 12-13.

4. Response to Rejections under 35 U.S.C. § 103(a)

a. Claims 4 and 6

The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu. Each of claims 4 and 6 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that each of claims 4 and 6 is allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with either of claims 4 or 6.

b. Claim 11

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

5. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: December 12, 2019

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	12/12/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/DORIS M KING/
*** 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.	

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.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14/646,554	Filing Date	2015-05-22	Docket Number (if applicable)	15-686-WO-US	Art Unit	2438
First Named Inventor	Frank Muller			Examiner Name	Vu, Phy Anh Tran		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☒ Other After Final Response filed December 12, 2019

☐ Enclosed

☐ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132490

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2019-12-31
Name	David A. Grabelsky	Registration Number	59280

This collection of information is required by 37 CFR 1.114. 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 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.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	1900	1900
		Total in USD ($)		**1900**

Electronic Acknowledgement Receipt

EFS ID:	38175895
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	31-DEC-2019
Filing Date:	21-MAY-2015
Time Stamp:	15:06:25
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1900
RAM confirmation Number	E2019BUF06543168
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	15-686-WO-US_Request_for_Continued_Examination_form_05Jul19_FOA.pdf	697835 0e6ae67c6fe6f7023f25c3feac9ad97b1da4ba5a	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30746 d94fc26603ba88cccfd7c17933e917366d6a4678	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	728581		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 02/28/2020

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
VU, PHY ANH TRAN	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
02/28/2020	PAPER

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

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

Office Action Summary	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA (FITF) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 12/31/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-13 and 16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-13 and 16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 5/21/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

1.☑ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☑ Interview Summary (PTO-413) Paper No(s)/Mail Date 1/13/2020.

4) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/31/2019 has been entered.

Notice of Pre-AIA or AIA Status

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

EXAMINER'S NOTE

In an effort to move the case forward, Examiner suggested to the Applicant's representative, Mr. David Grabelsky to further amend the independent claims. However, Mr. Grabelsky did not accept the suggestion on 01/16/2020.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claim 1 recites "..and representing an interaction between network devices in the core network". It is unclear what is representing an interaction between network devices in the core network. To expedite the prosecution process, the predetermined data type is interpreted as representing an interaction between network devices in the core network.

Claim 16 is rejected for the same rationale as claim 1 above.

Response to Arguments

Applicant's arguments with respect to claims 1 & 16 have been considered but are moot in view of the new interpretation of the reference.

In addition, to clarify the Examiner's position, Applicant's arguments are addressed below:

Regarding claim 1, on pages 9-13, Applicant seems to argue that Bu fails to disclose 1) monitoring of signaling in a network, 2) "wherein the telecommunications network is arranged to monitor, in the signaling internal to the telecommunications network, for an occurrence of a predetermined data type associated with the mobile telecommunications device, and representing an interaction between network devices in the core network" and 3) "wherein the telecommunications network is further arranged

to register when the occurrence exceeds a level for acceptable behaviour of the mobile telecommunications device in the telecommunication network"

In response, Examiner respectfully disagrees. Bu discloses methods and devices for defending a wireless network against a signaling attack *(at least in the Title)*. As discloses in Bu, in order to enable transmission to/from a mobile device, a dedicated channel, known as radio access bearer (RAB) has to be created ([0024]-[0026]). For instance, in a UMTS wireless network, in order to create a RAB, at least 24 signaling messages are exchanged between the mobile device, the base station controller (BSC) or radio network controller (RNC) and the core network *([0026])*. This is a significant amount of overhead for the RNC and causes severe processing overhead during signaling time intervals. As such, an attacker can exploit the heavy-duty signaling overhead required for setup of RABs by sending a low volume burst at appropriately timed periods so that immediately after a RAB is torn down due to inactivity, a burst arrives from the attacker to trigger an establishment of a new RAB. This frequent setup/release can easy overload wireless network by requiring an excessive amount of signaling messages *([0029])*. Therefore, in order to prevent such attack, Bu discloses a way to determine a signaling cost to data ratio. This signaling cost to data ratio allows malicious traffic to be identified as soon as it begins to introduce excessive signaling cost *([0045].)* Excessive signaling cost is additional signaling costs even though the volume of actual, transmitted data is low. In other word, when there are excessive signaling messages for setting up and releasing RABs are exchanged, but the actual data being transmitted is not much, the wireless network can reliably detect that a signaling attack is ongoing.

1) As discloses in table 2 and paragraphs [0054]-[0056], Bu clearly discloses when a packet is sent from a sender to a user, a signaling cost to data ratio is determined. In order to determine the signaling cost to data ratio, the wireless network tracks ***(monitors)*** the number of signaling messages ***(signals)*** that are required in order to establish a dedicated channel to transmit the packet, and compare the number of signaling messages required to the amount of data in the packet.

2) As discussed in point 1 above, in order to determine signaling cost to data ratio for a user/sender, the wireless network in Bu has to monitor traffics and tracks the signaling messages ***(monitor for an occurrence of a predetermined data type)***. Bu also teaches the signaling messages are messages that are exchanged between the mobile device and devices in the core network ***(representing an interaction between network devices in the core network)*** ([0026]).

3) As discloses in table 2 and at least paragraphs [0054]-[0057], when the signaling cost to data ratio of the packet exceeds a threshold, then flag the packet. In other word, when the number of signaling messages determined from the packet exceed a reference signaling messages, then the packet from the sender to the user will be flagged ***(wherein the telecommunications network is further arranged to register when the occurrence exceeds a level for acceptable behavior of the mobile telecommunication device the telecommunication network)***.

As such, contrasting to Applicant's arguments, Bu clearly discloses all the limitations argue above.

For all depending claims, see response to arguments above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5, 7-10, 12-13 and 16 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Bu et al. (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 1, Bu discloses a system comprising:

a telecommunications network *(figure s 1 & 5)* comprising a core network *(figures 2 & 4, core network)*; and

a hardware base station configured within the telecommunications network *(figures 1, 5 & 6, base station)*, wherein the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for transmitting the signals into the telecommunications network *([0023]-[0026], base station receives radio transmission from wireless devices, converts the radio transmission into signals and transmits the signals to the wireless network)*;

wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive a request from the mobile telecommunications device by way of the base station, and further to process the

request into signaling internal to the telecommunications network *([0023]-[0026] [0039]-[0040][0045]-[0047][0049]-[0053], i.e.: when a request is received from the wireless device, the request will be processed internally to determine a number of signaling messages (signaling) that need to be exchanged between entities in the wireless network)*,

wherein the telecommunications network is arranged to monitor, in the signaling internal to the telecommunications network, for an occurrence of a predetermined data type associated with the mobile telecommunications device and representing an interaction between network devices in the core network *(table 2, [0053]-[0057], the number of signaling messages is monitored for the wireless device to determine signaling cost to data ratio)*,

and wherein the telecommunications network is further arranged to register when the occurrence exceeds a level for acceptable behaviour of the mobile telecommunications device in the telecommunications network *([0056]-[0057], when the signaling cost to data ratio for the wireless device exceeds a threshold, subsequent traffic from the wireless device is flagged.)*

Regarding claim 2, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor for the occurrence of predetermined data type by counting that a number of occurrences of the predetermined data type is detected in the signaling when the occurrences exceed a predetermined temporal rate and further wherein the telecommunications network is arranged to register when the number of the detected occurrences exceeds a

predetermined threshold *(table 2; [0049]-[0050][0056]-[0057], if sufficient number of signaling cost to data ratios exceed threshold have been flagged, then filter may be applied)*.

Regarding claim 3, Bu discloses the system according to claim 2. Bu further discloses the telecommunications network is arranged to count the number of occurrences of the data of the predetermined data type in the signaling when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval *(table 2, [0056]-[0057], signaling cost to data ratios of traffic that have been flagged as suspicious for a predetermined period of time)*.

Regarding claim 5, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is further configured to detect when the occurrences in the signaling of the predetermined data type exceeds a predetermined rate *(table 2; [0054]-[0057], signaling cost to data ratios are tracked for predetermined threshold)*.

Regarding claim 7, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to register when the occurrences of the predetermined data type exceed the level for acceptable behaviour by setting a flag and/or starting a back off timer *([0057], flag is set)*.

Regarding claim 8, Bu discloses the system according to claim 1. Bu further discloses the predetermined data type indicates attachment of the mobile to telecommunications device to the telecommunications network *([0056][0060], signaling cost to data ratios that exceed threshold indicates possible attack from the wireless device to the network)*.

Regarding claim 9, Bu discloses the system according to claim 1. Bu further discloses the predetermined data type indicates setting up of a bearer by the mobile telecommunications device *([0023]-[0027], setting up RAB)*.

Regarding claim 10, Bu discloses the system according to claim 1. Bu further discloses the predetermined data type indicate handover of the mobile telecommunications device *([0007][0023][0027], handoff)*.

Regarding claim 12, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is arranged to monitor the occurrences in the signaling of the predetermined data type in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network *([0021][0056]-[0057], Serving Gateway Support Node (SGSN))*.

Regarding claim 13, Bu discloses the system according to claim 1. Bu further discloses the telecommunications network is further configured to identify at least one additional mobile telecommunications device,

receive signals from the at least one additional device and to process these signals into additional signaling internal to the telecommunications network *([0045]-[0047][0049]-[0053], signals from another mobile/user is obtained and are processed into signaling messages internal to the wireless network)*,

monitor for an occurrence in the additional signaling internal to the telecommunications network of the predetermined data type and to register when the occurrences exceed a level for acceptable behaviour of the mobile telecommunications device within the telecommunications network *([0049]-[0050][0056]-[0057], the signaling cost to data ratio is monitored, and when a sufficient number of signaling cost to data ratios have been flagged exceeds a certain threshold, signals as malicious)*,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device *([0051][0052], mobile/user profiles are aggregated)*.

Claim 16 is rejected for the same rationale as claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 6 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu (US 2006/0230450 A1-hereinafter Bu.)

Regarding claim 4, Bu discloses the system according to claim 3. Bu further discloses the telecommunications network includes a counter and a timer *(table 2, Flag ++, and timer)*, and wherein the telecommunications network is arranged to start the counter upon detection of an occurrence of the predetermined data type, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following detection of the predetermined data type occurs *(table 2,[0054][0056]-[0057] signaling cost to data ratios are counted)*.

Bu does not explicitly disclose increase the counter by one unit if a following detection of data of the first type occurs within the predetermined time interval T as measured by the timer.

However, as another option for determining if the data packets are part of an attack, Bu also discloses a timer which times the suspicious behavior of traffic from a user, if the behaviour continues within a predetermined time interval T as measured by the timer, then the future traffic from the user will be blocked *(table 2; [0050]-[0057], packets with signaling cost to data ratios exceeding threshold are tracked and counted for a predetermined period of time)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine the timer and the counter as discloses by Bu to provide another way of determining suspicious data packets from users.

Claim 6 is rejected for the same rationale as claim 4 above.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Bu and in view of Amin et al. (US Patent 5,953,652 hereinafter Amin.)

Regarding claim 11, Bu discloses the system according to claim 10. Bu also discloses the telecommunications network to monitor the mobile telecommunications device handover *(figure 5; [0007][0023][0027][0037]-[0039], handoff to different BS)*.

Bu does not disclose monitor a tracking area of the mobile telecommunications device and to register the occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

However, Amin discloses monitor tracking area of a mobile telecommunications device and to register occurrence of data indicating handover only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area *(column 7, lines 14-35, handover signal remains in a location would be detected as unrealistic geographic movement)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Amin into the system of Bu to enhance the collected state information of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH TRAN VU whose telephone number is (571)270-7317. The examiner can normally be reached on Monday-Friday 7 am-1 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571) 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/PHY ANH T VU/
Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA (FITF) Status No

All participants (applicant, applicant's representative, PTO personnel):

(1) PHY ANH TRAN. VU. (3) _____.

(2) David Grabelsky. (4) _____.

Date of Interview: 13 January 2020.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☑ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Bu et al. (US 2006/0230450 A1).

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

In an effort to move the case forward, Examiner contacted Applicant's reprentative, Mr. David Grabelsky to suggest further clarifying the independent claims. However, Mr. Grabelsky did not accept the suggestion on 01/20/2020..

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

Notice of References Cited	Application/Control No. 14/646,554	Applicant(s)/Patent Under Reexamination Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080022402-A1	01-2008	Francfort; Stanislas	H04L63/1408	726/22
*	B	US-20100304706-A1	12-2010	Haverty; James D.	H04K3/45	455/404.1
*	C	US-20160248789-A1	08-2016	NAKAMATSU; Ryouji	H04L63/1416	1/1
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L 63/14	5/2/2016; 6/23/2017; 7/4/2019; 2/27/2020	PVU
H04L 63/1425	5/2/2016; 6/23/2017; 7/4/2019	PVU
G06F12/14	02/27/2020	

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016	PVU
Keywords search	05/02/2016; 12/09/2016; 6/23/2017; 11/22/2017; 10/26/2018; 7/4/2019; 02/27/2020	PVU
Consulted with WG SPE and QAS regarding 101 issues	06/23/2017	PVU
IP.com	02/27/2020	PVU

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

ERICSSON EXHIBIT 1005, Page 626

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

ERICSSON EXHIBIT 1005, Page 627

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	**Art Unit**
	PHY ANH T VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016	06/23/2017	11/22/2017	10/26/2018	07/04/2019	02/27/2020		
	1	✓	✓	✓	✓	✓	✓	✓		
	2	✓	✓	✓	✓	✓	✓	✓		
	3	✓	✓	✓	✓	✓	✓	✓		
	4	✓	✓	✓	✓	✓	✓	✓		
	5	✓	✓	✓	✓	✓	✓	✓		
	6	✓	✓	✓	✓	✓	✓	✓		
	7	✓	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓	✓		
	9	✓	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓	✓		
	11	✓	✓	✓	✓	✓	✓	✓		
	12	✓	✓	✓	✓	✓	✓	✓		
	13	✓	✓	✓	✓	✓	✓	✓		
	14	✓	✓	-	-	-	-	-		
	15	✓	✓	-	-	-	-	-		
	16		✓	✓	✓	✓	✓	✓		

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 4961

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/646,554	05/21/2015 RULE	726	2438	15-686-WO-US

APPLICANTS

KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

INVENTORS

Frank Muller, Delft, NETHERLANDS;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/EP2013/074440 11/22/2013

**** FOREIGN APPLICATIONS ***************************

EUROPEAN PATENT OFFICE (EPO) 12193884.9 11/22/2012

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

07/07/2015

Foreign Priority claimed	☑ Yes ☐ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	☑ Yes ☐ No					
Verified and Acknowledged	/PHY ANH TRAN VU/ Examiner's Signature	Initials	NETHERLANDS	3	15	2

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

System to Detect Behaviour in a Telecommunications Network

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
1480	No._____ to charge/credit DEPOSIT ACCOUNT	☐ 1.16 Fees (Filing)
	No._____ for following:	☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)
		☐ Other _____
		☐ Credit

Discover | PAT | defend from signaling attack | + 0 mods | 2 filters | STIC

Visuals | Query | Results | 0 Selected | Relevance | None | None

1 - 50 189 results

1. **Securing medical devices through wireless monitoring and anomaly detection**

A medical device monitor (MedMon), method and computer readable medium is disclosed. The MedMon is configured to operate in a system having communications between a first medical device associated with a patient and a second device. The MedMon includes a receiver configured to snoop on...

CURRENT ASSIGNEES: PRINCETON UNIV (+1)
US10135849 | US PATENTS | 20-NOV-2018

2. **Detecting radiation-based attacks**

In a device having a plurality of circuits that can store at least a first value and a second value, a method can include configuring at least one circuit to persistently store the first value; determining whether the at least one circuit is storing the second value; and initiating a countermeasure...

CURRENT ASSIGNEES: ATMEL CORP
TW200820091A | TAIWAN APPLICATIONS | 01-MAY-2008

3. **Intrusion detection system in a wireless communication network**

A system and method for providing improved FGS identification in scalable video coding. According to the present invention, each FGS enhancement layer is assigned a unique dependency identifier and contains only FGS enhancement information. For subsequent enhancement layers, the base dependency...

CURRENT ASSIGNEES: ALCATEL LUCENT
EP1864469A2 | EPO APPLICATIONS | 12-DEC-2007

4. **Intrusion detection system in a wireless communication network**

A system and method for providing improved FGS identification in scalable video coding. According to the present invention, each FGS enhancement layer is assigned a unique dependency identifier and contains only FGS enhancement information. For subsequent enhancement layers, the base dependency...

CURRENT ASSIGNEES: EMPLOYEE INVESTM FUND FCP ZAL
WO2006092737A2 | WIPO APPLICATIONS | 08-SEP-2006

5. **System and methods for preventing denial of service attacks**

Conventional countermeasures to Distributed Denial of Service (DDoS) attacks typically focus on practices and rules for organizing a robust, DDoS-resilient network which anticipates proactive cooperation of users. Such measures involve widespread implementation cooperation and may be difficult or...

CURRENT ASSIGNEES: CISCO TECH INC
US7587760 | US PATENTS | 08-SEP-2009

6. **Early traffic regulation techniques to protect against network flooding**

Methods and apparatus for providing an Anti-Flooding Flow-Control (AFFC) mechanism suitable for use in defending against flooding network Denial-of-Service (N-DoS) attacks is described. Features of the AFFC mechanism include (1) traffic baseline generation, (2) dynamic buffer management, (3) packet...

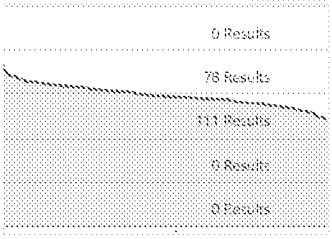
CURRENT ASSIGNEES: PALO ALTO NETWORKS INC
US7295516 | US PATENTS | 13-NOV-2007

7. **Early traffic regulation techniques to protect against network flooding**

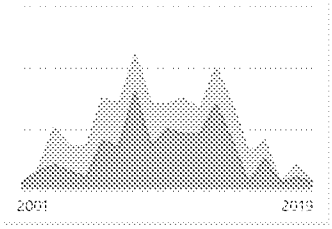
Result #1 PREV NEXT

Top 189 results

Relevance VIEW



Publication Date VIEW



First Cur Assignees by Relevance VIEW

- PRINCETON UNIV (1)
- ATMEL CORP (1)
- ALCATEL LUCENT (3)
- EMPLOYEE INVESTM FUND... (2)
- CISCO TECH INC (3)
- PALO ALTO NETWORKS INC (2)
- ZTE CORP (1)

More Visuals

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		H04I63/14.cpc. and (excessive near5 (request occurrence traffic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
		"20060230450".pn. and nas	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:23
		(monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
L1	816	(avoid$4 prevent$4) same (signal$4 near3 attack)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 19:30
L2	353	l1 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:31
L3	0	H04I63/1425.cpc. and l2	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/02/27 19:31
L4	203	(avoid$4 prevent$4) same (signal$4 near3 attack) and (telecommunications mobile)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 19:32
L5	71	l4 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:32
L6	1	(avoid$4 prevent$4) same (signal$4 near3 attack) and (set$up with release) and (excessive near3 signal$4 near5 message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/02/27 19:37
L7	1	(avoid$4 prevent$4) same (signal$4 near3 attack) and (set$up with release) and (excessive near3 signal$4 near5 messages)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/02/27 19:37

L8	0	l2 and G06f12/14.cpc.	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:38
L9	0	l1 and G06f12/14.cpc.	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:38
L10	1	l1 and h04l63/14.cpc.	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:38
L11	26	(avoid$4 prevent$4) same (signal$4 near3 attack) and 3g	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 19:39
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:23
S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19

S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12250043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:32
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT;	OR	OFF	2016/05/02 11:34

			IBM_TDB			
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16
S37	3	"20100064341".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:11
S38	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
S39	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13
S40	1342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S41	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S42	1121	(monitor$4 with (network with traffic) with event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52

S43	30	(monitor$4 with (network with traffic) with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S44	268	monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
S45	155	S44 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 11:54
S46	169	(network with indicat$4 near5 event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 12:55
S47	106	S46 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 12:55
S48	2	"20060230450".pn. and network	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:44
S49	1	"20060230450".pn. and bs	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:52
S50	1	"20060230450".pn. and pdsn	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:26
S51	2	"20150304345".pn. and (data near3 first near3 type)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:53
S52	13	"9684898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S53	2	"9684898".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S54	4	"9633208".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 18:00
S55	1	"20150304345".pn. and bearer	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:29

S56	0	"20060230450".pn. and handover	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:37
S57	0	"20060230450".pn. and hand$over	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S58	1	"20060230450".pn. and hand$off	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S59	1	H04I63/14.cpc. and (mobile and (excessive near5 occurrence))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:33
S60	1	H04I63/14.cpc. and (excessive near5 occurrence)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:34
S61	11	H04I63/14.cpc. and (excessive near5 (request occurrence traffic))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
S62	92	H04I63/14.cpc. and (excessive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:39
S63	48	S62 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:39
S64	237	H04I63/1425.cpc. and (mobile and excessive and (malicious attack suspicious))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:45
S65	71	S64 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:46
S66	461	(telecommunication with (exceed$4) near5 threshold)	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S67	2	(telecommunication with (exceed$4) near5 threshold) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S68	0	(telecommunication with (exceed$4) near5 threshold) same behavior	US-PGPUB; USPAT	OR	ON	2017/11/22 07:12
S69	0	(monitor$4 with data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S70	0	(monitor$4 same data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S71	64	(monitor$4 with abnormal) with data near5 streams	US-PGPUB; USPAT	OR	ON	2017/11/22 07:14

S72	19559	monitor$4 with data near5 streams	US-PGPUB; USPAT	OR	ON	2018/05/09 17:15
S73	62	(monitor$4 with streams) same (data near5 abnormal$3)	US-PGPUB; USPAT	OR	ON	2018/05/09 17:20
S74	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:33
S75	7	g06f12/14.cpc. and (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:35
S76	1734	(detect$4 defend$4) with (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:38
S77	28	(detect$4 defend$4) with (signal$4 near3 attack$4) same (3g near10 wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:39
S78	3	"20060230450"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2019/07/03 08:38
S79	0	H04l63/14.cpc. and (excessive near5 occurrence) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:26
S80	14	H04l63/14.cpc. and (attack$4) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:26
S81	69	H04l63/1425.cpc. and (attack$4) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:33
S82	24	S81 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2019/07/04 12:33
S83	2	"20150304345"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/01/13 11:27
S84	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/01/13 11:54
S85	0	"20060230450".pn. and (utms)	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	OFF	2020/02/26 10:24

			DERWENT; IBM_TDB			
S86	2	"20060230450".pn. and (umts)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/26 10:24
S87	2	"20190259485".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 10:15
S88	2	"20080189614".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 14:02

EAST Search History (Interference)

<This search history is empty>

2/27/2020 7:46:32 PM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank Muller
Art Unit	2438
Examiner Name	Phy Anh Tran Vu
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2011072719	WO	A1	2011-06-23	NOKIA SIEMENS NETWORKS OY		

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank Muller
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	15-686-WO-US

	1	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank Muller
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	15-686-WO-US

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David A. Grabelsky/	Date (YYYY-MM-DD)	2020-03-27
Name/Print	David A. Grabelsky	Registration Number	59208

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 June 2011 (23.06.2011)

PCT

(10) International Publication Number
WO 2011/072719 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/12* (2009.01)

(21) International Application Number:
PCT/EP2009/067170

(22) International Filing Date:
15 December 2009 (15.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **EISL, Jochen** [DE/DE]; Breslauer Str. 48, 85748 Garching (DE). **ABENDROTH, Joerg** [DE/DE]; Weidener Str. 3, 81737 München (DE). **MUSTAJARVI, Jari Pekka** [FI/FI]; Seitsemäs Järvikuja 6, FI-02730 Espoo (FI).

(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR/Patent administration, 80240 Munich (DE).

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

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

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: METHOD, APPARATUS AND RELATED COMPUTER PROGRAM PRODUCT FOR DETECTING CHANGES TO A NETWORK CONNECTION

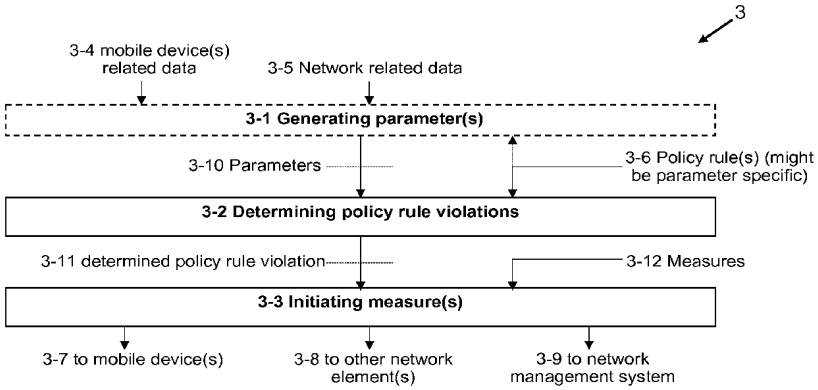


FIG 3

(57) **Abstract**: Disclosed is a method, a device and a computer program product for detecting changes to the connection of a device (preferably a mobile device) to a network and for initiating at least one measure when changes are detected. Changes might be caused by malicious users or malicious mobile phone SW in order to perform Denial of Service (DoS) attacks to the network. Those changes could be for example frequent handover actions, frequent attach/detach actions or frequent Packet Data Protocol context activation, deactivation or modification actions initiated by a mobile device or a group of mobile devices. The changes to the connection are detected by checking if parameters related to the mobile device, or related to network elements, violate defined policy rules. The detection itself is done in a network element, which is preferably a core network element.

WO 2011/072719 A1

DESCRIPTION

TITLE

METHOD, APPARATUS AND RELATED COMPUTER PROGRAM PRODUCT FOR DETECTING CHANGES TO A NETWORK CONNECTION

TECHNICAL FIELD OF THE INVENTION

[001] The present invention relates generally to wireless and fixed networks, and there to network connections between device(s) and the network. More specifically, the present invention relates to a method, an apparatus and a related computer program product for detecting changes to a network connection.

[002] Examples of the present invention are applicable, but not limited, to Global System for Mobile communication (GSM) networks, Universal Mobile Telecommunications System (UMTS) networks, Code Division Multiple Access (CDMA) networks, Worldwide Interoperability for Microwave Access (WIMAX) networks, Wireless Local Area Networks (WLAN), Long Term Evolution (LTE) and System Architecture Evolution (SAE) networks, Cable networks and DSL networks.

BACKGROUND OF THE INVENTION

[003] In a telecommunication network various causes exist why a connection between a device and the network might be changed. For example when a mobile device (or fixed device with access to a wireless network) connects or disconnect to/from the wireless network (when the device is switched ON or OFF or if the GPRS connection of a mobile device is switched ON or OFF) or if for example a mobile device moves and leaves the area of the network cell where it is currently connected to (which results in a handover action of the connection and so in a change of the connection). Further the

connection may be changed by activation, deactivation or changing one or more PDP context(s).

[004] In case of wireless networks typically handover actions will be performed from one cell to another cell within the same network. However due to the increasing availability of more and more different wireless access network types also the handover from one access network type to another access network type becomes more and more probable, assuming that the mobile device supports multiple access networks.

[005] Handover actions of a mobile device within the same wireless network, or between different wireless networks, can be triggered by several criteria, for example by detecting a change in the quality of the radio bearer based on measured radio link attributes or by observing changes to the end-to-end Quality of Service (QoS) on a radio link. If such a change is detected, and another radio bearer with sufficient quality is available, a handover action of the mobile device from one radio bearer to another radio bearer will be initiated. The handover action may be triggered automatically by the network or the device.

[006] With the 3rd Generation Partnership Project (3GPP) release 8 specification a mobile device may be connected either through a 3GPP access network or through a non 3GPP access networks to a 3GPP core network. Handover actions between 3GPP access networks and non 3GPP access network are possible and might be also initiated by the user of the mobile device.

[007] However, user initiated handover may be triggered by mistake, by a malicious user or even by malicious mobile device software. A user staying with his mobile device in an area with simultaneous access to several access networks may initiate handover actions between the different access

networks in a continuous way. Movement of the user is not necessary in this case.

[008] Same applies to situations where network connection of a mobile device are established or torn down, or to situations where one or more Packet Data Protocol (PDP) context are activated, deactivated or changed (for example by switching GPRS ON or OFF), also those actions might be triggered by mistake, by a malicious user or by malicious software.

[009] Handover actions, network connection establishment or teardown actions and PDP context activation, deactivation or modification actions consume network resources which in turn reduces performance of the network, especially if frequent actions occur. Therefore those actions without purpose (without any real need) should be avoided. It is noted that such frequent handover actions and frequent connections establishment / teardown actions, which may be initiated by a malicious user or software, are just example for not needed actions which consume network resources and so reduce network performance. Same applies in practice to any connection related parameter or to requested connection resources, which could be also changed without any real need.

[0010] With the introduction of user initiated handover the probability of continuous changes to a network connection of a mobile device without any real purpose, so called denial-of service (DOS) attacks, increases and becomes a threat for mobile networks. For example a single user or a group of users could trigger frequent actions leading to frequent changes of the connection between mobile device(s) and a network. DOS attacks could be also caused mobile devices infected for example by malicious software. Infected mobile devices might start malicious activities based on the geographical position of the mobile devices. When entering such an area the mobile device could try to identify other infected mobile devices in the same area and start a DOS

attack for example by coordinated frequent handover, connection establishment/teardown actions or PDP context activation/deactivation or modification actions, or the mobile device could even try to infect other mobile devices located in the same area.

SUMMARY OF THE INVENTION

[0011] In consideration of the above, it is an object of the present invention to overcome the above mentioned problem of possible changes to a connection of device(s) (preferable mobile devices) to a network caused by for example a malicious user or mobile device. In particular, the present invention provides a method, an apparatus and a related computer program product for detecting changes to a connection of mobile device(s) to a network. If changes to the connection, resulting for example from frequent actions without purpose, are detected measures may be applied in order to for example inhibit such frequent actions or inform the user or network operator about it.

[0012] According to an example of the present invention, in a first aspect, this object is for example achieved by **a method** for detecting changes to a connection of a mobile device to a network whereby the detecting is done by determining if at least one parameter related to the mobile device or related to the network is violating a policy rule related to the changes, and if a policy rule is violated initiating at least one measure related to the detected changes.

[0013] According to further refinements of the example of the present invention as defined under the above first aspect, the method further comprises the claimed subject matter of any of the claims 2 to 21.

[0014] According to an example of the present invention, in a second aspect, this object is for example achieved by **a**

network element for detecting changes to a connection of a mobile device to a network, the network element comprising a determining means determining if at least one parameter related to the mobile device or related to the network is violating a policy rule and a measure means initiating at least one measure related to the detected changes if a policy rule is violated.

[0015] According to further refinements of the example of the present invention as defined under the above second aspect, the network element further comprises the claimed subject matter of any of the claims 23 to 43.

[0016] According to an example of the present invention, in a third aspect, this object is for example achieved by **an apparatus** for detecting changes to a connection of a mobile device to a network, the apparatus comprising a determining means determining if at least one parameter related to the mobile device or related to the network is violating a policy rule and a measure means initiating at least one measure related to the detected changes if a policy rule is violated.

[0017] According to further refinements of the example of the present invention as defined under the above third aspect, the apparatus further comprises

- a generating block for generating the at least one parameter from data received from a mobile device or from at least one other network element
- a measure block applying measures to the mobile device or a management system or another network element after detecting the changes to the connection of the mobile device to the network
- optionally at least one processor and at least one memory including computer program code, wherein the at least one memory and the computer program code are configured to, with the at least one processor.

[0018] According to further refinements of the example of the present invention as defined under the above third aspect, the apparatus further comprises at least the claimed subject matter of any of the claims 23 to 43.

[0019] According to an example of the present invention, in a fourth aspect, this object is achieved by **a computer program** comprising code for detecting changes to a connection of a mobile device to a network as claimed in any one of the claims 1 to 21 when the computer program is run on a processor.

[0020] According to further refinements of the example of the present invention as defined under the above fourth aspect, wherein the computer program is a computer program product further comprises a computer-readable medium bearing computer program code embodied therein for use with a computer.

[0021] Embodiments of the present invention can provide one or more of the following advantages:

- Consumption or reservation of network resources without purpose is avoided.
- DoS attacks can be detected, reported and inhibited.
- Decrease of network performance, and so the decrease of user experience in the network, is avoided.
- Possible network outage or unavailability due to overload situations caused by malicious frequent connection changes is avoided.
- Only malicious connection changes are detected and inhibited while still allowing normal connection changes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] Examples of the present invention are described herein below with reference to the accompanying drawings, in which:

[0023] Fig. 1 illustrates a first example embodiment of a high level network architecture where the invention is used; and

[0024] Fig. 2 presents a second example embodiment of a high level network architecture where the invention is used; and

[0025] Fig. 3 shows method steps related to the present invention; and

[0026] Fig. 4 illustrates method steps related to the present invention in more detail; and

[0027] Fig. 5 shows a third example embodiment of a network element according to the present invention; and

[0028] Fig. 6 presents a first example signaling diagram according to the present invention; and

[0029] Fig. 7 presents a second example signaling diagram according to the present invention; and

[0030] Fig. 8 presents a third example signaling diagram according to the present invention; and

[0031] Fig. 9 presents a fourth example embodiment of a network element according to the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

[0032] Examples of the present invention are described herein below with reference to the accompanying figures. The figures include mandatory, as well as optional elements, related to the present invention. Furthermore, the figures include mainly elements that are important for the present invention, or that are useful in the context of describing the present invention. Not important network elements, messages or signals (like for example elements where information is just relayed/passed through, or messages just acknowledging the receipt of another message) might have been left out of the figures and the description for simplification purposes.

[0033] In the description the terms Policy and Charging Rule Function (PCRF), Network Management System (NMS), Packet Data Network Gateway (PDN-GW), Mobile Device (MD), Mobility Anchor, base station (BTS), access point (AP), base station controller (BSC), Radio Network Controller (RNC), GPRS Support Node, Mobility Management Entity (MME), access network and core network are examples for elements, functions and networks without restricting or limiting them to functions, elements or networks of this specific type, or excluding any possible alternatives. The described embodiments are not limited to the mentioned networks, network elements, messages and signals.

[0034] The following paragraphs define certain terms and elements used throughout this application. These definitions are related to the example embodiments of the invention as described below and might not be directly applicable to other, alternative, embodiments of the invention not described within this document.

[0035] The term “connection” refers to a connection of a mobile device to a network or network element in a very broad sense. It covers for example the connection between the mobile device and the base station, as well as the connection between a mobile device and a core network element (for

example a Serving GPRS Support Node - SGSN, where a mobile devices may attach to when establishing a GPRS connection). Further on the term "changes to a connection" covers changes to the connection between a mobile device and an access point (for example caused by a handover action to another base station/access point, where the other base station/access point might belong to the same or a different network), as well as for example attach or detach actions between the mobile device and a core network node and Packet Data Network context activation, deactivation and modification. Note, the above mentioned interpretations related to the terms "connection" and "changes to a connection" are just examples, changes related to any kind of connection between one or more mobile device and any other network element shall be covered by those terms as well.

[0036] An access network is the part of a network including for example access points (like for example base stations in case of a mobile network or a Digital Subscriber Line Access Multiplexer (DSLAM) in case of a fixed network) where the devices are connected to, and access network controller(s) or access network gateway(s) where the access points are connecting to. The access network controller(s) or access network gateway(s) are access network elements providing the interface towards a core network. An access network controller could be for example a Base Station Controller (BSC) or a Radio Network Controller (RNC) in case of a wireless or mobile network, an access network gateway could be for example an Access Service Network Gateway (ASN-GW) of a Wimax network. Typically the controller or access point network elements could include at least partly handover functionality. Access networks of different types could be for example GERAN, UTRAN, E-UTRA, CDMA2000 RAN, WLAN or Wimax (note this is just an example list and might not be complete).

[0037] A core network (or network core) is the central part of a telecom network that provides various services to

customers who are connected by the access networks. Several access networks of similar or different types can be connected to one core network. Examples of core network functions are traffic aggregation, authentication, call control, switching & routing, charging, services and gateway functionality to connect to other networks (for example the Internet). Core network element may be involved in handover activities, especially if the handover relates to inter RAN handover actions between different access networks which might be even of different types. Examples for core network elements involved in handover activities are Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobility Management Entity (MME), Serving Gateway (SGW) and Packet Data Network Gateway (PGW). For example a SGSN might be involved in attach or detach actions of mobile device when it establishes or tears down a connection to the network.

[0038] A policy rule in the context of this application is a rule which might be applied to a whole network, parts of a network, one or more network elements, one or more mobile devices or one or more mobile subscribers. Further a policy rule might be specific for a traffic type (for example circuit switched or packet switched traffic or traffic with different Quality of Service (QoS) requirements). Policy rules might be used to steer and shape traffic in a network, to detect abnormal situation or to control/authorize QoS related traffic or requests. They are typically stored centrally in one network element (for example in a Policy and Charging Rules Function (PCRF) network element) but may be also stored in a distributed manner in several network elements (for example several PCRFs serving different parts of the network). Policy rules can be stored and implemented basically in any network element in the core or access network. In addition to the policy rules those network elements (like for example the PCRF) might also include information about the measures that shall be applied if a policy rule is violated.

[0039] An attach/detach action describes situations where a mobile device connects/disconnects to/from a network. Examples for such actions are when the mobile device is switched ON or OFF or when the mobile device established a new type of connection with a network (like for example a GPRS data connection while still maintaining another connection like for example a voice connection).

[0040] A handover action means the shifting of a mobile device connection from one base station or access point to another one. Handover action may be caused for example by a mobile device moving from one cell served by one base station or access point to another cell, by actively selecting another base station or access point or by changing network conditions (for example if base station or access point breaks down or its maximum capacity is exceeded). The handover action can be for example triggered by the network, the mobile device or the user of the mobile device. A handover action may happen within the same access network, between access networks which may be of different types (so called heterogeneous access networks) or even between different core networks.

[0041] A Packet Data Protocol (PDP) context offers a packet data connection over which a mobile device and a network can exchange IP packets. To a PDP context belongs a data structure (or data record) including subscriber session related information for an active session (for example subscribers IP address, Tunnel end point identifier, subscriber identifier, …). Several PDP contexts can co-exist. The PDP context(s) is an important part of the connection. A PDP context can be activated (newly generated), modified (for example to change connection parameter like reserved connection resources) or deactivated.

[0042] A mobile device (MD) connects to the base station or access point of a network and may be a mobile phone, a Personal Digital Assistant (PDA), a portable computer, a

pager, a stationary device capable to access a wireless network or any kind of other device connecting via a radio interface to a wireless network. A stationary device could be for example a stationary computer connecting via a WLAN or HSPA dongle to a wireless network or a metering device connected to a wireless network and reporting for example events detected via sensors or acting on remotely received commands. One mobile device may have the ability to connect to several access points/networks in parallel at the same time.

[0043] A network element (for example the network element implementing the claimed invention) could be any network element located in the access or the core network. Synonyms used in the application and the claims for the term "network element" are the terms device, network device or apparatus. With respect to the present application a mobile device is not a network element.

[0044] A network management system (NMS) is a combination of hardware and software used to monitor and manage a network. Individual network elements within a network could be managed by a NMS.

[0045] A Policy and Charging Rule Function may be included in one or more core network element(s) housing policy and charging rules for a network (for example a PCRF).

[0046] Denial of Service (DoS) attacks or a distributed DOS attacks (DDoS) are attempts to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine, node or network with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted node(s) to reset, or consuming its resources that it can no longer provide its intended service, or obstructing

the communication media between the intended users and the targeted node so that the users can no longer communicate adequately with the target node or the network. DoS attacks might cause for example frequent handover actions, frequent attach or detach actions or frequent PDP context activation, modification or deactivation actions initiated by one or more mobile devices thus loading the involved access and/or core network nodes and so degrading the experienced network performance or availability of the normal network users. Loading of the network might happen for example on the user plane by reserving resources without using them, or on the control plane by generating extra traffic related to not needed actions caused by the DOS attack.

[0047] Frequent handover, frequent attach or detach or frequent PDP context activation, modification or deactivation actions mean in the context of this application abnormal frequent actions caused by for example a malicious user or malicious software performing a DOS attack to the network. Such actions will cause "frequent" changes to a connection between a mobile device and a network. An expert in the art is able to define criteria (for example thresholds for mobile device or network related parameters) in order to distinguish normal changes of a connection between a mobile device and a network from abnormal (frequent) changes caused by for example DOS attacks. Those criteria (thresholds) can then be used for defining policy rules to detect frequent changes to a connection caused by those frequent (abnormal) actions. For example a criteria could be the number of connection changes that happened during a specific time window. Within the description of this patent application the term "frequent changes to a connection" refers to changes caused by abnormal behavior (like for example by DOS attacks).

[0048] In general all shown figures relate to example embodiments of the present invention where one or more devices, preferably mobile devices (MDs) are causing changes to a connection between the mobile device(s) and one or more

networks. Those changes are detected by a network element based on the data provided and/or collected from other network elements and/or the mobile device(s). If the detected changes of the connection violate one or more defined policy rules related to the connection (for example to detect DOS attacks), measures may be initiated or taken to stop the "frequent" connection changes, to inform the users of the mobile device(s) or to inform the network operator (for example via the network management system) about the detected "frequent" changes to the connection.

[0049] The main advantages of the above outlined invention are that the consumption or reservation of network resources without purpose is avoided, decreasing of network performance (and so the decrease of user experience) in the network is avoided, possible network outages or unavailability due to overload situations caused by malicious frequent changes to mobile device connections to the network are avoided, DoS attacks are detected and alarmed and only malicious frequent changes to mobile device connections are detected and inhibited, while still allowing normal actions like normal handover, attach/detach pr PDP context activation/modification/ deactivation actions.

[0050] Fig. 1 shows a high level example network 1 where mobile devices 1-8 to 1-11 are connected via access networks 1-1 and 1-2 to a core network 1-3, and there to a core network element 1-4 (for example a mobility anchor). The shown connections between the network elements refer to user data connections.

[0051] The access networks 1-1 and 1-2 may be heterogeneous access network (like shown in fig 1) or may be access networks from the same type (not shown). Mobile devices 1-8 to 1-11 are connected to access points (AP) 1-6 or 1-7 of one of the 2 access networks 1-1 or 1-2. Access point 1-6 or 1-7 could be for example a base station, a WLAN hot spot or a DSLAM (in case that one of the access networks is a fixed

network and that the mobile device is a stationary device connected on the one hand to the fixed access network and on the other hand capable to connect to a wireless access network).

[0052] Mobile devices 1-8 to 1-11 might be in the range of both access points 1-6 and 1-7 as shown in fig 1. Therefore those mobile devices can establish connections with both access networks (assuming that the mobile devices support both access network types and possess valid credentials for accessing the networks).

[0053] When a mobile device is switched on it either selects manually or automatically one the available access networks and attach to it. If it is switched off it detaches automatically.

[0054] If an ongoing connection of a mobile device shall be shifted from one access network to another access network a so called handover action is initiated. A handover action might be initiated for various reasons like for example by movement of the mobile device, by the user of a mobile device, by resource optimization actions or any other actions to optimize load distribution in the network. As one example the need for a handover action may be detected if the radio signal received from the access point where the mobile device is currently connected to degrades.

[0055] The handover action may be performed and/or controlled by the mobility anchor node 1-4 in the core network, by access network elements or by the mobile device itself. If for example the mobile device just changes from one access point (AP) to another one in the same access network, the handover might be performed and/or controlled by a controller or gateway located in the access network (not shown). In another situation the mobile device may decide on a handover action based on mobility policies received from

core network, for example from Access Network Discovery and Selection Function (ANDSF).

[0056] Further on when a mobile device starts for example a GPRS connection, a PDP context will be activated (generated) including parameters related to the GPRS connection between the mobile device and for example a core network element like a GGSN. Those parameters related to the GPRS connection may be for example the subscribers IP address, subscriber identifier like International Mobile Subscriber Identity (IMSI) or Tunnel Endpoint Identifier(s) (TEIDs).

[0057] Compared to those reasonable and needed attach/detach, handover or PDP context activation/deactivation/modification actions as described above, unnecessary changes to a connection of a mobile device might be initiated, for example by a malicious mobile device software or any other means which can be used for initiating frequent - not needed - changes to the connection (for example frequent attach, detach, handover actions or actions related to activation, modification or deactivation of a PDP context). Reasons for such unnecessary changes to the connection might be for example DoS attacks towards the network(s) where the mobile device is connected to. DoS attack(s) might be for example coordinated between different mobile devices connected to the same network(s) which might be located in the same area or connected to the same cell. DoS attacks might be started at certain time points or time windows and are usually performed with the goal to disturb normal network operation, degrade network performance or even interrupt network operation.

[0058] One network element (for example the mobility anchor 1-4 shown in fig 1) collects information about changes to the connection of one or more mobile device. The information might be collected from data received or requested for example from the mobile devices, or from data received or requested from other network elements which are aware about

changes to the connection of a mobile device to a network (for example aware of attach/detach, handover or PDP context activation/modification/deactivation related actions). This network element might be either located in one of the access networks or in the core network. Alternatively the collection functionality might be distributed to two or more network elements, however a central network element for the collection of this kind of information is the preferred solution.

[0059] Further on the one or more network element might have also access to policy rules data. These policy rules could include rules related to frequent changes of the connection of one or more mobile devices (for example rules related to frequent attach/detach, handover or PDP context activation/modification/ deactivation actions) which are then used to check from the collected data if frequent changes to the connection of one or more mobile devices are detected. As an alternative the policy rules might be also configured or pre-programmed directly in the network element performing the detection (for example the mobility anchor 1-4). Possible detailed policy rules (criteria) for detecting frequent changes to the connection of at least one mobile device to a network, and parameters used for the detection, are described later with respect to the detailed description of figure 4. In addition information about measures to be performed if policy rules are violated might be provided together with the policy rule data.

[0060] Fig 2 illustrates another example network 2, showing network elements and logical connections between them concentrating on the transfer of information related to the detection of changes to the connection of one or more mobile device (like for example attach/detach, handover or PDP context related information) connected to the network.

[0061] The core network 2-2 and the access networks 2-3 and 2-4 are comparable to the ones shown in fig 1. Same applies

to the mobile devices 2-10 to 2-12 and the network element 2-6 acting as mobility anchor. In addition fig 2 shows a Policy and Charging Rules Function (PCRF) 2-5, which may provide policy rules 2-15, for detecting changes to network connections (for example caused by frequent abnormal actions), to one or more network elements detecting those changes (for example the mobility anchor 2-6). The policy rules might be either retrieved by the network element 2-6 from the PCRF 2-5 or they might be pushed by the PCRF to the network element. In addition to the policy rules also information about measures, to be performed if a policy rule is violated, might be provided by the PCRF. Instead of the PCRF providing the policy rules (and optionally the measures) they might be also located/stored in another network element or in the network element 2-6 itself.

[0062] Further on a Network Management System (NMS) 2-1 is shown in fig 2. The NMS provides for example configuration data 2-13 and 2-14 to the PCRF or the network element 2-6. This configuration data might be related to policy rules, for example policy rules for detecting frequent (abnormal) changes to the connection of at least one mobile device and optionally also to the measures that should be performed when a policy is violated. Further on the NMS 2-1 might receive 2-14 data and information from the network elements (for example the mobility anchor 2-6) or other network elements reporting information related to detected frequent changes to a connection directly (not shown) to the NMS 2-1. The mobility anchor 2-6 (or any other comparable network element collecting information related to the frequent changes of a connection) may receive policy rules for detecting frequent changes of a connection for example from the PCRF 2-5 or from the NMS 2-1.

[0063] Still further on fig. 2 shows also other network elements 2-7 to 2-9, which could be either located in one of the access networks 2-3 or 2-4 (for example a base station or access point), in the core network 2-2 (for example a SGSN)

or at the border between one of the access networks and the core networks as a binding network element between them. Those binding network elements could be for example a gateway network element or an access network controller (like a base station controller (BSC) or a radio network controller (RNC)).

[0064] Network elements 2-7 to 2-9 and the mobile devices 2-10 to 2-11 might receive configuration data from network element 2-6 (for example the mobility anchor 2-6 as shown in fig 2) or from the NMS directly (not shown). This configuration data might include potential measures applied to those network element and/or the mobile devices after detecting frequent changes to a network connection. Further on the network elements 2-7 to 2-9 and the mobile devices 2-10 to 2-12 might report information related to the connection of mobile devices (for example related to changes of the network connection) to the network element 2-6, to the NMS 2-1 directly (not shown) or to any other network element involved in the detection of frequent changes to the connection of at least one mobile device to the network.

[0065] The procedure for detecting frequent changes to the connection is the same as explained in the description related to fig 1, therefore it is not repeated here.

[0066] The network element 2-6 (for example a mobility anchor) may receive or pull information related to changes of the connection of the mobile devices from other network elements or the mobile devices. Based on this information the network element 2-6 checks if defined policy rules are violated in order to detect frequent changes of the connection. If frequent changes are detected this might be reported to the NMS 2-1 (for example in form of an alarm or performance data information which will be fetched from the NMS 2-1). Further on measures might be applied to the mobile devices or the network elements in order to stop not needed

frequent changes to the connection or to inform the user(s) of the mobile device(s) about it.

[0067] The PCRF 2-5 is just a preferred network element for providing policy rules (and optionally measures) related to the detection of the frequent changes. Basically those policy rules and measures might be also stored and provided by any other network element, or could be configured directly to the network element detecting the frequent changes (for example the mobility anchor 2-6).

[0068] The mobility anchor 1-3/2-6 shown in fig 1 and fig 2 is just a preferred network element for detecting frequent changes of the connection of at least one mobile device to the network. In principle the detection can be also done by any other network element or a group of network elements. If the detection is not done in the mobility anchor, the mobility anchor might need to transfer information/data related to changes of the connection to other network element(s) implementing the detection function.

[0069] Fig 3 and fig 4 illustrate flow diagrams of a method related to the present invention. Flow diagram boxes with dotted lines show optional elements while boxes with solid lines show mandatory elements. Elements included in a box with dotted lines are automatically optional, independent if they are shown with dotted or solid lines.

[0070] Turning to fig 3 which illustrates a high level flow diagram 3 of a method related to the present invention.

[0071] In a first step 3-1 one or more parameters are generated which are later on used to determine policy rule violations and as a consequence detecting frequent changes to a connection of at least one mobile device. The data needed to generate those parameters is either automatically received (for example periodically) or requested from mobile device(s)

3-4 or from other network elements 3-5. The generated parameters might depend on the applied policy rules (3-6).

[0072] The generated parameters may be specific parameters for a dedicated mobile device, for a group of mobile devices, for the whole network or for a part of the network (for example one or more cells of the network). Further on the parameters may include a time dimension, which means that the parameters are generated for data or events falling into a specific time window. The generated parameters are then transferred 3-10 to the second step 3-2. More details related to the generated parameters are described in connection with fig 4.

[0073] In a second step 3-2 the generated parameters will be evaluated together with one or more policy rule 3-6 to determine if a policy rule is violated and as a result detecting frequent changes to the connection of at least one mobile device connected to a network. Those policy rules might be either received from external (as shown in fig 3 by 3-6) or might be preconfigured. A time dimension (which might be part of the policy rule) may be taken into account when doing the evaluation (note, this is optional for step 3-2). If a violation of a policy rule is determined frequent changes to the connection are recognized and information about the violated policy rule is forwarded 3-11 to the third step 3-3. The forwarded information may include information about the violated policy rules, the one or more mobile devices which are violating the policy rule and the network or network portion where the violation was detected. More details about the policy rules are described in connection with fig 4.

[0074] In a third step 3-3 information about the violated policy rule(s) is received 3-11 and measures are selected and initiated to the at least one mobile device 3-7, to other network elements 3-8 or to the NMS 3-9. Information about the measures may be received from external 3-12, for example from

a PCRF or a NMS which might provide them together with the policy rules. Alternatively the measures may be pre-programmed. The other network elements may be network elements located in the core or access network(s) where the one or more mobile device is currently connected to, handed over to, tried to be handed over to or involved with for any of the previously mentioned actions. These network elements could be for example base stations, access points, base station controllers (RNC/BSC) or gateways. If the network element which has determined the violation of a policy rule is involved in the handover, attach/detach or PDP context activation/modification/deactivation action itself, measures might be also initiated or applied directly to the network element including the determining function. Initiated or applied measures could be for example blocking network access for an indefinite or limited time or informing the NMS or the user(s) of the mobile device(s) about the frequent actions. More details about possible measures are described in connection with fig 4.

[0075] Fig 4 shows a more detailed view on the steps of the flow diagram illustrated and described in connection with fig 3.

[0076] Details of the optional generation of parameters are shown in step 4-1. Received mobile device related data 4-4 may be for example indications of a performed or planned handover, attach/detach action or PDP context activation/modification/deactivation actions, optionally with timing information (like when has the action happened or when is it planned to happen). Further on information about the involved networks or network parts (for example cells) and the reasons for the action (for example initiated by the user, initiated by the device due to degrading radio signal or initiated by the by the network …) may be included.

[0077] The mobile device related data is processed in the "mobile device related parameters" sub-step 4-10, and

parameters like for example the number of completed actions 4-12 (for example handover actions, attach/detach actions, PDP context activation/modification/ deactivation actions), the duration of the last connection of a mobile device to a network 4-13 and the number of connection changes 4-14 of a mobile device to a network are generated. The mentioned parameters are just examples for parameters that can be used to detect frequent changes to the connection of at least one mobile device, therefore the mentioned list of mobile device parameters is not exclusive. Other possible parameters could be for example the amount of data transferred during a connection.

[0078] Mobile device related parameters 4-10 might be generated for a single mobile device or a group of mobile device. Further on the parameters might be generated for a defined time window, which means that only events falling into the sliding time window are counted. Different time windows might be defined for different parameters.

[0079] Received network related data 4-5 may include information related to handover actions, attach/ detach actions or PDP context activation/modification/ deactivation actions. Further on the data may include information about the involved one or more mobile devices, the network area or cell(s) where the actions occurred, the target and the originating networks involved in the actions (for example in case of handover actions) and other related data (for example the amount of transferred data during a connection). Further on information about the reason(s) for initiating the actions and timing information might be included. The network related data is processed in the "network related parameters" sub-step 4-11. Generated network related parameters may be the number of completed actions 4-20 for the total network or parts of the network 4-15, number of actions originated in the network or in parts of the network 4-16, number of actions targeted to the network or at least to parts of the network 4-17, number of actions originated in one cell of the

network 4-18 or number of actions targeted to one cell of the network 4-19. The mentioned parameters are just examples of parameters that may be used, therefore the mentioned list of network related parameters is not exclusive.

[0080] Network related parameters 4-11 might be generated for a defined time window, which means that only events falling into the sliding time window are counted. Different time windows might be defined for different parameters.

[0081] In general a selection of all the parameters to be generated in step 4-1 (mobile 4-10 and device related parameters 4-11) might depend from the policy rules 4-6 to be used for detecting frequent changes to the connection of at least one mobile device to a network.

[0082] The one or more time windows mentioned for the generation of the mobile device or network related parameters might be pre-configured, could be configured on the fly (for example via a network management system - not shown) or could be extracted from the policy rules 4-6. Further on defined time windows might be modified if frequent actions were detected (for details refer to the description related to initiating measures step 4-3 of fig 4 below).

[0083] The generated one or more parameters are forwarded 4-40 from the generating parameter step 4-1 to the determining policy rule violation step 4-2.

[0084] In the determining policy rule violation step 4-2 the received parameters 4-40 are processed together with policy rules in order to detect policy rule violations indicating frequent changes to a connection. Policy rules might be either pre-programmed or received from external (for example from PCRF or a NMS as shown in fig 2). Different policy rules might apply for different areas or groups (for example for detecting frequent changes of a connection of a single mobile device or of a group of mobile devices, or for detecting

frequent changes of one or more connections in a network or in parts of a network …) or might be related to a combination of those. Within one area or group one or more criteria (for example number of completed handover actions, number of attach/detach actions, number of PDP context activations/modifications/ deactivations, duration of a connection, number of handover actions originated in a cell …) might be used within one policy rule.

[0085] A policy rule might include one or more thresholds for one or more parameter. A device may be assumed to violate a policy if one or more of those thresholds are crossed. A timing window (comparable to the one used in step 4-1) can be applied also for a policy rule. A policy rule might include AND, OR, less than, more than, equal and other operations for different parameters and related thresholds. The thresholds itself might be part of the policy rules.

[0086] Example of a policy rule:

Parameters:

- A = number of completed handover actions of mobile one device
- B = Duration of last network connection of the mobile device

Policy rule:
IF ((within TW (A>5)) and (B<10s)) THEN policy_rule = VIOLATED

TW = time window = e.g. 1 minute

[0087] In the above example "5" is the threshold for the number of the completed handover actions and "10s" is the connection time threshold.

[0088] Determining frequent changes to the connection might happen utilizing several policy rules, which might be related to different parameters or different combination of parameters, in parallel as shown in step 4-2 (see 4-21, 4-22 and 4-23).

[0089] The result of the different policy rule checks 4-21 to 4-23 may be transferred separately to the initiating measures step 4-3, or may be combined to a single indication (not shown in fig 4) by logical AND/OR operations of the one or more policy rules. In addition information about which policy rule is violated, which threshold are when crossed and how much it is exceeded might be transferred in 4-41 together with the result(s) from the policy rule check to step 4-3.

[0090] The initiating measures step 4-3 checks the result from the determining policy rule violation step 4-2 and may initiate or apply at least one measure accordingly. The at least one measure might dependent from the violated policy rule (and related parameters and information received from 4-2 as described in the previous paragraph) and might be either pre-programmed or received from external 4-43, for example together with the related policy rules 4-6 possibly from a PCRF. Alternatively the measure(s) might be requested on demand 4-43 from an external network element. The measure(s) might be applied to a network element involved in the action(s) causing the frequent changes to a connection 4-8 (for example to a base station or base station controller for blocking mobile device access to the network 4-31), a network element storing the policy rules 4-42 (for example the PCRF in fig 2 or the network element performing the determining step 4-2 if the policy rules are stored there), a network management system (NMS) 4-9 or to at least one mobile device 4-7 (for example sending a message to the mobile device(s)). If coordinated frequent actions of a group of mobile devices are detected then also the measure(s) may be initiated or applied for/to the whole group of mobile devices.

[0091] Possible measures may be rejecting changes to connection related parameters 4-38 (for example modifying a PDP context), informing the network management system (NMS) 4-37 (for example by raising an alarm or providing status information which can be read be the NMS), blocking network access for the mobile device 4-31, modifying policies 4-32 (these could be policies related to the policy rules for detecting frequent changes to a network connection of a device or network access policies stored in the mobile device), sending messages to the mobile device(s) 4-33 informing the user(s) about the detected frequent changes to the connection, rejecting further handover request from the mobile device(s) 4-34, constraining the list of available networks for handover 4-35 and blocking network access for at least one application 4-36.

[0092] A time window for applying the measure(s) might be defined, thus for example the blocking of network access for one or more mobile devices might be limited to a certain time. The time window might be common for several measures or could be specific for only one measure.

[0093] Fig 5 shows a network element 5-1 implementing the present invention of detecting frequent changes to a connection of at least one mobile device to a network. The network element 5-1 might be either a dedicated network element for the shown functionality or it might be integrated into another network element (for example to a PCRF or a Packet Data Network Gateway).

[0094] The network element 5-1 may receive data from the at least one mobile device 5-6 or from other network elements 5-7 involved in or observing actions related to changes of the connection of at last one mobile devices to a network (for example handover, attach/ detach actions or PDP context activation/modification/ deactivation) and generates in a generating block the needed parameters as described in detail with respect to fig 4 step 4-1. Alternatively those

parameters might be generated external from the network element 5-1 and might be provided to the network element either on request, on a periodic basis or in real time (refer to 5-8 and 5-9). A logical OR selection 5-3 shown in fig 5 underlines the options, however the OR function might not be part of the network element 5-1.

[0095] Independently if the parameters are generated by the network element 5-1 internally or received from external, those parameters are fed into a determining block 5-4 which might also receives policy rules 5-10 and performs a policy rule check taking those parameters into account. Alternatively to receiving the policy rules from external the policy rules might also pre-configured (not shown) in the network element 5-1, for example pre-configured by a network management system (refer to fig 2 and the related sections of the description). The determination if one or more policy rules are violated happens as described for fig 4 step 4-2. The result is forwarded to the initiating measures block 5-5.

[0096] The initiating measures block 5-5 initiates or applies measures according to the determination results provided by block 5-4. Those measures could initiated or applied for example to the network element storing the policy rules 5-42 (for example a PCRF), to at least one mobile device 5-11, to other network element 5-12 or to a network management system (NMS) 5-13. The measures might be either pre-programmed or received from external 5-44 (for example from a PCRF or a NMS). The measures might be provided together with the policy rules to the network element, however they might be also requested by the network element on demand from the external network element. The initiated or applied measures as described with respect to fig 4 step 4-3 apply also to the initiating measures block 5-5 and are therefore not described here in detail again. The initiating measures block 5-5 might be included in the element 5-1 as shown in fig 5, or it might be part of an external network element (not shown). If the initiating measures block 5-5 is

not part of network element 5-1 the results from the determining block 5-4 will be output 5-43 from network element 5-1 and transmitted towards a network element including the initiating measures block functionality.

[0097] Fig 6 shows a signaling diagram related to an example embodiments of the present invention. The signaling diagram 6 describes a standard 3GPP attach procedure of a mobile device 6-1 via a non-3GPP IP access network 6-2 to a network. The standard attach procedure is extended by one element 6-16 related to the present invention and certain additions are proposed to already existing steps and network element as described below.

[0098] Further shown network elements are the following 3GPP core network elements:

- a Packet Data Network Gateway 6-3 (PDN-GW)
- a visited network Policy and Charging Rule Function 6-4 (vPCRF)
- a visited network Authentication, Authorization and Accounting proxy server 6-5 (AAA Proxy)
- a home network PCRF 6-6 (hPCRF)
- a home network Home Subscriber Server (HSS) / AAA server 6-7).

[0099] A DoS Attack Recognition Function (DARF) 6-16 is introduced which includes functionality related to parts of the present invention for detecting frequent changes to a connection of one or more mobile devices to a network. The DARF function might be a stand alone element or might be integrated into another network element as for example shown into the PDN-GW 6-3.

[00100] Only the steps important for the invention will be described in connection with figure 6, parts of the signaling diagram that reflects standard (known) functionality will be only roughly or not at all described.

[00101] First the mobile device 6-1 performs together with the trusted non-3GPP IP access network 6-2 initial layer 2 procedures 6-11 to initiate the setup of a connection. In next steps 6-12 and 6-13 the mobile device is authenticated. If a frequent change to the connection of the mobile device has been recognized earlier (for example a DoS attack which caused frequent attach/detach actions) the HSS/AAA server may be aware about it (the HSS/AAA server might have been informed about it via measure 4-8 of fig 4). The HSS/AAA server may then reject the request at this stage (not shown) or inform the mobile device about it (not shown).

[00102] If the authentication and authorization was successful the mobile device triggers a layer 3 attach action 6-14. The proxy binding update message 6-17 may be then used as an indication for the Packet Data Network Gateway 6-3 (PDN-GW) to perform a check in order to detect frequent changes to the connection of the mobile device. The PDN-GW might obtain related information (for example policy rules and related measures) from the PCRF in step 6-18. Via the DoS Attack Recognition Function (DARF) 6-16, which implements the detection functionality for detecting frequent changes to a connection, the PDN-GW performs a corresponding check. If frequent changes to the connection are detected the PDN-GW 6-3 might report this in step 6-19 to the HSS/AAA server 6-7 (for example by applying a measure to the HSS/AAA server 6-7 to reject future attach requests from this mobile device). In step 6-20 the PDN-GW may then reject the current connection request of the mobile device 6-1.

[00103] If no frequent changes to the connection of the mobile device are detected in step 6-16 the attach procedure is continued in steps 6-21 and 6-22 and finalized in step 6-23.

[00104] It should be noted, that a similar diagram could be drawn also for the detach case. If multiple mobile devices perform a coordinated attach this may be detected by the DARF

function 6-16 by correlating the result from the checks performed for several mobile devices.

[00105] Turning now to figure 7 showing another signaling diagram related to another example embodiment of the present invention. The signaling diagram 7 describes a standard 3GPP handover procedure of a mobile device 7-1 from a 3GPP access 7-8 to a trusted non-3GPP IP access network 7-2. The standard handover procedure is extended by one element 7-16 related to the present invention, and certain additions are proposed to already existing steps and network element as described below.

[00106] Further shown network elements are the following 3GPP core network elements:

- a Packet Data Network Gateway 7-3 (PDN-GW)
- a visited network Policy and Charging Rule Function 7-4 (vPCRF)
- a visited network Authentication, Authorization and Accounting proxy server 7-5 (AAA Proxy)
- a home network PCRF 7-6 (hPCRF)
- a home network Home Subscriber Server (HSS) / AAA server 7-7).
- a 3GPP access network 7-8
- a Mobility Management Entity (MME) / Serving GPRS Support Node (SGSN) 7-9
- Serving Gateway 7-10

[00107] A DoS Attack Recognition Function (DARF) 7-16 is introduced which includes functionality related to parts of the present invention for detecting frequent changes to a connection of one or more mobile devices. The DARF functionality might be a stand alone element or might be integrated into another network element as for example shown into the PDN-GW 7-3.

[00108] Like in fig 6 only the steps important for the invention are described in connection with figure 7, parts of

the signaling diagram that reflects standard (known) functionality will be only roughly or not at all described.

[00109] Instead of fig 6 the mobile device 7-1 has already established a connection 7-11 via the trusted 3GPP access network 7-8, the serving GW 7-10 and the PDN-GW 7-3. Now the mobile device 7-1 discovers a trusted non 3GPP access network 7-2 and initiates a handover action 7-12.

[00110] In next steps 7-13 and 7-14 the mobile device is authenticated via the trusted non 3GPP access network 7-2. Like in fig 6 HSS/AAA server may reject the request at this stage (not shown) if a frequent change to the connection of the mobile device has been recognized earlier (for example caused by earlier frequent handover actions).

[00111] If the authentication and authorization was successful the mobile device triggers a layer 3 attach action 7-15. The proxy binding update message 7-18 may be used as an indication for the Packet Data Network Gateway 7-3 (PDN-GW) to perform a check in order to detect frequent changes to the connection of the mobile device 7-1. The PDN-GW might obtain related information (for example policy rules and related measures) from the PCRF in step 7-19. Via the DoS Attack Recognition Function (DARF) 7-16 the PDN-GW performs a check in order to detect frequent changes of the connection of the mobile device 7-1. If frequent changes to the connection are detected (for example frequent handover actions) the PDN-GW 7-3 might report this to the HSS/AAA server (not shown). As a result the PDN-GW may then reject the current connection (handover) request of the mobile device in step 7-21.

[00112] If no frequent changes to the connection of the mobile device are detected in step 7-16 the handover procedure is continued via steps 7-20 to 7-26 until it has been successfully completed.

[00113] If multiple mobile devices perform a coordinated DOS attack this could be detected by the DARF function 7-16 by correlating the result from the checks performed for several mobile devices.

[00114] Figure 8 shows a third signaling diagram related to another example embodiment of the present invention. The signaling diagram 8 describes a standard 3GPP PDP context modification procedure initiated by the mobile device 8-1 or the user of the mobile device (not shown). The standard PDP context modification procedure is extended by one element 8-7 related to the present invention.

[00115] Following network elements are shown in fig 8:

- Mobile device (MD) 8-1
- Base Transceiver Station 8-2
- Mobility Management Entity (MME) 8-3
- Serving Gateway (SGW) 8-4
- Packet Data Network Gateway (PDN-GW) 8-5
- Policy and Charging Rule Function (PCRF) 8-6

[00116] A DoS Attack Recognition Function (DARF) 8-7 is introduced which includes functionality related to parts of the present invention for detecting frequent changes to a connection of one or more mobile devices connected to a network. The DARF functionality might be implemented in a stand alone network element or might be integrated into another network element as for example shown integrated to the PDN-GW 8-5.

[00117] The mobile device 8-1 initiates the modification of an existing PDP context by issuing for example a request for a bearer resource modification 8-11 to the Mobility Management Entity (MME) network element 8-3 (the request could also include a modification request of any other parameter related to the connection or PDP context parameter). Such a request for a bearer resource modification 8-11 might request more resources (for example an increase of

the guaranteed bandwidth). The MME validates the request and sends a Bearer Resource Command message 8-12 to the selected Serving Gateway (SGW) 8-4.

[00118] The SGW sends the Bearer Resource Command message 8-13 to a Packet Data Network Gateway (PDN-GW) 8-5. The PDN-GW contacts 8-14 the PCRF 8-6 and may retrieve (beside other information) policy rules and optionally measures related to the detection of frequent changes to a connection between a mobile device and a network.

[00119] In a next step the DARF function 8-7 (which might be integrated into the PDN-GW) performs a detection check according to the present invention in order to identify frequent changes to a network connection (here frequent PDF context modifications). If frequent changes to a connection between the mobile device 8-1 and the network are detected, the request for bearer resource modification issued by the mobile device might be for example rejected (not shown), or any other measure might be applied (refer to the detailed description of figure 4 where several examples of possible measures are given).

[00120] If no frequent changes to the connection are detected by the DARF function 8-7, and if all other requirements are fulfilled (like for example sufficient available resources to handle the request), the PDP context might be modified according to the request 8-15 and the session modification ends with step 8-16.

[00121] Similar diagrams could be drawn also for the PDP context activation and deactivation cases. If multiple mobile devices perform a coordinated PDP context modification/activation/deactivation this may be detected by the DARF function 8-7 by correlating the result from the checks performed for several mobile devices.

[00122] The signaling diagrams shown in figures 6, 7 and 8 are just example diagrams shown 3 possible ways how the invention can be embodied into already existing procedures. Those signaling diagrams are not limiting the present invention to the shown networks or network elements.

[00123] Figure 9 shows a network element 9-1 implementing the present invention of detecting changes to a connection of at least one mobile device to a network. Compared to figure 5 this figures shows on a high level the software and hardware components where the invention (or at least parts of the invention) may be implemented. Such components may be a processor 9-2 (where a computer program which might implement parts of the invention may be running on), a memory 9-3 where the computer program may be stored in and where the process may fetch or deliver information/data from/to and other hardware and/or application logic (which might include for example the blocks shown in figure 5), where the application logic might interact with other network elements and/or mobile devices via at least one input 9-5 and at least one output 9-6. Alternatively the interaction with the external network elements/devices might happen also directly (not shown) via the processor 9-2.

[00124] Time aspects included in Figs. 1 to 9 do not restrict any one of the shown steps to be limited to the step sequence as outlined. This applies in particular to method steps that may be functionally disjunctive with each other.

[00125] Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is to detect changes to a connection of at least one mobile device to a network and to apply measures to the at least mobile device, network elements or a network management system after detecting changes of the connection. This may be done in order to prevent for example possible DOS attacks causing frequent changes to the connection.

[00126] Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware and application logic. The software, application logic and/or hardware may reside on one or more network element, network devices or apparatuses. If desired, part of the software, application logic and/or hardware may reside on one or more core network element and part of the software, application logic and/or hardware may reside on one or more access network element. In an example embodiment, the application logic, software or an instruction set is maintained on any one of various conventional computer-readable media. In the context of this document, a "computer-readable medium" may be any media or means that can contain, store, communicate, propagate or transport the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer, with examples of a computer described and depicted in Figure 9 in connection with the network element shown in Figure 5. A computer-readable medium may comprise a computer-readable storage medium that may be any media or means that can contain or store the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer.

[00127] If desired, the different functions discussed herein may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the above-described functions may be optional or may be combined.

[00128] Although various aspects of the invention are set out in the independent claims, other aspects of the invention comprise other combinations of features from the described embodiments and/or the dependent claims with the features of the independent claims, and not solely the combinations explicitly set out in the claims.

[00129] It is also noted herein that while the above describes example embodiments of the invention, these descriptions should not be viewed in a limiting sense. Rather, there are several variations and modifications which may be made without departing from the scope of the present invention as defined in the appended claims.

[00130] Reference signs included in the claims are added to show how the claims could be mapped to the example embodiments and are not limiting the scope of protection of the claims.

[00131] Used abbreviations:

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
ASN-GW	Access Service Network Gateway
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code division multiple access
DARF	DoS Attack Recognition Function
DoS	Denial of Service
DDoS	Distributed DOS
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data rates for GSM Evolution
EPS	Evolved Packet System
E-UTRA	Evolved Universal Terrestrial Radio Access
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GTP	Gateway Tunneling Protocol
GW	Gateway
IMSI	International Mobile Subscriber Identity
HO	Handover
HSS	Home Subscriber Server
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
LTE	Long Term Evolution
MD	Mobile Device

MME	Mobility Management Entity
NE	Network Element
NMS	Network Management System
PCRF	Policy and Charging Rule Function
vPCRF	visited PCRF
hPCRF	home PCRF
ePDG	Evolved Packet Data Gateway
PDA	Personal Digital Assistant
PDN-GW	Packet Data Network Gateway
PDP	Packet Data Protocol
PGW	PDN Gateway (PDN-GW)
PMIP	Proxy Mobile IP
QoS	Quality of Service
RAN	Radio Access Network
RNC	Radio Network Controller
SAE	System Architecture Evolution
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
TEID	Tunnel Endpoint Identifier
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS RAN
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks

CLAIMS:

1. A method for detecting changes to a connection of a mobile device (2-10) to a network (2-2), whereby the detecting is done by determining if at least one parameter related to the mobile device (4-10) or related to the network (5-9) is violating a policy rule (4-21) related to the changes, and if a policy rule is violated initiating at least one measure (4-3).

2. A method of claim 1 wherein the changes to the connection of the mobile device to the network are frequent attach or detach actions (6).

3. A method of claim 2 wherein the at least one parameter related to the mobile device contains
- number of completed attach actions of the mobile device (4-12) or
- number of completed detach actions of the mobile device (4-12) or
- duration of the last connection of the mobile device to the network (4-13) or
- number of connection changes to a network of the mobile device (4-14).

4. A method of claim 2 wherein the at least one parameter related to the network contains
- number of completed attach actions in the network (4-15) or
- number of completed detach actions in the network (4-15) or
- number of completed attach actions in at least one specific cell of the network (4-15) or
- number of completed detach actions in at least one specific cell of the network (4-15).

5. A method of claim 1 wherein the changes to the connection of the mobile device to the network are frequent handover actions (7).

6. A method of claim 5 wherein the at least one parameter related to the mobile device contains
- number of completed handover actions of the mobile device (4-12) or
- duration of the last connection of the mobile device to the network (4-13) or
- number of connection changes to a network of the mobile device (4-14).

7. A method of claim 5 wherein the at least one parameter related to the network contains
- number of completed handover actions in the network (4-15) or
- number of completed handover actions in a part of the network (4-15) or
- number of completed handover actions originated in at least one specific cell of the network (4-18) or
- number of completed handover actions originated in the network (4-16) or
- number of completed handover actions targeted to at least one specific cell of the network (4-19) or
- number of completed handover actions targeted to the network (4-17).

8. A method of claim 1 wherein the changes to the connection of the mobile device to the network are frequent Packet Data Protocol context activation or deactivation or modification actions (8).

9. A method of claim 8 wherein the at least one parameter related to the mobile device contains
- number of completed Packet Data Protocol context activation actions triggered by the mobile device (4-12) or
- number of completed Packet Data Protocol context deactivation actions triggered by the mobile device (4-12) or
- number of completed Packet Data Protocol context modification actions triggered by the mobile device (4-12) or

- duration of the last active Packet Data Protocol context of the mobile device (4-13) or
- number of changes related to Packet Data Protocol contexts of the mobile device (4-14).

10. A method of claim 8 wherein the at least one parameter related to the network contains
- number of completed Packet Data Protocol context activation actions in the network (4-15) or
- number of completed Packet Data Protocol context activation actions in at least one cell of the network (4-15) or
- number of completed Packet Data Protocol context deactivation actions in the network (4-15) or
- number of completed Packet Data Protocol context deactivation actions in at least one cell of the network (4-15) or
- number of completed Packet Data Protocol context modification actions in the network (4-15) or
- number of completed Packet Data Protocol context modification actions in at least one cell of the network (4-15).

11. A method of claim 1 wherein the changes to the connection of the mobile device to the network are at least one of
- changes to the reserved network resources of at least one part of the connection (8) and
- changes to at least one connection parameter related to the connection (8).

12. A method of any of the preceding claims wherein the policy rule is configurable and specific for the at least one parameter (3-6).

13. A method of any of the preceding claims wherein different policy rules can be configured for different mobile devices or different groups of mobile devices or

different groups of mobile users or different parts of the network (3-6).

14. A method of any of the preceding claims wherein the policy rule is violated if a threshold for the at least one parameter is passed within a defined period of time (4-21).

15. A method of any of the proceeding claims wherein the changes to the connection are caused by at least one of a malfunction of the mobile device, a denial of service attack and a user of the mobile device.

16. A method of claim 15 wherein the denial of service attack is caused by malicious mobile device software.

17. A method of any of the preceding claims wherein multiple mobile devices are performing changes to their connections in parallel.

18. A method of any of the preceding claims wherein the detection is performed by correlating at least one of the determination results and the selected parameters of at least two mobile devices (4-2).

19. A method of any of the preceding claims wherein the at least one measure is one of

- blocking access to the network (4-31) of the mobile device or
- rejecting further attach or detach or handover requests (4-34) of the mobile device or
- rejecting further Packet Data Protocol context activation, deactivation or modification requests (4-34) of the mobile device or
- rejecting further changes requested to at least one parameter of the connection (4-38) of the mobile device or
- constraining a list of available access networks (4-35) to the mobile device or

- modifying at least one policy rule used to detect the changes to the connection (4-32) of the mobile device or
- blocking network access for at least one application running on the mobile device (4-36).

20. A method of claim 19 wherein the at least one measure is only taken for a specific time.

21. A method of any of the claims 1 to 18 wherein the at least one measure is one of
- sending a message to the mobile device (5-11) and inform a user about the detected frequent changes to the connection (4-33) or
- sending a message to the mobile device asking for re-configuration of an access selection policy of the mobile device (4-32) or
- informing a network management system (4-37).

22. A network element for detecting changes to a connection of a mobile device (2-10) to a network (2-2), the network element comprising
a determining means (5-4) determining if at least one parameter related to the mobile device (5-8) or related to the network (5-9) is violating a policy rule (5-10) related to the changes and
a measure means initiating at least one measure (4-3) if a policy rule is violated.

23. A network element of claim 22 wherein the changes to the connection are frequent attach or detach actions (6).

24. A network element of claim 23 wherein the at least one parameter related to the mobile device contains
- number of completed attach actions of the mobile device (4-12) or
- number of completed detach actions of the mobile device (4-12) or

- duration of the last connection of the mobile device to the network (4-13) or
- number of connection changes to a network of the mobile device (4-14).

25. A network element of claim 23 wherein the at least one parameter related to the network contains
- number of completed attach actions in the network (4-15) or
- number of completed detach actions in the network (4-15) or
- number of completed attach actions in at least one specific cell of the network (4-15) or
- number of completed detach actions in at least one specific cell of the network (4-15).

26. A network element of claim 22 wherein the changes to the connection are frequent handover actions (7).

27. A network element of claim 26 wherein the at least one parameter related to the mobile device contains
- number of completed handover actions of the mobile device (4-12) or
- duration of the last connection of the mobile device to the network (4-13) or
- number of connection changes to a network of the mobile device (4-14).

28. A network element of claim 26 wherein the at least one parameter related to the network contains
- number of completed handover actions in the network (4-15) or
- number of completed handover actions in a part of the network (4-15) or
- number of completed handover actions originated in at least one specific cell of the network (4-18) or
- number of completed handover actions originated in the network (4-16) or
- number of completed handover actions targeted to at least one specific cell of the network (4-19) or

- number of completed handover actions targeted to the network (4-17).

29. A network element of claim 23 wherein the changes to the connection are frequent Packet Data Protocol context activation or deactivation or modification actions (8).

30. A network element of claim 29 wherein the at least one parameter related to the mobile device contains
- number of completed Packet Data Protocol context activation actions triggered by the mobile device (4-12) or
- number of completed Packet Data Protocol context deactivation actions triggered by the mobile device (4-12) or
- number of completed Packet Data Protocol context modification actions triggered by the mobile device (4-12) or
- duration of the last active Packet Data Protocol context of the mobile device (4-13) or
- number of changes related to Packet Data Protocol contexts of the mobile device (4-14).

31. A network element of claim 29 wherein the at least one parameter related to a network contains
- number of completed Packet Data Protocol context activation actions in the network (4-15) or
- number of completed Packet Data Protocol context activation actions in at least one cell of the network (4-15) or
- number of completed Packet Data Protocol context deactivation actions in the network (4-15) or
- number of completed Packet Data Protocol context deactivation actions in at least one cell of the network (4-15) or
- number of completed Packet Data Protocol context modification actions in the network (4-15) or
- number of completed Packet Data Protocol context modification actions in at least one cell of the network (4-15).

32. A network element of claim 22 wherein the changes to the connection are at least one of
- changes to the reserved network resources of at least one part of the connection (8) and
- changes to at least one parameter related to the connection (8).

33. A network element of any of the claims 22 to 32 wherein the at least one parameter is generated by a generating means (5-2) receiving data from the mobile device (5-6) or from at least one other network element (5-7).

34. A network element of any of the claims 22 to 33 wherein the policy rule is configurable and specific for the at least one parameter (3-6).

35. A network element of any of the claims 22 to 34 wherein different policy rules can be configured for different mobile devices, different groups of mobile devices, different groups of mobile users or different parts of the network (3-6).

36. A network element of any of the claims 22 to 35 wherein the policy rule is violated if a threshold for the at least one parameter is passed within a defined period of time (4-21).

37. A network element of any of the claims 22 to 36 wherein the detection is performed by correlating at least one of the determination results and the selected parameters of at least two mobile devices (4-2).

38. A network element of any of the claims 22 to 37 wherein the at least one measure is one of
- blocking access to the network (4-31) of the mobile device or
- rejecting further attach or detach or handover requests (4-34) of the mobile device or

- rejecting further Packet Data Protocol context activation, deactivation or modification requests (4-34) of the mobile device or
- rejecting further changes requested to at least one parameter of the connection (4-38) of the mobile device or
- constraining a list of available access networks (4-35) to the mobile device or
- modifying at least one policy rule used to detect the changes to the connection (4-32) of the mobile device or
- blocking network access for at least one application running on the mobile device (4-36).

39. A network element of claims 38 wherein the at least one measure is only taken for a specific time.

40. A network element of any of the claims 22 to 37 wherein the at least one measure is one of
- sending a message to the mobile device (5-11) and inform a user about the detected changes to the connection (4-33) or
- sending a message to the mobile device (5-11) asking for re-configuration of an access selection policy of the mobile device (4-32) or
- informing a network management system (4-37).

41. A network element of any of the claims 22 to 40 wherein the network is one of a core network (2-2), a 3GPP access network (2-3) and a non 3GPP access network (2-4).

42. A network element of any of the claims 22 to 41 wherein the changes to the connection are performed between at least two heterogeneous access networks (7).

43. A network element of any of the claims 22 to 42 wherein the network element (2-6) is one of a Policy and Charging Rules Function or a Packet Data Network Gateway or a Serving GPRS Support Node or a Mobility Management Entity or an evolved Packet Data Gateway.

44. A computer program comprising code for detecting changes to a connection of a mobile device to a network as claimed in any one of the claims 1 to 21 when the computer program is run on a processor.

45. The computer program according to claim 44, wherein the computer program is a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.

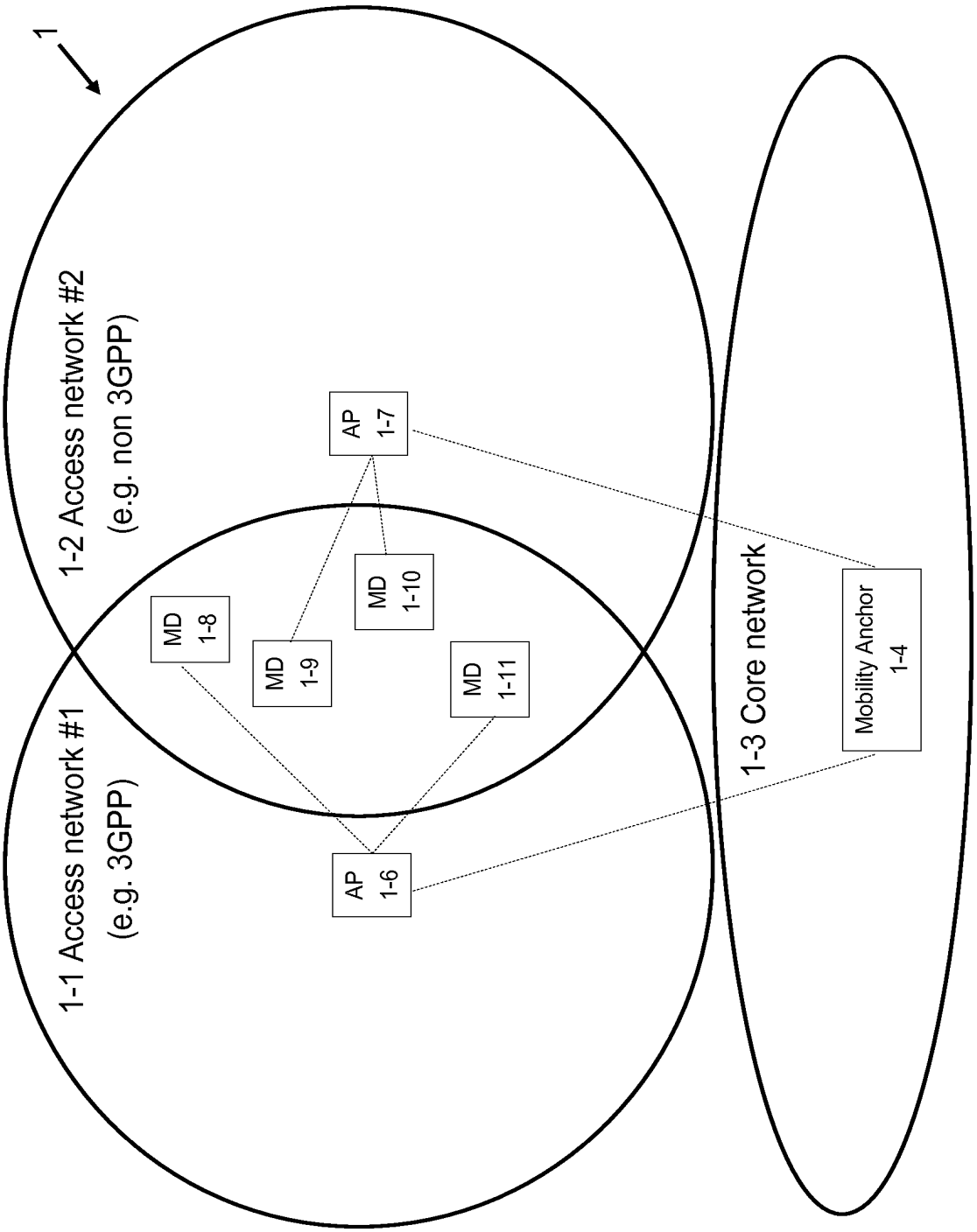

1
1-2 Access network #2
(e.g. non 3GPP)
1-1 Access network #1
(e.g. 3GPP)
1-3 Core network
AP
1-7
AP
1-6
MD
1-8
MD
1-9
MD
1-10
MD
1-11
Mobility Anchor
1-4

FIG 1

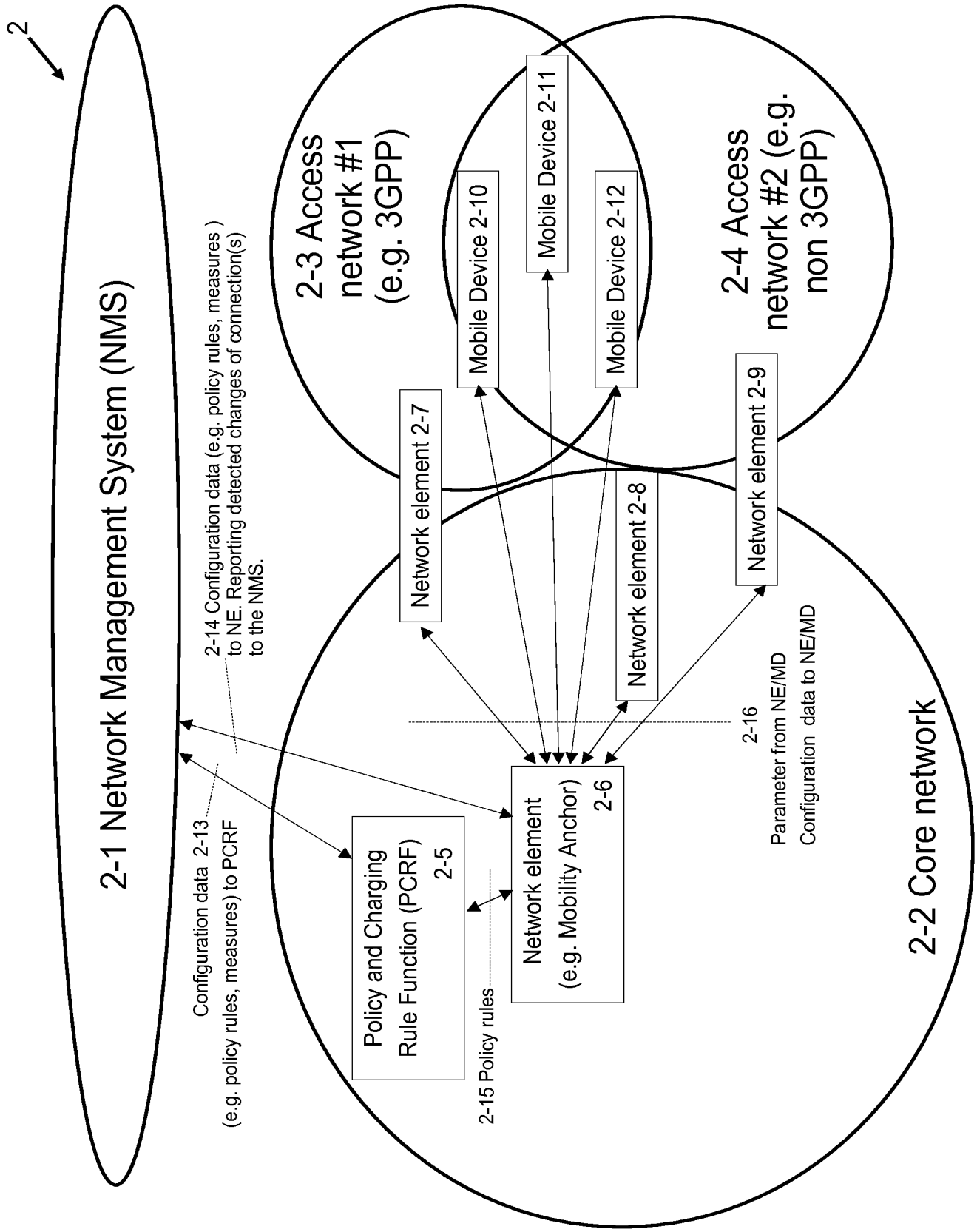

2
2-1 Network Management System (NMS)
2-14 Configuration data (e.g. policy rules, measures) to NE. Reporting detected changes of connection(s) to the NMS.
Configuration data 2-13 (e.g. policy rules, measures) to PCRF
2-3 Access network #1 (e.g. 3GPP)
2-4 Access network #2 (e.g. non 3GPP)
Mobile Device 2-10
Mobile Device 2-11
Mobile Device 2-12
Network element 2-7
Network element 2-8
Network element 2-9
2-16 Parameter from NE/MD Configuration data to NE/MD
Policy and Charging Rule Function (PCRF) 2-5
2-15 Policy rules
Network element (e.g. Mobility Anchor) 2-6
2-2 Core network

FIG 2

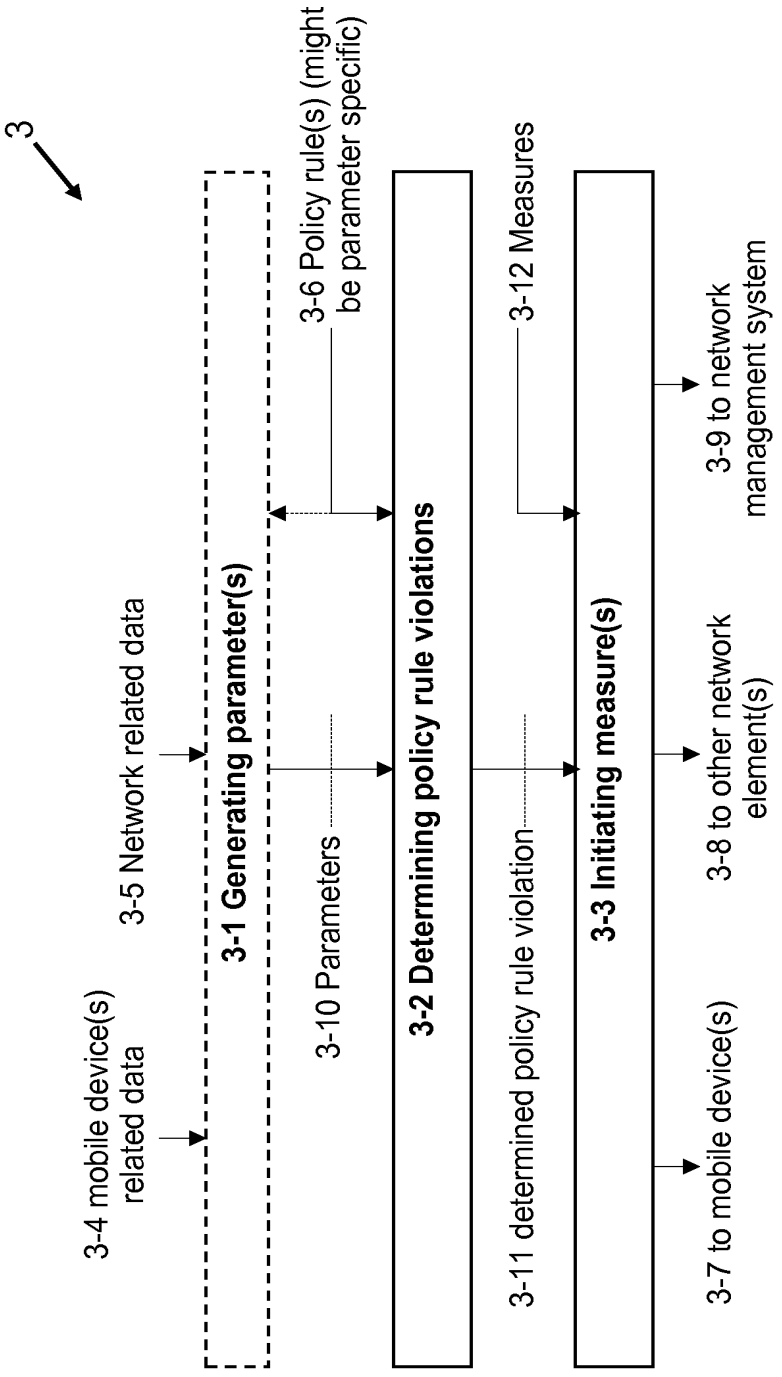

3
3-4 mobile device(s) related data
3-5 Network related data
3-1 Generating parameter(s)
3-6 Policy rule(s) (might be parameter specific)
3-10 Parameters
3-2 Determining policy rule violations
3-11 determined policy rule violation
3-12 Measures
3-3 Initiating measure(s)
3-7 to mobile device(s)
3-8 to other network element(s)
3-9 to network management system

FIG 3

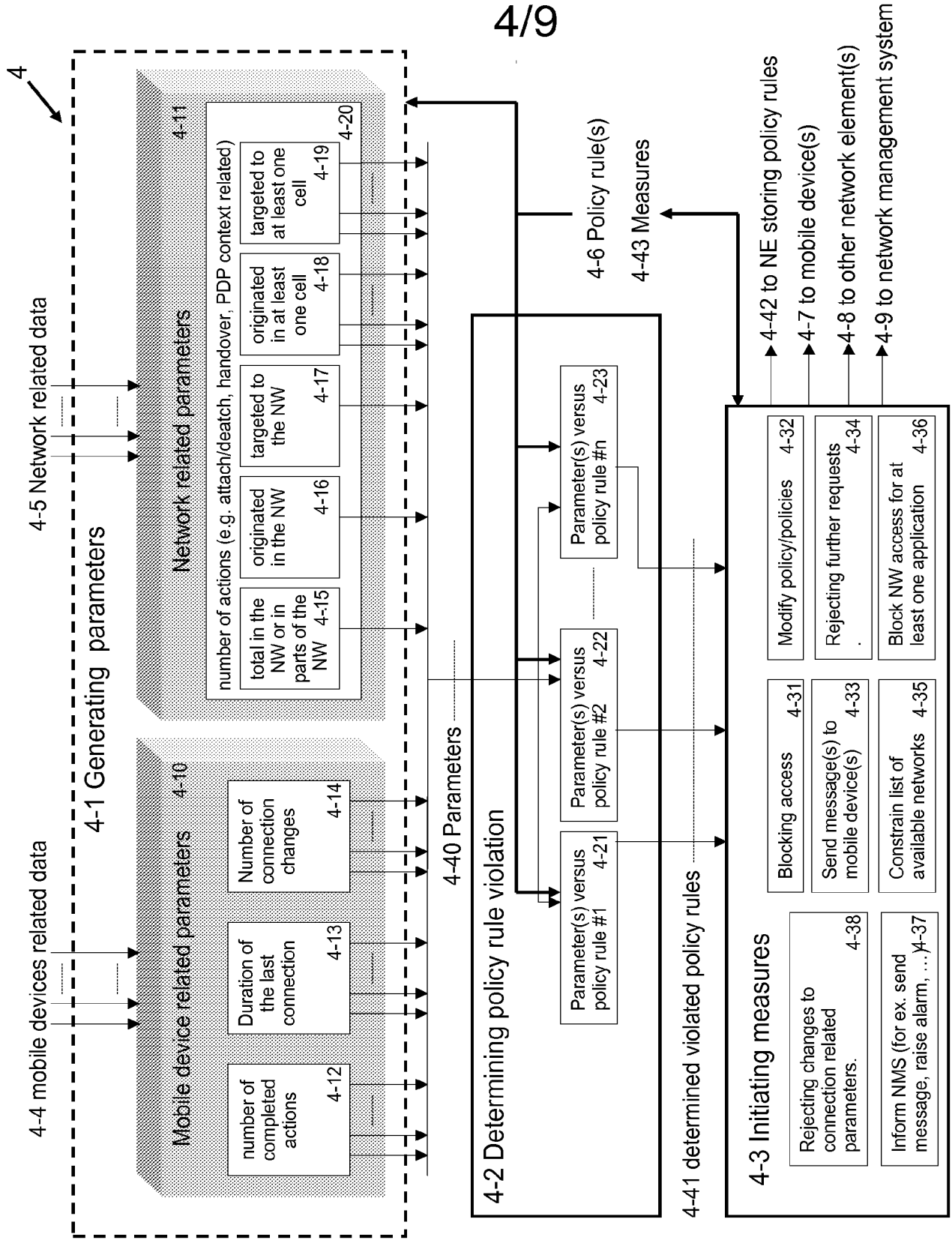

4
4-4 mobile devices related data
4-5 Network related data
4-1 Generating parameters
Mobile device related parameters 4-10
number of completed actions 4-12
Duration of the last connection 4-13
Number of connection changes 4-14
Network related parameters 4-11
number of actions (e.g. attach/deatch, handover, PDP context related)
total in the NW or in parts of the NW 4-15
originated in the NW 4-16
targeted to the NW 4-17
originated in at least one cell 4-18
targeted to at least one cell 4-19
4-20
4-40 Parameters
4-2 Determining policy rule violation
Parameter(s) versus policy rule #1 4-21
Parameter(s) versus policy rule #2 4-22
Parameter(s) versus policy rule #n 4-23
4-6 Policy rule(s)
4-43 Measures
4-41 determined violated policy rules
4-3 Initiating measures
Rejecting changes to connection related parameters. 4-38
Inform NMS (for ex. send message, raise alarm, ...)4-37
Blocking access 4-31
Send message(s) to mobile device(s) 4-33
Constrain list of available networks 4-35
Modify policy/policies 4-32
Rejecting further requests 4-34
Block NW access for at least one application 4-36
4-42 to NE storing policy rules
4-7 to mobile device(s)
4-8 to other network element(s)
4-9 to network management system

FIG 4

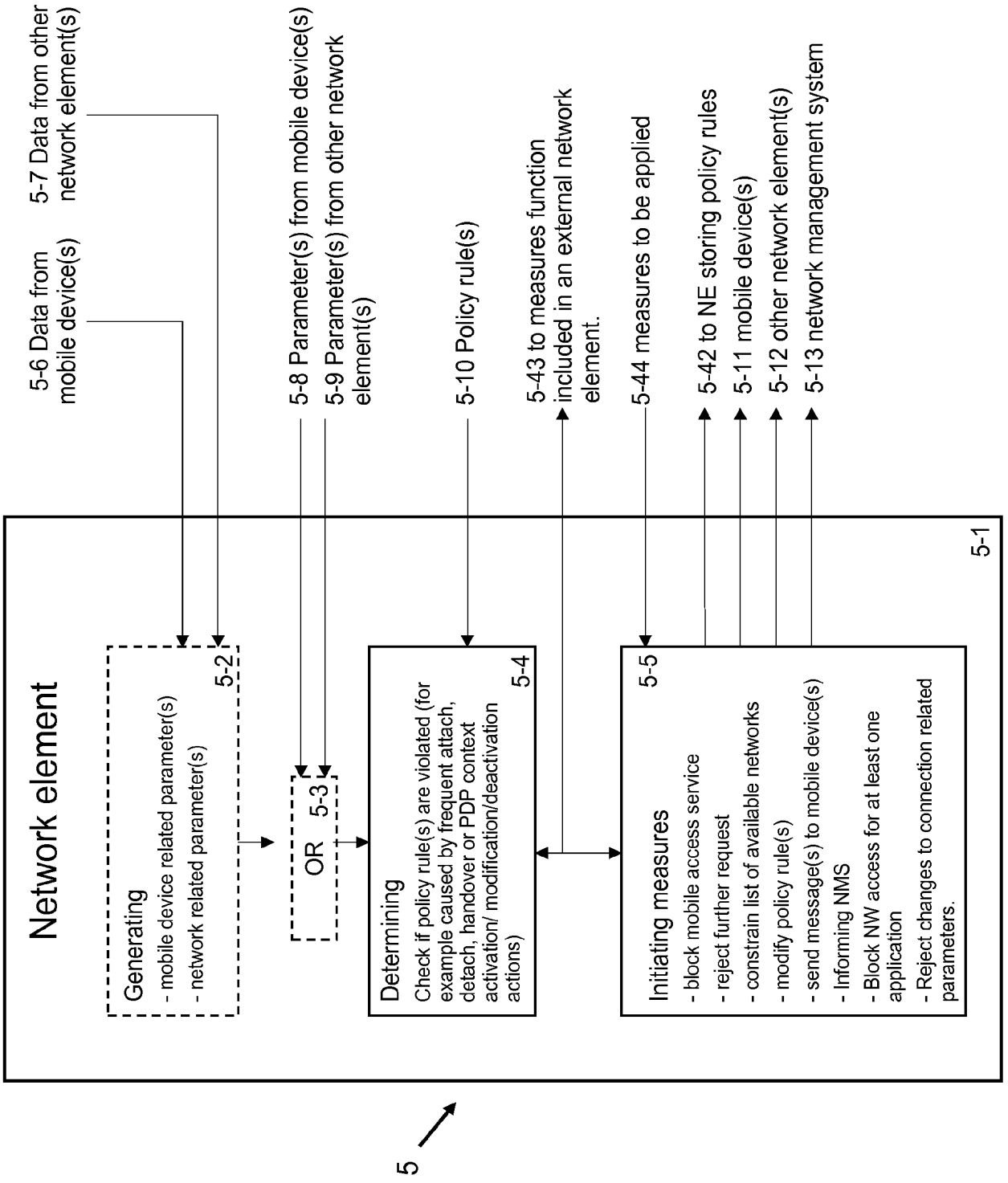

5-6 Data from mobile device(s)
5-7 Data from other network element(s)
5-8 Parameter(s) from mobile device(s)
5-9 Parameter(s) from other network element(s)
5-10 Policy rule(s)
5-43 to measures function included in an external network element.
5-44 measures to be applied
5-42 to NE storing policy rules
5-11 mobile device(s)
5-12 other network element(s)
5-13 network management system
Network element
Generating
- mobile device related parameter(s)
- network related parameter(s)
5-2
OR 5-3
Determining
Check if policy rule(s) are violated (for example caused by frequent attach, detach, handover or PDP context activation/ modification/deactivation actions)
5-4
Initiating measures
5-5
- block mobile access service
- reject further request
- constrain list of available networks
- modify policy rule(s)
- send message(s) to mobile device(s)
- Informing NMS
- Block NW access for at least one application
- Reject changes to connection related parameters.
5-1
5

FIG 5

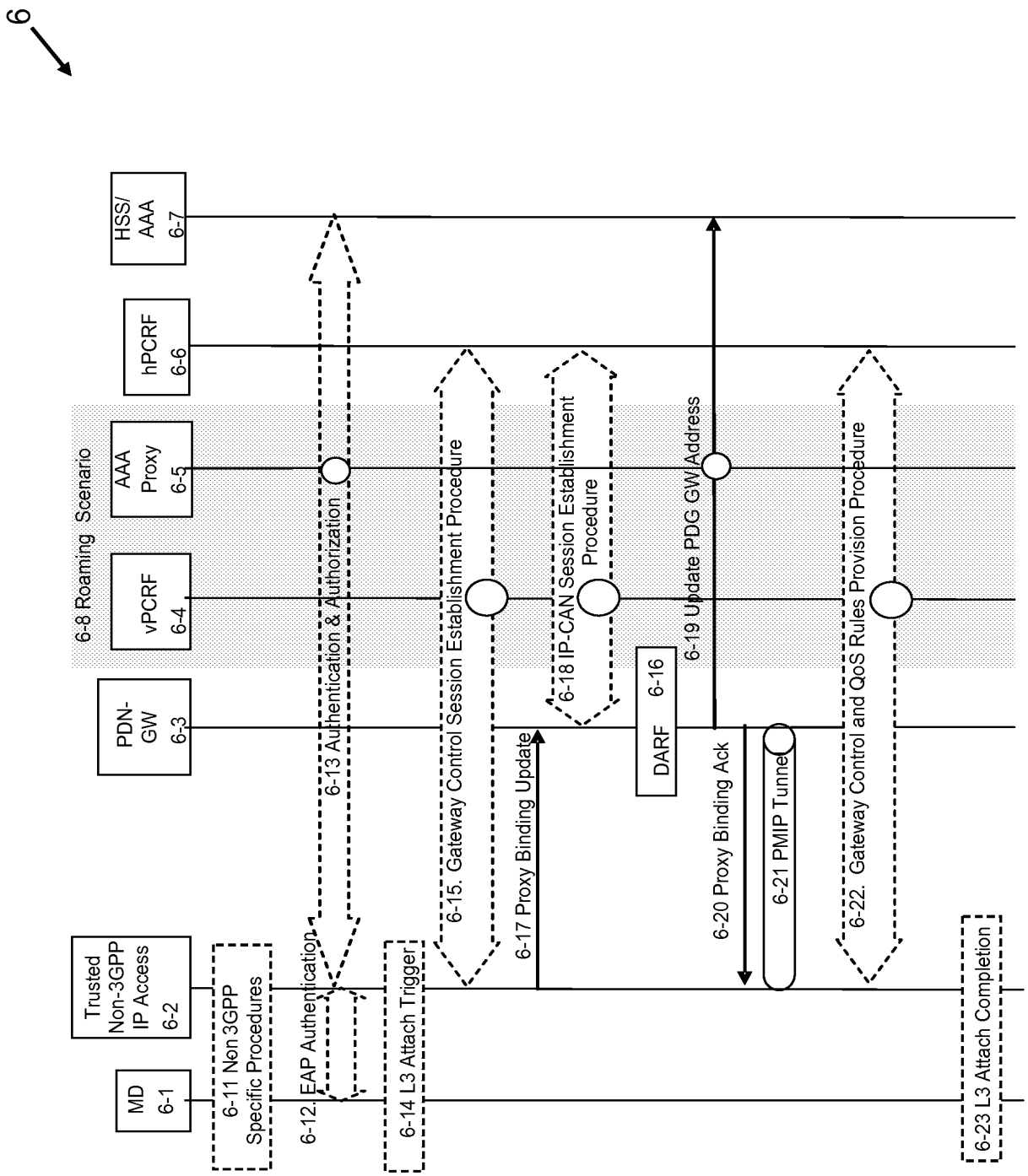

6
MD 6-1
Trusted Non-3GPP IP Access 6-2
PDN-GW 6-3
vPCRF 6-4
AAA Proxy 6-5
hPCRF 6-6
HSS/ AAA 6-7
6-8 Roaming Scenario
6-11 Non 3GPP Specific Procedures
6-12. EAP Authentication
6-13 Authentication & Authorization
6-14 L3 Attach Trigger
6-15. Gateway Control Session Establishment Procedure
6-17 Proxy Binding Update
6-18 IP-CAN Session Establishment Procedure
DARF 6-16
6-19 Update PDG GW Address
6-20 Proxy Binding Ack
6-21 PMIP Tunnel
6-22. Gateway Control and QoS Rules Provision Procedure
6-23 L3 Attach Completion

FIG 6

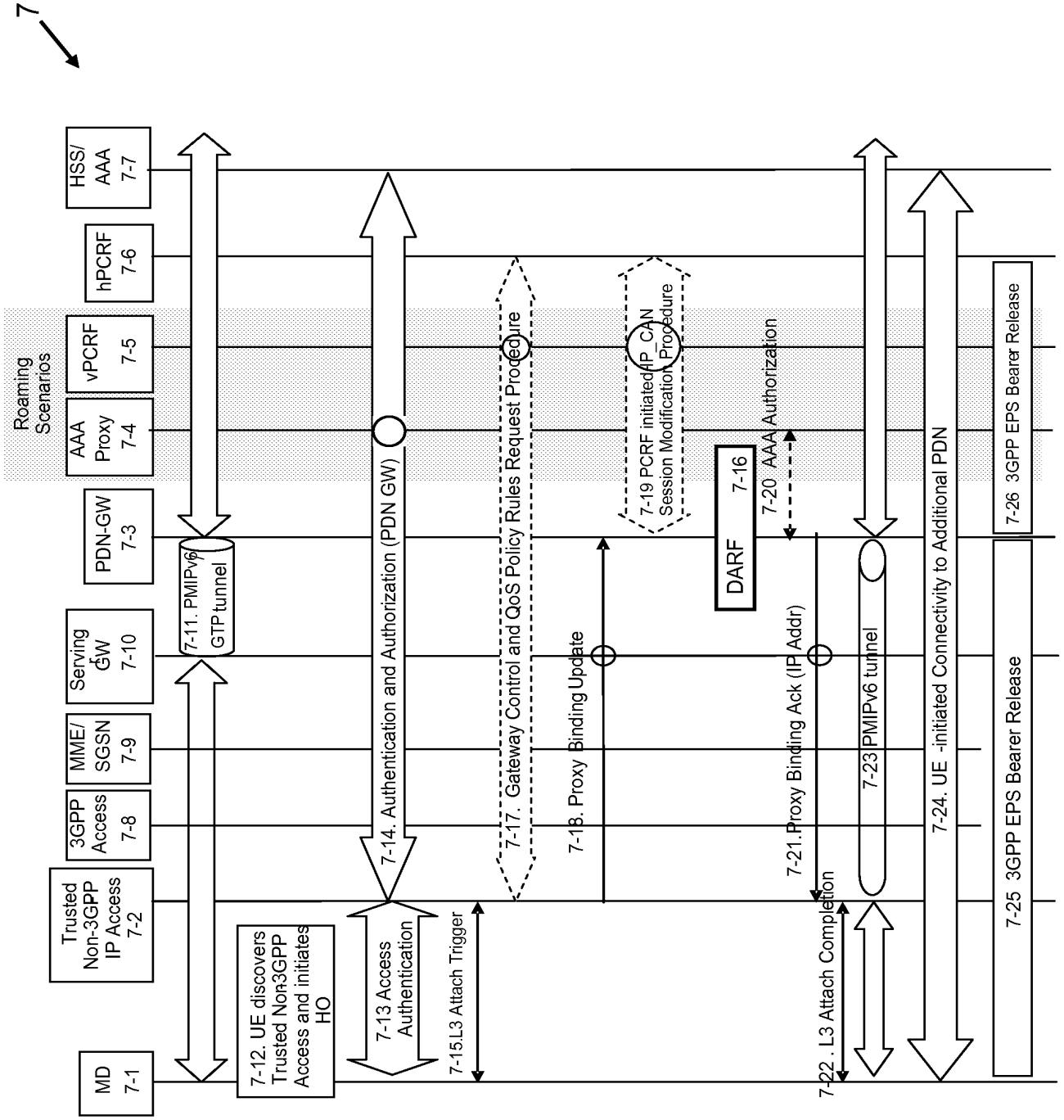

7
Roaming Scenarios
HSS/ AAA 7-7
hPCRF 7-6
vPCRF 7-5
AAA Proxy 7-4
PDN-GW 7-3
Serving GW 7-10
MME/ SGSN 7-9
3GPP Access 7-8
Trusted Non-3GPP IP Access 7-2
MD 7-1
7-11. PMIPv6 GTP tunnel
7-12. UE discovers Trusted Non3GPP Access and initiates HO
7-13 Access Authentication
7-14. Authentication and Authorization (PDN GW)
7-15.L3 Attach Trigger
7-17. Gateway Control and QoS Policy Rules Request Procedure
7-18. Proxy Binding Update
7-19 PCRF initiated IP CAN Session Modification Procedure
DARF 7-16
7-20 AAA Authorization
7-21. Proxy Binding Ack (IP Addr)
7-22 . L3 Attach Completion
7-23 PMIPv6 tunnel
7-24. UE -initiated Connectivity to Additional PDN
7-25 3GPP EPS Bearer Release
7-26 3GPP EPS Bearer Release

FIG 7

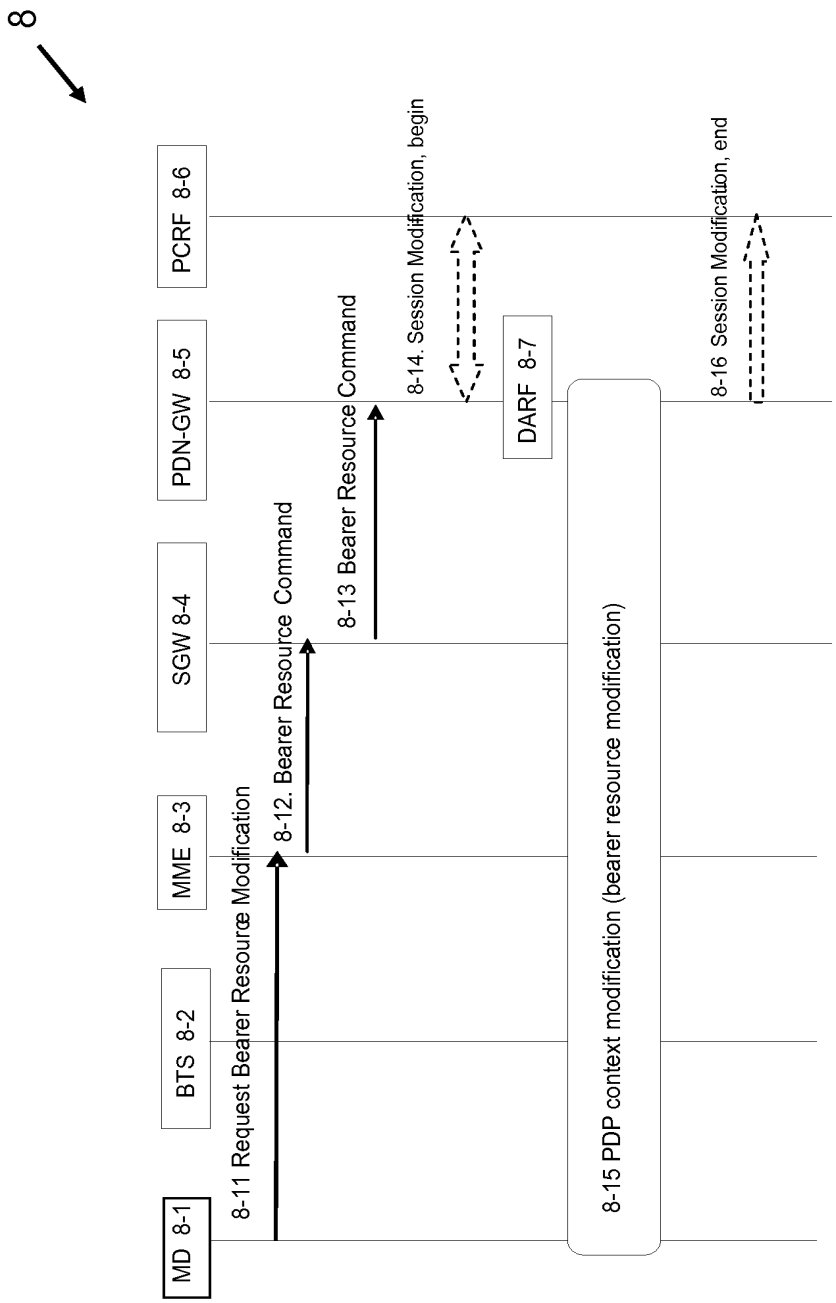

8
MD 8-1
BTS 8-2
MME 8-3
SGW 8-4
PDN-GW 8-5
PCRF 8-6
DARF 8-7
8-11 Request Bearer Resource Modification
8-12. Bearer Resource Command
8-13 Bearer Resource Command
8-14. Session Modification, begin
8-15 PDP context modification (bearer resource modification)
8-16 Session Modification, end

FIG 8

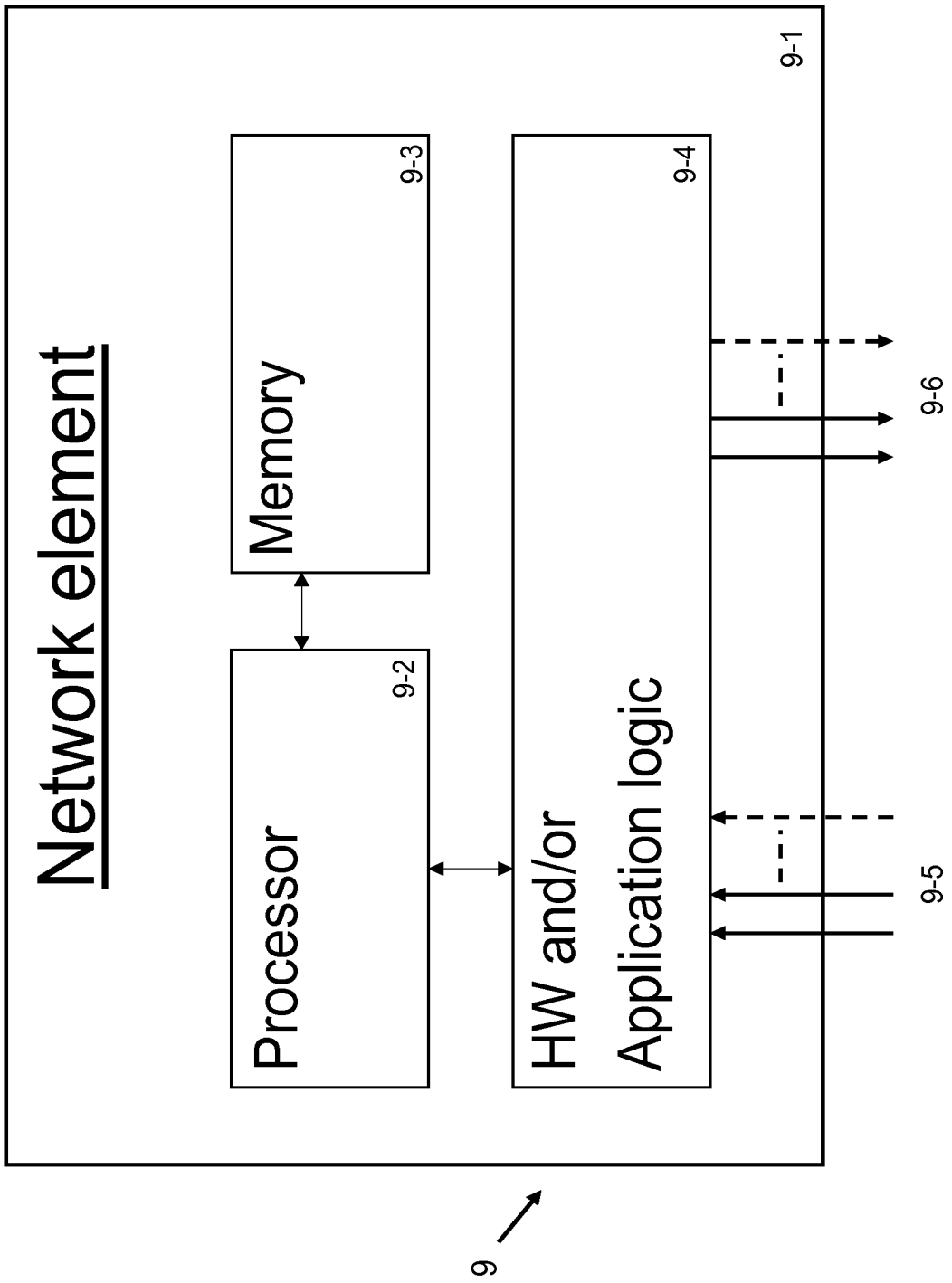

Network element
Memory
Processor
HW and/or
Application logic
9-1
9-2
9-3
9-4
9-5
9-6
9

FIG 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/067170

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/12
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, COMPENDEX, INSPEC, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/098610 A1 (HRASTAR SCOTT E [US]) 20 May 2004 (2004-05-20) * abstract paragraph [0029] - paragraph [0247] figures 1-14	1-45
X	US 6 779 120 B1 (VALENTE LUIS FILIPE PEREIRA [US] ET AL) 17 August 2004 (2004-08-17) * abstract column 4, line 14 - column 42, line 39 figures 1-5B	1-45

-/--

[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 October 2010	19/10/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Körbler, Günther

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

ERICSSON EXHIBIT 1005, Page 702

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/067170

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2008/066419 A1 (ERICSSON TELEFON AB L M [SE]; LIDSTROEM MATTIAS [SE]; MATTI MONA [SE];) 5 June 2008 (2008-06-05) * abstract page 1, line 5 - page 1, last line figures 1-6	1-45
X	US 2007/206552 A1 (YAQUB RAZIQ [US] ET AL) 6 September 2007 (2007-09-06) * abstract paragraph [0036] - paragraph [0097] figures 1-5	1-45
A	WO 2009/025601 A1 (ERICSSON TELEFON AB L M [SE]; KVERNVIK TOR [SE]) 26 February 2009 (2009-02-26) * abstract page 1, line 4 - page 33, line 17	1-45

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

ERICSSON EXHIBIT 1005, Page 703

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/067170

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004098610 A1	20-05-2004	NONE	
US 6779120 B1	17-08-2004	AU 2089301 A	24-07-2001
		WO 0152496 A2	19-07-2001
		US 2004250112 A1	09-12-2004
WO 2008066419 A1	05-06-2008	US 2010091671 A1	15-04-2010
US 2007206552 A1	06-09-2007	CA 2644151 A1	02-03-2007
		WO 2007103280 A2	13-09-2007
WO 2009025601 A1	26-02-2009	EP 2196037 A1	16-06-2010

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	1806	1	240	240
		Total in USD ($)		**240**

Electronic Acknowledgement Receipt

EFS ID:	38994990
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	27-MAR-2020
Filing Date:	21-MAY-2015
Time Stamp:	16:54:29
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$240
RAM confirmation Number	E20203QG54529541
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	15-686-WO-US_Information_Disclosure_Statement_27Mar20.pdf	1034334 02e2f90258ddd05083d208aa036fc5569624f423	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Foreign Reference	WO2011072719.pdf	2405774 0ab1458257767c076298f09d3f575d2eda384641	no	62
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30574 f5a959ba3922c880f6785052f8456b0da06a1b40	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3470682		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 15-686-WO-US

Application Number: 14/646,554

Filed: May 22, 2015

For: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

Art Unit: 2438

Examiner: Vu, Phy Anh Tran

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132490.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 59208.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David A. Grabelsky/ — Signature

July 28, 2020 — Date

David A. Grabelsky — Typed or printed name

312-913-3353 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
			Total in USD ($)	**600**

Electronic Acknowledgement Receipt

EFS ID:	40124450
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	System to Detect Behaviour in a Telecommunications Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	28-JUL-2020
Filing Date:	21-MAY-2015
Time Stamp:	13:51:24
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	E20207RD51495788
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	15-686-WO-US_Response_28Feb20_OA.pdf	239502 aa0294e7b8bb6e1e5534978697a578bb8fea222a	no	18
Warnings:					
Information:					
2	Extension of Time	15-686-WO-US_Petition_for_two-month_Extension_of_Time.pdf	188081 e31abe7f485e9599aeb79d2d8e54375c8c5beedc	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30713 7732a1a85f7e2d952e67b27f0c5ef32ff0f110e2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	458296		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADMARK OFFICE
(Attorney Docket No. 15-686-WO-US)

In re Application of: Frank Muller	)	**Examiner: Vu, Phy Anh Tran**
Serial No.: 14/646,554	)	**Art Unit: 2438**
Filed: May 22, 2015	)	**Confirmation No.: 4961**
Title: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK	)	

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

RESPONSE TO OFFICE ACTION MAILED FEBRUARY 28, 2020

In response to the Final Office Action mailed February 28, 2020, Applicant submits the following amendments and remarks. In addition, a Petition for Extension of Time under 37 C.F.R. § 1.136(a) (two-month), along with requisite fees. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Amendments to the Claims

1. (Currently amended) A system comprising:

a telecommunications network configured to identify at least one mobile telecommunications device and comprising a core network and a base station, wherein the base station is configured to receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network,[[; and]]

~~a hardware base station configured within the telecommunications network, wherein the base station is configured for receiving radio transmissions from mobile telecommunications devices, and for converting the received radio transmissions into signals, and for transmitting the signals into the telecommunications network;~~

~~wherein the telecommunications network is configured to identify at least one mobile telecommunications device and to receive a request from the mobile telecommunications device by way of the base station, and further to process the request into signaling internal to the telecommunications network,~~

wherein the telecommunications network is arranged to ~~monitor, in the signaling internal to the telecommunications network, for an~~ count in the core network a number of occurrences of a certain predetermined ~~data type~~ signal associated with the mobile telecommunications device, ~~and~~ the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals,

and wherein the telecommunications network is further arranged to register when the number of occurrences exceeds a level ~~for~~ indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

2. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to ~~monitor for~~ count in the core network the number of occurrences ~~of predetermined data type~~ by counting ~~that~~ a number of times the occurrence is detected when the occurrences ~~of the predetermined data type is detected in the signaling when the occurrences~~ exceed a predetermined temporal rate, and wherein the telecommunications network is further arranged to register when the number of the detected occurrences exceeds a predetermined threshold.

3. (Currently amended) The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences ~~of the predetermined data type in the signaling~~ when a time between a detected occurrence and the previously detected occurrence is within a predetermined time interval.

4. (Currently amended) The system according to claim 3, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of [[an]] the occurrence ~~of the predetermined data type~~ and further to start the timer, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following ~~detection of the predetermined data type occurs~~ occurrence is within the predetermined time interval T as measured by the timer.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

5. (Currently amended) The system according to claim 1, wherein the telecommunications network is further configured to detect when the occurrence[[s]] ~~in the signaling of the predetermined data type~~ exceeds a predetermined rate.

6. (Currently amended) The system according to claim 5, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of [[an]] the occurrence ~~of the predetermined data type~~ and further to start the timer, and wherein the telecommunications network is further arranged to calculate a rate as a ratio of a counted ~~detection~~ number of detected occurrences ~~of the predetermined data type~~ to time as measured by the timer.

7. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to register when the ~~occurrences of the predetermined data type~~ number exceeds the level for acceptable behaviour by setting a flag and/or starting a back off timer.

8. (Currently amended) The system according to claim 1, wherein the certain predetermined ~~data type~~ signal indicates attachment of the mobile telecommunications device to the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

9. (Currently amended) The system according to claim 1, wherein the certain predetermined ~~data type~~ signal indicates setting up of a bearer by the mobile telecommunications device.

10. (Currently amended) The system according to claim 1, wherein the certain predetermined ~~data type~~ signal indicates handover of the mobile telecommunications device.

11. (Currently amended) The system according to claim 10, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device and to register the number of occurrences ~~of data indicating handover~~ only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

12. (Currently amended) The system according to claim 1, wherein the telecommunications network is arranged to ~~monitor~~ count the number of occurrences in ~~the signaling of the predetermined data type in~~ a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

13. (Currently amended) The system according to claim 1, wherein the telecommunications network is further configured to:

identify at least one additional mobile telecommunications device,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

receive radio signals from the at least one additional mobile telecommunications device and to process these radio signals into ~~additional signaling internal to the telecommunications~~ processed signals and to transmit the processed signals to the core network,

count in the core network a number of occurrences of a certain predetermined signal associated with the at least one additional mobile telecommunications device, the certain predetermined processed signal representing an interaction between network devices for normal processing of signals,

~~monitor for an occurrence in the additional signaling internal to the telecommunications network of the predetermined data type and to~~ register when the ~~occurrences~~ number exceeds a level ~~for~~ indicating acceptable behaviour of the at least one additional mobile telecommunications device within the telecommunications network,

and wherein the telecommunications network is further arranged to aggregate the registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device.

14. (Canceled)

15. (Canceled)

16. (Currently amended) A method for detecting behaviour of a mobile telecommunications device in a telecommunications network comprising a core network, the telecommunications network including a base station, the method comprising:

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

at the base station, receiving radio ~~transmissions~~ signals from the mobile telecommunications device, ~~the received radio transmissions including a request~~ and processing the radio signals into processed signals and transmitting the processed signals to the core network;

~~at the base station, converting the received radio transmissions into signals, and transmitting the signals into the telecommunications network;~~

in the telecommunications network, identifying the mobile telecommunications device;

~~in the telecommunications network, receiving the request from the mobile telecommunications device by way of the base station, and processing the request into signaling internal to the telecommunications network;~~

~~in~~ the telecommunications network counting, ~~monitoring, in the signaling internal to the telecommunications network, for an~~ in the core network, the number of occurrences of a certain predetermined ~~data type~~ signal associated with the mobile telecommunications device, ~~and~~ the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals; and

registering when the number of occurrences ~~of the predetermined data type~~ exceeds a level ~~for~~ indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Remarks

1. Summary of the Office Action

In the Office Action mailed February 28, 2020 ("Current Office Action," hereinafter), the Examiner rejected claims 1 and 16 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph as allegedly being indefinite. The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by U.S. Patent Pub. No. 2006/0230450 (Bu). The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu, and rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of U.S. Patent No. 5,953,652 (Amin).

2. Status of the Claims

Currently pending are claims 1-13 and 16, of which claims 1 and 16 are independent, and the remaining claims are dependent. Applicant has amended various other claims as follows.

Applicant has amended claim 1 to describe the recited "base station" as being configured to "receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network," where the term "processed" distinguishes between "radio signals" received by the "base station" and those that the "base station" transmits to the "core network." Applicant has further amended claim 1 to replace "monitoring" with "counting," and applying the "counting" to "occurrences of a certain predetermined signal associated with the mobile telecommunications device," and describe the "certain predetermined signal" as "representing an interaction between network devices in the core network for normal processing of signals." Support for this amendment can be found generally throughout the original application, and specifically at least

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

at page 2, lines 17-21; page 3, lines 19-30 and lines 32-38; page 4, lines 35-37; page 5; page 8, lines 1-6; in the originally filed claims; and in Figure 1, for example.

Applicant has amended claim 16 in a manner similar to that of claim 1. Support for this amendment is generally the same as for the amendment to claim 1.

Applicant has amended each of claims 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13 to ensure consistency of antecedent basis with base claim 1.

No new matter has been introduced by way of any of the above amendments.

3. Response to Rejections under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph

The Examiner rejected claims 1 and 16 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph as allegedly being indefinite. Specifically, the Examiner asserted that is unclear what the term "representing" applies to, stating "[i]t is unclear what is representing an interaction between network devices in the core network." (Current Office Action, page 3.) Without acquiescing to the Examiner's assertion of indefiniteness, Applicant has amended claims 1 and 16, as described above, to describe the "certain predetermined signal" as "representing an interaction between network devices in the core network for normal processing of signals." Applicant submits that at least this amendment makes clear what it is that represents "an interaction between network devices in the core network for normal processing of signals." Accordingly, Applicant requests that the Examiner withdraw the rejections of claims 1 and 16 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph as allegedly being indefinite.

4. Response to Rejections under 35 U.S.C. § 102(b)

The Examiner rejected claims 1-3, 5, 7-10, 12-13, and 16 under pre-AIA 35 U.S.C. § 102(b) as being allegedly anticipated by Bu. Applicant submits that Bu fails to teach each and

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

every element set forth in any of claims 1-3, 5, 7-10, 12-13, or 16, and that these claims are allowable. Applicant starts by addressing claim 1, then subsequently addresses claims 2-3, 5, 7-10, 12-13, and 16.

Before discussing details, Applicant first summarizes the ways in which Bu fails to anticipate claim 1 as follows:

1) Bu does not *count* "signaling messages," but only *estimates* the signaling cost.
2) Bu does not count the number of occurrences of a "certain predetermined signal" associated with the *same* mobile telecommunications device whose behavior is determined, but estimates "signaling cost to data ratio" for a mobile device that receives data from a *different* mobile device that is the subject of behavior detection.
3) Bu does not count the number of occurrences of a "certain predetermined signal" associated with the mobile telecommunications device, but estimates *all* messages exchanged between a different mobile device and the core network.
4) Bu does not count *in the core network*, but estimates the number of messages exchanged between a different mobile device and the core network, which includes the messages between the base station and the different mobile device – i.e., Bu's estimate include messages that are *not* between network devices in the core network.
5) Bu does not teach: "wherein the telecommunications network is further arranged to register when the number of occurrences exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network."

Applicant first summarizes the fundamental bases and principles of Bu that are relevant to the rejections in the Current Office Action, and the manner in which the Examiner appears to have miscomprehended Bu's teachings.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

1) Bu teaches *ESTIMATING* signaling costs *from data traffic arrival patterns.* Bu does *not* teach counting or monitoring signaling messages.

Applicant respectfully submits that assertions by the Examiner to the contrary appear to be based on *a fundamental technical miscomprehension and/or erroneous technical analysis of Bu's teachings*. Specifically, the Examiner has cited to paragraphs [0024]-[0026] in Bu as teaching "at least 24 signaling messages" required to set up a "radio access bearer (RAB)." (Current Office Action, page 4.) But as Applicant has pointed out in more than one previous Office Action Response, Bu's teachings in paragraphs [0024]-[0026] serve to explain signaling protocols – that is, what signals are *specified to be used* when an RAB is set up or torn down. There *is no teaching* in paragraphs [0024]-[0026] or anywhere else in Bu of actively monitoring signaling messages when an actual set-up or tear-down of an RAB takes place.

Further, the Examiner cited to paragraphs [0054]-[0056] in Bu as teaching "[i]n order to determine the signaling cost to data ratio, the wireless network tracks **(monitors)** the number of signaling messages **(signals)** that are required in order to establish a dedicated channel to transmit the packet, and compare the number of signaling messages required to the amount of data in the packet." (Current Office Action, page 5; emphasis in original.) Applicant respectfully submits that the Examiner's assertion that "the wireless network tracks **(monitors)** the number of signaling messages **(signals)**" is factually incorrect, and appears to be a fundamental, technical miscomprehension of Bu's teachings.

More particularly, it is self-evident that the "signaling cost to data ratio" implies obtaining a measure of "signaling cost" and a measure of "data" in order to be able to form a ratio of the two measures. *However, it is simply not the case that Bu teaches the "signaling cost" is obtained by monitoring signaling messages*. Rather, in paragraphs [0046]-[0047], Bu

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

teaches that "signaling cost" incurred by a user is *estimated* based on data traffic arrival patterns at the mobile device of the user:

> The present inventors discovered a simple, yet novel mechanism of ***estimating*** *the signaling cost* ***from traffic arrival patterns*** assuming knowledge of signaling call(s). The present inventions provide for methods and devices for detecting an attack *using the so* ***estimated*** *signaling cost*. (Emphasis added.)
>
> …In one embodiment of the present invention, the *signaling cost is* ***estimated*** *from traffic arrival patterns*. This requires *knowledge of the signaling protocols* inside wireless elements. Table 1 shows an example of a technique for ***estimating*** *signaling cost* (due to RAB establish/release) in a UMTS network according to one embodiment of the present invention. Similar techniques within the scope of the present invention can be used to ***estimate*** *other types of signaling costs* for CDMA2000 networks according to alternative embodiments of the present invention. (Emphasis added.)

As Applicant has pointed out in more than one previous Office Action Response, the teachings in these two paragraphs, and elsewhere in Bu, make it clear that the "signaling cost" used in the "signaling cost to data ratio" is obtained as *an estimate based on applying "knowledge of the signaling protocols" to observed traffic arrival patterns* to a given user. This also emphasizes that the purpose of paragraphs [0024]-[0026] is to provide "knowledge of the signaling protocols." What Bu *does not teach* is that "the wireless network tracks **(monitors)** the number of signaling messages **(signals)**."

2) Bu does not teach counting the number of occurrences of a certain predetermined signal associated with the same mobile telecommunications device whose behavior is determined. Instead, Bu teaches estimating "signaling cost to data ratio" for data traffic arriving *to "user i" from "sender s"* in order to detect *if "sender s" is launching an attack*. Thus, the "signaling cost" estimate determined for the mobile device of "user i" is used *to detect if a <u>different</u> mobile device (that of "user s") is an attacker*.

The Examiner cited to paragraphs [0054]-[0057] in Bu as teaching "when the signaling cost to data ratio of the packet exceeds a threshold, then flag the packet. In other word[s], when the number of signaling messages determined from the packet exceed a reference signaling messages, then *the packet from the sender to the user will be flagged*." (Current Office Action,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

page 5; emphasis added.) Referring to Table 1 and Table 2 in Bu, Applicant submits that these paragraphs cited by the Examiner clearly teach that the "signaling costs" and "signaling cost to data ratio" for the mobile device associated with "user i" are estimated based on data sent by "sender s," and when this estimated "signaling cost to data ratio" exceeds a threshold, "*sender s*" is flagged as an attacker. Put another way, Bu teaches if the mobile device of "user i" is determined to be causing excessive signaling messages due to data received from "sender s," *it is the mobile device of "sender s"* that is identified as a misbehaving mobile device, *not the mobile device of "sender i."*

In contrast, amended claim 1 is generally directed to monitoring or counting in the core network occurrences of a certain predetermined signal associated with a particular mobile telecommunications device, and based on the number of occurrences, determining if *that particular mobile device* – i.e., the one associated with the certain predetermined signal being monitored or counted – is behaving acceptably in the telecommunications network. This is clearly and very distinctly different from the teachings of Bu, which entail determining the behavior of "sender s" based on an estimated "signaling to data ratio" of a different user – "user i" – incurred due to "sender s."

3) Bu does not teach: "wherein the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device, the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals." Instead Bu teaches *estimating all* messages exchanged between another mobile device and the core network.

As noted above, the Examiner cited to paragraphs [0054]-[0056] in Bu as teaching "the wireless network tracks **(monitors)** the number of signaling messages **(signals)** that are required in order to establish a dedicated channel to transmit the packet." On page 7 of the Current Office Action, the Examiner again cited to these paragraphs, asserting that "the number of signaling

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

messages is monitored for the wireless device to determine signaling cost to data ratio." As discussed above, Applicant submits that the Examiner's assertion is factually incorrect, and represents an erroneous technical analysis of Bu's teachings.

Notwithstanding the failure of Bu to teach "the wireless network tracks **(monitors)** the number of signaling messages **(signals)** that are required in order to establish a dedicated channel to transmit the packet," and without acquiescing to the Examiner's errant assertion to the contrary, Applicant has amended claim 1, as described above, to recite, *inter alia*, "wherein the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device." This amendment makes clear that monitoring of a "certain predetermined signal associated with the mobile telecommunications device" entails *counting* those specific occurrences, and is carried out in the core network.

Further, Applicant notes that the Examiner has equated "signaling messages" in Bu with "signals" recited, *inter alia*, in claim 1. As such, the Examiner appears to have recognized the distinction in Bu between "signaling messages" used to set up and tear down RABs, and data "traffic," which is transported on RABs and other legs of bearer channels. In equating "signaling messages" in Bu with "signals" in claim 1, the Examiner has therefore applied at least a similar interpretation to "signals" of claim 1, and at least a similar recognition of a distinction between "signals" and user data or other user traffic. It follows that the Examiner's equating "signaling messages" in Bu with "signals" in claim 1 provides a further basis by which claim 1 distinguishes over Bu's teachings.

Specifically, Bu's "mechanism of estimating signaling cost from traffic arrival patterns assuming knowledge of signaling call(s)" relies fundamentally on an *assumed* accounting of *all*

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

"signaling messages" involved in set-up and tear-down of a RAB (e.g., 24 messages to establish a RAB, etc.). So even though Bu does not teach any actual monitoring or counting of "signaling messages," the estimation technique computes a tally of *all* the "signaling messages" that are *assumed* to have been transmitted. As such, Bu's technique would fail to provide the desired estimated signaling cost if it only accounted for just a "certain" signaling message: doing so would underestimate the "signaling cost" and undermine the basis for the technique. Further, Bu's technique entirely lacks any way to distinguish or identify individual "signaling messages." Rather, it is based entirely on an assumed knowledge of the *total number* of "signaling messages" associated with set-up and tear-down of a RAB, since the observation of "traffic arrival patterns" serves to only indirectly detect RAB set-ups/tear-downs, and is therefore the only indication that "signaling messages" have been transmitted.

In contrast, claim 1 recites, *inter alia*, counting "in the core network a number of occurrences of *a certain predetermined signal* associated with the mobile telecommunications device" (emphasis added). That is, the counting entails identifying a specific ("certain") predetermined signal. Bu's "signaling cost" estimation technique is not capable of identifying specific "signaling messages." And even if it was, Bu's technique requires an assumed accounting of *all* "signaling messages," so accounting for only a certain signaling message would cause Bu's technique to fail.

4) Bu does not teach counting in the core network, but estimates the number of messages exchanged between a different mobile device and the core network, which includes the messages between the base station and the different mobile device

As explained above, Bu's estimation technique is based entirely on an assumed knowledge of the *total number* of "signaling messages" associated with set-up and tear-down of a RAB, since the observation of "traffic arrival patterns" serves to only indirectly detect RAB set-ups/tear-downs, and is therefore the only indication that "signaling messages" have been

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

transmitted. This estimation however, takes into account all signaling messages related to a RAB setup and therefore also includes the signaling messages exchanged between the base station and the different mobile device. That is, Bu's estimation *necessarily* includes assumed transmissions of signaling messages between devices that are *not* in the core network. It is clear, however, that such messages are *not* included in the counting in the core network as recited, *inter alia*, in claim 1.

5) Bu does not teach: "wherein the telecommunications network is further arranged to register when the number of occurrences exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network"

As noted above, the Examiner cited to paragraphs [0054]-[0057] in Bu as teaching "when the number of signaling messages determined from the packet exceed a reference signaling messages, then the packet from the sender to the user will be flagged." On page 7 of the Current Office Action, the Examiner again cited to paragraphs [0054]-[0057] in Bu, asserting that "when the signaling cost to data ratio for the wireless device exceeds a threshold, subsequent traffic from the wireless device is flagged." As also discussed above, Bu's teachings in paragraphs [0054]-[0057], taken with the teachings in paragraphs [0046]-[0047] and Tables 1 and 2, describe how "signaling messages" associated with the mobile device of "user i" may be used to detect an attack by the mobile device of "sender s."

To summarize once more, Bu teaches that a "signaling cost" and "signaling cost to data ratio" are estimated for "user i" due to data received from "sender s." When this estimated "signaling cost to data ratio" exceeds a threshold, "sender s" is flagged as a possible (or actual) attacker. Thus, the behaviour of *"sender s"* is determined based on estimated "signaling cost" and "signaling cost to data ratio" associated with *"user i."*

In contrast, claim 1 recites, *inter alia*, "wherein the telecommunications network is further arranged to register when the number of occurrences exceeds a level *indicating*

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

acceptable behaviour of the mobile telecommunications device in the telecommunications network" (emphasis added). That is, the "mobile telecommunications device" associated with the occurrences of the "certain predetermined signal" is the *same* "mobile telecommunications device" whose behaviour is determined. Bu teaches that the mobile device associated with the estimated "signaling messages" is *different* from the mobile device whose behaviour is the subject of detection. Clearly, claim 1 distinguishes over Bu in this respect, in addition to at least that discussed above.

For at least the reasons above, Applicant submits that claim 1 distinguishes over Bu, and that claim 1 is therefore allowable.

Claim 16 includes, *inter alia*, limitations similar to those of claim 1 discussed above. Applicant submits that, by similar reasoning to the discussion above, claim 16 is allowable for at least the same reasons that claim 1 is allowable.

Each of claims 2-3, 5, 7-10, and 12-13 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claims 2-3, 5, 7-10, and 12-13 are each allowable for at least the reason that each depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with any of claims 2-3, 5, 7-10, or 12-13.

5. Response to Rejections under 35 U.S.C. § 103(a)

a. Claims 4 and 6

The Examiner rejected claims 4 and 6 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu. Each of claims 4 and 6 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that each of claims 4 and 6 is allowable for at least the reason that each depends from an allowable claim. Further,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

Applicant does not concede any the Examiner's specific assertions in connection with either of claims 4 or 6.

b. Claim 11

The Examiner rejected claim 11 under pre-AIA 35 U.S.C. § 103(a) as being allegedly being unpatentable over Bu in view of Amin. Claim 11 depends from claim 1, which is allowable for at least the reasons above. Applicant therefore submits that claim 11 is allowable for at least the reason that it depends from an allowable claim. Further, Applicant does not concede any the Examiner's specific assertions in connection with claim 11.

6. Conclusion

For the foregoing reasons, Applicant submits that the claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the Current Office Action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3353.

Respectfully submitted,

McDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Dated: July 28, 2020

By: /David A. Grabelsky/
David A. Grabelsky
Reg. No. 59,208

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE,
CHICAGO, IL 60606
(312)913-0001

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	07/28/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/Theresa OKON/
*** 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.	

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.

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/646,554	Filing Date 05/21/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	10/29/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 11	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/JEFFERY L OLSEN/
*** 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.	

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

20306 7590 10/30/2020

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 10/30/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

TITLE OF INVENTION: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	02/01/2021

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

ERICSSON EXHIBIT 1005, Page 736

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

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

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

20306 7590 10/30/2020

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

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

Certificate of Mailing or Transmission

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

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

TITLE OF INVENTION: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	02/01/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
VU, PHY ANH TRAN	2438	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

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

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

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

20306 7590 10/30/2020

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
VU, PHY ANH TRAN	
ART UNIT	**PAPER NUMBER**
2438	

DATE MAILED: 10/30/2020

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

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

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

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

ERICSSON EXHIBIT 1005, Page 738

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA (FITF) Status No

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

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

1. ☑ This communication is responsive to 7/28/2020.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-7,11-13 and 16 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☑ All b) ☐ Some *c) ☐ None of the:

   1. ☑ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

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

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

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 3/27/2020.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. 10/15/2020.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/PHY ANH T VU/
Primary Examiner, Art Unit 2438

DETAILED ACTION

This Office Action is in response to the Amendment filed on 03/27/2020.

Authorization for this Examiner's Amendment is given by the attorney of record, Mr. David Grabelsky on 10/23/2020.

Notice of Pre-AIA or AIA Status

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

EXAMINER'S AMENDMENTS

Amend claims 1 -13 and 16 as follow:

Claim 1:

A system comprising:

a telecommunications network configured to identify ~~**at least one**~~ mobile telecommunications device and comprising a core network and a base station, wherein the base station is configured to receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network,

wherein the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device, the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals,

and wherein the telecommunications network is further arranged to register when the number of occurrences **of the certain predetermined signal** exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network,

wherein the certain predetermined signal indicates handover of the mobile telecommunications device.

Claim 2:

The system according to claim 1, wherein the telecommunications network is arranged to count in the core network the number of occurrences **of the certain predetermined signal** by counting a number of times ~~**the**~~ occurrence **of the certain predetermined signal** is detected when the **number of** occurrences exceed a predetermined temporal rate, and wherein the telecommunications network is further arranged to register when the number of **times** the **occurrence of the certain predetermined signal** detected ~~**occurrences**~~ exceeds a predetermined threshold.

Claim 3:

The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences **of the certain predetermined signal** when a time between a detected occurrence and ~~**the**~~ **a** previously detected occurrence is within a predetermined time interval.

Claim 4:

The system according to claim 3, wherein the telecommunications network includes a counter and a timer, and wherein the telecommunications network is arranged to start the counter upon detection of the occurrence and further to start the timer, and wherein the telecommunications network is further arranged to increase the counter by one unit if a following occurrence is within the predetermined time interval ~~T~~ as measured by the timer.

Claim 5:

The system according to claim 1, wherein the telecommunications network is further configured to detect when the **number of** occurrence**s of the certain predetermined signal** exceeds a predetermined rate.

Claim 7:

The system according to claim 1, wherein the telecommunications network is arranged to register when the number **of occurrences of the certain predetermined signal** exceeds the level for acceptable behaviour by setting a flag and/or starting a back off timer.

Claim 8: (Canceled)

Claim 9: (Canceled)

Claim 10: (Canceled)

Claim 11:

The system according to claim ~~10~~ **1**, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device and to register the number of occurrences **of the certain predetermined signal** only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.

Claim 12:

The system according to claim 1, wherein the telecommunications network is arranged to count the number of occurrences **of the certain predetermined signal** in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.

Claim 13:

The system according to claim 1, wherein the telecommunications network is further configured to:

identify at least one additional mobile telecommunications device,

receive radio signals from the at least one additional mobile telecommunications device and to process these radio signals into processed signals and to transmit the processed signals to the core network,

count in the core network a number of occurrences of a certain predetermined signal associated with the at least one additional mobile telecommunications device, the certain predetermined processed signal representing an interaction between network devices for normal processing of signals,

register when the number **of occurrences of a certain predetermined signal associated with the at least one additional mobile telecommunications device** exceeds a level indicating acceptable behaviour of the at least one additional mobile telecommunications device within the telecommunications network,

~~and~~ wherein the telecommunications network is further arranged to aggregate ~~**the**~~ registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device,

and wherein the certain predetermined signal associated with the at least one additional mobile telecommunications device indicates handover of the at least one additional mobile telecommunications device.

Claim 16:

A method for detecting behaviour of a mobile telecommunications device in a telecommunications network comprising a core network, the telecommunications network including a base station, the method comprising:

at the base station, receiving radio signals from the mobile telecommunications device, and processing the radio signals into processed signals and transmitting the processed signals to the core network;

in the telecommunications network, identifying the mobile telecommunications device;

the telecommunications network counting, in the core network, ~~the~~ **a** number of occurrences of a certain predetermined signal associated with the mobile telecommunications device, the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals; and

registering when the number of occurrences **of the certain predetermined signal** exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network,

wherein the certain predetermined signal indicates handover of the mobile telecommunications device.

ALLOWABLE SUBJECT MATTER

Claims 1-7, 11-13 and 16 are allowed, while claims 8-10 and 14-15 are cancelled.

The following is an examiner's statement of reasons for allowance:

The amendments and/or arguments submitted by Applicant have been considered and are persuasive, in particular those found on pages 9-16 of the Arguments/Remarks filed on 7/28/2020.

Therefore, the claims are allowable over the prior arts of records.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH TRAN VU whose telephone number is (571)270-7317. The examiner can normally be reached on Monday-Friday 7 am-1 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571) 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access

to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PHY ANH T VU/
Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No. 14/646,554	Applicant(s) Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	AIA (FITF) Status No

All participants (applicant, applicant's representative, PTO personnel):

(1) PHY ANH TRAN. VU. (3) _____.

(2) David Grabelsky. (4) _____.

Date of Interview: 15 October 2020.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☑ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Bu et al. (US 2006/0230450 A1).

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: In an effort to expedite prosecution, Examiner contacted Applicant's representative, Mr. David Grabelsky to inform him that the arguments filed on 07/28/2020 in combination with the previous proposed amendments would overcome the cited art Bu and place in the application in better condition for allowance. Mr. Grabelsky consulted with his client and an agreement was reached. Authorization was given to the Examiner to make the changes via the Examiner's Amendments on 10/23/2020.

Notice of References Cited	Application/Control No. 14/646,554	Applicant(s)/Patent Under Reexamination Muller, Frank	
	Examiner PHY ANH T VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20110230192-A1	09-2011	TIWARI; Kundan	H04W36/0022	455/436
*	B	US-20120129517-A1	05-2012	Fox; David Andrew	H04W12/12	455/425
*	C	US-8387141-B1	02-2013	Zhukov; Igor	H04W12/1208	726/22
*	D	US-20120180119-A1	07-2012	Bessis; Thierry C.	H04W12/0602	726/11
*	E	US-20070283436-A1	12-2007	Duffield; Nicholas	H04L63/1425	726/23
*	F	US-20070121596-A1	05-2007	Kurapati; Krishna	H04M7/0078	370/356
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L 63/14	5/2/2016; 6/23/2017; 7/4/2019; 2/27/2020; 10/23/2020	PVU
H04L 63/1425	5/2/2016; 6/23/2017; 7/4/2019 ; 10/23/2020	PVU
G06F12/14	02/27/2020 ; 10/23/2020	

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

ERICSSON EXHIBIT 1005, Page 752

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	Art Unit
	PHY ANH T VU	2438

Search Notes		
Search Notes	**Date**	**Examiner**
PLUS search	05/02/2016	PVU
Inventor names search	05/02/2016; 10/23/2020	PVU
Keywords search	05/02/2016; 12/09/2016; 6/23/2017; 11/22/2017; 10/26/2018; 7/4/2019; 02/27/2020; 10/23/2020	PVU
Consulted with WG SPE and QAS regarding 101 issues	06/23/2017	PVU
IP.com	02/27/2020	PVU
Consulted with Luu regarding 101 for system claim	10/23/2020	PVU
Google Patent search	10/23/2020	PVU

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
H04L	63/14	10/23/2020	PVU
H04L	63/1425	10/23/2020	PVU
G06F	21/554	10/23/2020	PVU

/PHY ANH T VU/ Primary Examiner, Art Unit 2438	

ERICSSON EXHIBIT 1005, Page 753

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	**Art Unit**
	PHY ANH T VU	2438

CPC						
Symbol					**Type**	**Version**
H04L	/	63	/	14	F	2013-01-01
H04L	/	63	/	1425	I	2013-01-01
H04W	/	24	/	08	I	2013-01-01
H04W	/	88	/	02	A	2013-01-01

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	11	
/PHY ANH T VU/ Primary Examiner, Art Unit 2438	23 October 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	**Art Unit**
	PHY ANH T VU	2438

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	11	/	00
G06F	/	12	/	14
G06F	/	12	/	16

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	11	
/PHY ANH T VU/ Primary Examiner, Art Unit 2438	23 October 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	**Art Unit**
	PHY ANH T VU	2438

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		10												
2	2	8	11												
3	3	9	12												
4	4	10	13												
5	5		14												
6	6		15												
7	7	11	16												
	8														
	9														

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/PHY ANH T VU/ Primary Examiner, Art Unit 2438	23 October 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/646,554	Muller, Frank
	Examiner	**Art Unit**
	PHY ANH T VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	05/02/2016	12/09/2016	06/23/2017	11/22/2017	10/26/2018	07/04/2019	02/27/2020		
1	1	✓	✓	✓	✓	✓	✓	✓		
2	2	✓	✓	✓	✓	✓	✓	✓		
3	3	✓	✓	✓	✓	✓	✓	✓		
4	4	✓	✓	✓	✓	✓	✓	✓		
5	5	✓	✓	✓	✓	✓	✓	✓		
6	6	✓	✓	✓	✓	✓	✓	✓		
7	7	✓	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓	✓		
	9	✓	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓	✓		
8	11	✓	✓	✓	✓	✓	✓	✓		
9	12	✓	✓	✓	✓	✓	✓	✓		
10	13	✓	✓	✓	✓	✓	✓	✓		
	14	✓	✓	-	-	-	-	-		
	15	✓	✓	-	-	-	-	-		
11	16		✓	✓	✓	✓	✓	✓		

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		H04l63/14.cpc. and (excessive near5 (request occurrence traffic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
		"20060230450".pn. and nas	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:23
		(monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
		"199833340".pdpt.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S1	1	"14646554"	US-PGPUB; USPAT	OR	OFF	2016/05/02 08:25
S2	1	"20060288407".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:16
S3	0	"2006104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S4	1	"20060104752".pn.	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:19
S5	0	wo-20060104752	US-PGPUB; USPAT	OR	OFF	2016/05/02 09:22
S6	0	wo-20060104752	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:22
S7	0	wo06/104752	US-PGPUB; USPAT; USOCR;	OR	OFF	2016/05/02 09:23

			DERWENT; IBM_TDB			
S8	1	(2006/0104752)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:24
S9	4	"2006010108"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:27
S10	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:28
S11	2	"5953652".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:29
S12	2	"20090323965".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:30
S13	1	"20060230450".pn. and (RAB)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 09:55
S14	2	"5953652".pn. and detect$3	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:19
S15	1	"5953652".pn. and (detect$3 with location)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:20
S16	0	"5953652".pn. and (detect$3 with handover)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21

S17	0	"5953652".pn. and (detect$3 with handover$3)	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:21
S18	0	wo1998033340	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:23
S19	0	wo1998033340	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S20	12,250,043	wo "1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:24
S21	1	"1998033340"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:27
S22	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S23	0	WO1998033340.pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S24	0	WO1998033340.ptpn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:28
S25	0	(wo-199833340)	US-PGPUB; USPAT; USOCR;	OR	OFF	2016/05/02 11:32

			FPRS; EPO; DERWENT; IBM_TDB			
S26	0	(wo199833340)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:33
S27	1	"5953652".pn. and unrealistic	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:34
S28	4	WO-9833340-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/05/02 11:35
S29	57	(monitor$3 with behavior$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:44
S30	0	h04l63/14.cpc. and (monitor$3 with telecommunicat$3)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S31	73	h04l63/14.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S32	30	S31 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:50
S33	109	h04l63/1425.cpc. and (monitor$3 with mobile)	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S34	18	h04l63/1425.cpc. and (monitor$3 with mobile) same malicious	US-PGPUB; USPAT	OR	OFF	2016/05/02 12:52
S35	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 13:45
S36	1	"14727408"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/08 16:16
S37	3	"20100064341".pn.	US-PGPUB; USPAT;	OR	OFF	2016/12/09 10:11

			USOCR; FPRS; EPO; DERWENT; IBM_TDB			
S38	3	wo-2007075423-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:12
S39	2	"20120155274".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:13
S40	1,342	(monitor$3 same (malicious suspicious)) same mobile	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S41	37	(monitor$3 same (malicious suspicious)) same mobile same (threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2016/12/09 10:14
S42	1,121	(monitor$4 with (network with traffic) with event)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S43	30	(monitor$4 with (network with traffic) with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:52
S44	268	monitor$4 with (network with event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 11:53
S45	155	S44 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 11:54

S46	169	(network with indicat$4 near5 event) same (exceed$4 near10 threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/04/05 12:55
S47	106	S46 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/04/05 12:55
S48	2	"20060230450".pn. and network	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:44
S49	1	"20060230450".pn. and bs	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 07:52
S50	1	"20060230450".pn. and pdsn	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:26
S51	2	"20150304345".pn. and (data near3 first near3 type)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 13:53
S52	13	"9684898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S53	2	"9684898".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/22 16:31
S54	4	"9633208".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	OFF	2017/06/22 18:00

			DERWENT; IBM_TDB			
S55	1	"20150304345".pn. and bearer	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:29
S56	0	"20060230450".pn. and handover	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:37
S57	0	"20060230450".pn. and hand$over	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S58	1	"20060230450".pn. and hand$off	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2017/06/23 09:38
S59	1	H04l63/14.cpc. and (mobile and (excessive near5 occurrence))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:33
S60	1	H04l63/14.cpc. and (excessive near5 occurrence)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:34
S61	11	H04l63/14.cpc. and (excessive near5 (request occurrence traffic))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:35
S62	92	H04l63/14.cpc. and (excessive)	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2017/06/23 11:39

			DERWENT; IBM_TDB			
S63	48	S62 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:39
S64	237	H04I63/1425.cpc. and (mobile and excessive and (malicious attack suspicious))	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2017/06/23 11:45
S65	71	S64 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2017/06/23 11:46
S66	461	(telecommunication with (exceed$4) near5 threshold)	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S67	2	(telecommunication with (exceed$4) near5 threshold) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:11
S68	0	(telecommunication with (exceed$4) near5 threshold) same behavior	US-PGPUB; USPAT	OR	ON	2017/11/22 07:12
S69	0	(monitor$4 with data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S70	0	(monitor$4 same data$stream) with abnormal	US-PGPUB; USPAT	OR	ON	2017/11/22 07:13
S71	64	(monitor$4 with abnormal) with data near5 streams	US-PGPUB; USPAT	OR	ON	2017/11/22 07:14
S72	19,559	monitor$4 with data near5 streams	US-PGPUB; USPAT	OR	ON	2018/05/09 17:15
S73	62	(monitor$4 with streams) same (data near5 abnormal$3)	US-PGPUB; USPAT	OR	ON	2018/05/09 17:20
S74	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:33
S75	7	g06f12/14.cpc. and (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:35
S76	1,734	(detect$4 defend$4) with (signal$4 near3 attack$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	OFF	2018/10/26 12:38

			DERWENT; IBM_TDB			
S77	28	(detect$4 defend$4) with (signal$4 near3 attack$4) same (3g near10 wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2018/10/26 12:39
S78	3	"20060230450"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2019/07/03 08:38
S79	0	H04l63/14.cpc. and (excessive near5 occurrence) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:26
S80	14	H04l63/14.cpc. and (attack$4) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:26
S81	69	H04l63/1425.cpc. and (attack$4) with (normal near5 packets)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2019/07/04 12:33
S82	24	S81 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2019/07/04 12:33
S83	2	"20150304345"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/01/13 11:27
S84	2	"20060230450".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/01/13 11:54
S85	0	"20060230450".pn. and (utms)	US-PGPUB; USPAT; USOCR;	OR	OFF	2020/02/26 10:24

			FPRS; EPO; DERWENT; IBM_TDB			
S86	2	"20060230450".pn. and (umts)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/26 10:24
S87	2	"20190259485".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 10:15
S88	2	"20080189614".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 14:02
S89	816	(avoid$4 prevent$4) same (signal$4 near3 attack)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 19:30
S90	353	S89 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:31
S91	0	H04l63/1425.cpc. and S90	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/02/27 19:31
S92	203	(avoid$4 prevent$4) same (signal$4 near3 attack) and (telecommunications mobile)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 19:32
S93	71	S92 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:32
S94	1	(avoid$4 prevent$4) same (signal$4 near3 attack) and (set$up with release) and (excessive near3 signal$4 near5 message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/02/27 19:37

S95	1	(avoid$4 prevent$4) same (signal$4 near3 attack) and (set$up with release) and (excessive near3 signal$4 near5 messages)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/02/27 19:37
S96	0	S90 and G06f12/14.cpc.	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:38
S97	0	S89 and G06f12/14.cpc.	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:38
S98	1	S89 and h04l63/14.cpc.	US-PGPUB; USPAT	OR	OFF	2020/02/27 19:38
S99	26	(avoid$4 prevent$4) same (signal$4 near3 attack) and 3g	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/02/27 19:39
S100	7	("20120180119" "20070283436" "20070121596").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/10/15 11:26
S101	2	"20150304345".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2020/10/15 13:43
S102	0	H04l63/14.cpc. and (count$4 determin$4) with (number with signal) same (core MME SGSN)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 11:05
S103	3	H04l63/14.cpc. and (count$4 determin$4) with (signal) same (core MME SGSN)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 11:06
S104	21,391	(count$4 sum$5 total$4) with (signal message traffic) same (core MME SGSN)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 11:16

S105	1,982	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 11:24
S106	13	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) same (handover handoff) and (abnormal anomal$4 intrusion un$usual$4 suspicious)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 11:25
S107	199	("4154984" "4608685" "5029204" "5195126" "5245636" "5553223" "5608781" "5826191" "5974126" "6047385" "6094681" "6134618" "6208718" "6229887" "6298039" "6307841" "6310950" "6353902" "6381453" "6404734" "6421323" "6463287" "6516195" "6574216" "6625460" "6763190" "6874022" "6934367" "7099660" "7130397" "7142853" "7143153" "7293082" "7363548" "7412600" "7627348" "7945252" "7945252" "8107951" "8300644" "8359022" "8411846" "8442233" "8504846" "8638717" "8665325" "8738004" "8750906" "8787869" "9031206").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 11:30
S108	23	"2011072719"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 13:34
S109	22	"2009067170"	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 13:35
S110	10	H04l63/1425.cpc. and (count$4 determin$4) with (signal) same (core MME SGSN)	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 13:39
S111	115	g06f21/554.cpc. and (count$4 determin$4) with (signal) same (core MME SGSN)	US-PGPUB; USPAT; USOCR;	OR	ON	2020/10/23 14:03

			FPRS; EPO; DERWENT; IBM_TDB			
S112	80	S111 and @ad<"20121122"	US-PGPUB; USPAT	OR	OFF	2020/10/23 14:04
S113	119	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2020/10/23 14:24

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2	h04l63/14.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious)	US-PGPUB; USPAT	OR	ON	2020/10/23 15:44
L3	24	h04l63/1425.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious)	US-PGPUB; USPAT	OR	ON	2020/10/23 15:49
L4	135	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious).clm.	US-PGPUB; USPAT	OR	ON	2020/10/23 16:42
L5	2	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) same (handover handoff) and (abnormal anomal$4 intrusion un$usual$4 suspicious).clm.	US-PGPUB; USPAT	OR	ON	2020/10/23 16:43
L6	80	g06f21/554.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious)	US-PGPUB; USPAT	OR	ON	2020/10/23 16:47
L7	3,699,573	g06f21/554.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (exceed$4 over) (threshold acceptable)	US-PGPUB; USPAT	OR	ON	2020/10/23 17:12
L8	3,699,571	g06f21/554.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (handover handoff) same (core	US-PGPUB; USPAT	OR	ON	2020/10/23 17:13

		MME SGSN) same (exceed$4 over) (threshold acceptable)				
L9	0	g06f21/554.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (handover handoff) same (core MME SGSN) same (exceed$4 over) near5 (threshold acceptable)	US-PGPUB; USPAT	OR	ON	2020/10/23 17:13
L10	2	g06f21/554.cpc. and (count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) same (exceed$4 over) near5 (threshold acceptable)	US-PGPUB; USPAT	OR	ON	2020/10/23 17:14
L11	206	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) same (exceed$4 over) near5 (threshold acceptable)	US-PGPUB; USPAT	OR	ON	2020/10/23 17:19
L12	4,194	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) same (exceed$4 over) near5 (threshold acceptable)".clm"	US-PGPUB; USPAT	OR	ON	2020/10/23 17:19
L13	36	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) same (exceed$4 over) near5 (threshold acceptable).clm.	US-PGPUB; USPAT	OR	ON	2020/10/23 17:19
S114	90	(count$4 sum$6 total$4) with (signal message traffic) same (core MME SGSN) and (abnormal anomal$4 intrusion un$usual$4 suspicious).ab.	US-PGPUB; USPAT	OR	ON	2020/10/23 14:25

10/23/2020 6:04:38 PM
C:\Users\pvu3\Documents\EAST\Workspaces\14646554.wsp

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

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14646554
Filing Date	2015-05-21
First Named Inventor	Frank Muller
Art Unit	2438
Examiner Name	Phy Anh Tran Vu
Attorney Docket Number	15-686-WO-US

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/P.T.V/	1	2011072719	WO	A1	2011-06-23	NOKIA SIEMENS NETWORKS OY		

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.T.V/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14646554
	Filing Date	2015-05-21
	First Named Inventor	Frank Muller
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	15-686-WO-US

	1	

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

EXAMINER SIGNATURE

Examiner Signature	/PHY ANH T VU/	Date Considered	10/23/2020

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.T.V/

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 4961

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/646,554	05/21/2015	726	2438	15-686-WO-US

APPLICANTS

KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

INVENTORS

Frank Muller, Delft, NETHERLANDS;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/EP2013/074440 11/22/2013

**** FOREIGN APPLICATIONS ***************************

EUROPEAN PATENT OFFICE (EPO) 12193884.9 11/22/2012

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

07/07/2015

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/PHY ANH TRAN VU/ Examiner's Signature	☐ Initials	NETHERLANDS	3	15	2

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

System to Detect Behaviour in a Telecommunications Network

FILING FEE RECEIVED		
1480	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

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

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

20306 7590 10/30/2020
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

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

Certificate of Mailing or Transmission

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

David A. Grabelsky	(Typed or printed name)
/David A. Grabelsky/	(Signature)
January 12, 2021	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	05/21/2015	Frank Muller	15-686-WO-US	4961

TITLE OF INVENTION: SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	02/01/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
VU, PHY ANH TRAN	2438	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

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

1 McDonnell Boehnen
2 Hulbert & Berghoff LLP
3

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Koninklijke KPN N.V.	Rotterdam, Netherlands
Nederlandse Organisatie Voor Toegepast-Natuurwetenschappelijk Onderzoek TNO	's-Gravenhage, Netherlands

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

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 13-2490

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature /David A. Grabelsky/ Date January 12, 2021

Typed or printed name David A. Grabelsky Registration No. 59,208

Electronic Patent Application Fee Transmittal

Application Number:	14646554
Filing Date:	21-May-2015
Title of Invention:	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK
First Named Inventor/Applicant Name:	Frank Muller
Filer:	David A. Grabelsky/Carol Neth
Attorney Docket Number:	15-686-WO-US

Filed as Large Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1200	1200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1200**

Electronic Acknowledgement Receipt

EFS ID:	41619058
Application Number:	14646554
International Application Number:	
Confirmation Number:	4961
Title of Invention:	SYSTEM TO DETECT BEHAVIOUR IN A TELECOMMUNICATIONS NETWORK
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	David A. Grabelsky
Filer Authorized By:	
Attorney Docket Number:	15-686-WO-US
Receipt Date:	12-JAN-2021
Filing Date:	21-MAY-2015
Time Stamp:	13:08:37
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1200
RAM confirmation Number	E20211BD09060965
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	15-686-WO-US_IssueFeeTransmittal.pdf	112920 9254a6de1d98618397b638ce5aee71ca42d83f70	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30544 f910b045657fe6a243c267c58b99566c94812dc0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	143464		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/646,554	02/16/2021	10924500	15-686-WO-US	4961

20306 7590 01/27/2021

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

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

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

Frank Muller, Delft, NETHERLANDS;
KONINKLIJKE KPN N.V., The Hague, NETHERLANDS
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, 's-Gravenhage, NETHERLANDS;

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