



(51) International Patent Classification:

H04W 28/08 (2009.01) *H04W* 12/08 (2009.01)
H04W 24/08 (2009.01)

(21) International Application Number:

PCT/US2017/012740

(22) International Filing Date:

9 January 2017 (09.01.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

15/052,812 24 February 2016 (24.02.2016) US

(71) Applicant: **IXIA** [US/US]; 26601 West Agoura Road, Calabasas, CA 91302 (US).

(72) Inventors: **RAJ, Avinash Raj Nambi**; 2946 Meadow Brook Drive, Woodbury, MN 55125 (US). **SCHWENK, Alan, Richard**; 8432 Lunar Stone Place, Raleigh, NC 27613 (US). **CHIRIACESCU, Gabriel**; 8436 Broderick Place, Cary, NC 27519 (US).

(74) Agent: **HUNT, Gregory, A.**; Jenkins, Wilson, Taylor & Hunt, P.A., 3015 Carrington Mill Boulevard, Suite 550, Morrisville, NC 27560 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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).

Published:

— with international search report (Art. 21(3))

(54) Title: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR DISTRIBUTING MONITORED NETWORK TRAFFIC

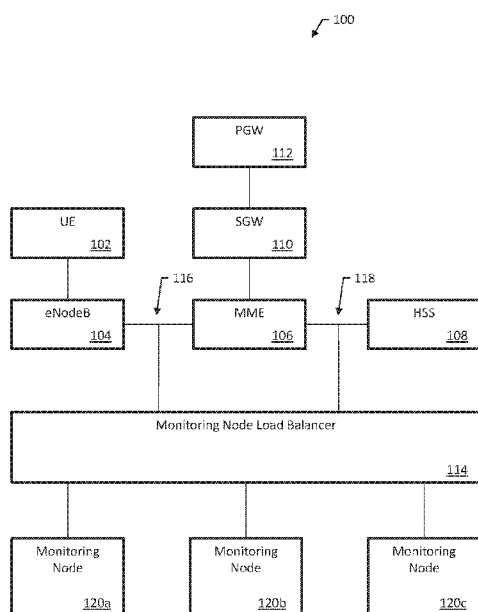


FIG. 1

(57) Abstract: The subject matter described herein relates to methods, systems, and computer readable media for test system connection resiliency. In some examples, a method for distributing monitored network traffic includes monitoring S1 -MME traffic and S6a traffic in a core network of a telecommunications network. The method includes decrypting encrypted S1 -MME traffic using information extracted from the S6a traffic. The method includes load balancing between a plurality of monitoring nodes using the decrypted S1 -MME traffic.

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR DISTRIBUTING MONITORED NETWORK TRAFFIC

PRIORITY CLAIM

5 This application claims the benefit of U.S. Patent Application No. 15/052,812, filed February 24, 2016; the disclosure of which is incorporated herein by reference in its entirety.

10 TECHNICAL FIELD

The subject matter described herein relates generally to distributing monitored network traffic. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for load balancing between monitoring nodes at a monitoring node load balancer.

15 BACKGROUND

Network analysis tools are used within communication networks to monitor network traffic and to detect events, such as undesired network intrusions. When multiple network analysis tools are being utilized in parallel to monitor network traffic, it can be desirable to load balance the monitored network traffic among the network analysis tools, e.g., so that some network analysis tools do not get overloaded while others are underutilized. Further, network analysis tools can be configured to receive all packets associated with a particular communication session for a mobile user device in order to enhance the ability of the network analysis tool to provide effective monitoring of the network traffic. For example, as mobile user equipment moves through a communication network, it can be useful for all the network traffic associated with that user equipment to be identified and forwarded to the same network analysis tool. This may be difficult to achieve, for example, for load balanced systems when mobile user devices can use different identifiers at different times.

SUMMARY

The subject matter described herein relates to methods, systems, and computer readable media for test system connection resiliency. In some examples, a method for distributing monitored network traffic includes monitoring S1-MME traffic and S6a traffic in a core network of a telecommunications network. The method includes decrypting encrypted S1-MME traffic using information extracted from the S6a traffic. The method includes load balancing between a plurality of monitoring nodes using the decrypted S1-MME traffic.

10 The subject matter described in this specification may be implemented in hardware, software, firmware, or combinations of hardware, software and/or firmware. In some examples, the subject matter described in this specification may be implemented using a non-transitory computer readable medium storing computer executable instructions that when
15 executed by one or more processors of a computer cause the computer to perform operations. Computer readable media suitable for implementing the subject matter described in this specification include non-transitory computer-readable media, such as disk memory devices, chip memory devices, programmable logic devices, random access memory (RAM), read
20 only memory (ROM), optical read/write memory, cache memory, magnetic read/write memory, flash memory, and application specific integrated circuits. In addition, a computer readable medium that implements the subject matter described in this specification may be located on a single device or computing platform or may be distributed across multiple devices
25 or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of an example telecommunications network including at least one user equipment (UE) mobile device;

30 Figure 2 is a block diagram of an example monitoring node load balancer;

Figure 3 is a call flow diagram illustrating an example exchange of messages monitored by the monitoring node load balancer;

Figure 4 is a diagram illustrating an example network stack for communications between the UE and the MME; and

Figure 5 is a flow chart illustrating an example method for distributing monitored network traffic.

5

DETAILED DESCRIPTION

Figure 1 is a block diagram of an example telecommunications network **100** including at least one user equipment (UE) mobile device **102** connected to a core network of the telecommunications network.

10 Telecommunications network **100** can be any appropriate type of data communications network, e.g., a long term evolution (LTE) network. The core network can include one or more nodes of a system architecture evolution (SAE) core or evolved packet core (EPC) network or any appropriate network nodes.

15 UE **102** can be any appropriate type of communications device, e.g., a mobile phone. UE **102** communicates with an evolved node B (eNodeB) **104**, e.g., over a radio access network. eNodeB **104** can include any suitable entity (e.g., a base transceiver station (BTS) or a node B) for providing data via an air interface. For example, eNodeB **104** may be an
20 LTE mobile network entity having functionality similar to that of a radio network controller (RNC) and a base station (BS) in 2G networks or an RNC and a Node B in 3G mobile networks.

In some examples, eNodeB **104** may communicate directly with user devices and may be responsible for header compression, ciphering, reliable
25 delivery of packets, admission control, and radio resource management. eNodeB **104** may also communicate with various other modules and/or nodes, e.g., mobility management entity (MME) **106**, for performing various control plane signaling functions such as network attaching, UE authentication, bearer channel setup, and mobility management.

30 MME **106** is configured for performing one or more mobility management functions, such as tracking movements associated with UE **102**. In some examples, MME **106** may communicate information (e.g., mobility-related information) to other nodes in or associated with

telecommunications network **100**. For example, MME **106** may receive registration requests from eNodeB **104** and may communicate with a home subscriber server (HSS) **108** for performing authentication and/or for updating the current location of the subscriber. Additionally, MME **106** may
5 communicate with a serving gateway (SGW) **110**.

HSS **108** is configured for maintaining and/or providing one or more subscriber data management functions. HSS **108** may maintain subscriber-related information, such as user identification, control information for user authentication and authorization, location information, and user profile data.
10 For example, HSS **108** may include a database containing details about subscribers associated with UEs, e.g., UE **102**, services available to UEs, and the current locations (e.g., current serving nodes) of UEs.

SGW **110** is configured for routing and forwarding data packets. For example, SGW **110** may include functions similar to and/or functions
15 different from a gateway GPRS support node (GGSN) in a 3G network. SGW **110** may include nodes for providing data paths between eNodeB **104** and a packet gateway (PGW) **112**. For example, SGW **110** and eNodeB **104** may communicate via an S1-U or other interface and SGW **110** and PGW **112** may communicate via an S5 or S8 interface.

20 SGW **110** may be configured to act as a mobility anchor for the user or data plane (e.g., during inter-eNB handovers). SGW **110** may manage and store UE contexts, e.g., information associated with an IP bearer service. For example, for an idle state UE, SGW **110** may terminate a downlink data path and initiate paging when downlink data arrives for the
25 UE. SGW **110** may also be used for communicating with other mobile networks, such as 2G/3G networks. SGW **110** may provide charging services and/or policy enforcement for UE **102**.

PGW **112** can be configured for communicating with external packet data networks. For example, PGW **112** may be an access point for traffic to
30 UE **102** from a packet network. PGW **112** may perform policy enforcement, packet filtering, charging support, lawful interception, and/or other functions. PGW **112** may also act as a mobility anchor between 3GPP and non-3GPP networks, such as CDMA and WiMAX networks. In some examples, UE **102**

may have simultaneous connectivity with multiple PGWs for accessing multiple packet networks.

eNodeB **104** communicates with MME **106** over a S1-MME interface **116**, and MME **106** communicates with HSS **108** over an S6a interface **118**.

5 A monitoring node load balancer **114** monitors S1-MME traffic on S1-MME interface **116** on a first input port and S6a traffic on S6a interface **118** on a second input port. Monitoring node load balancer **114** distributes tapped traffic from the core network across a number of monitoring nodes **120a-c**. Each of monitoring nodes **120a-c** is configured to perform one or more
10 monitoring functions for telecommunications network **100**.

The tapped traffic can be, e.g., lawfully intercepted S1-MME traffic or S6a traffic or both. Monitoring node load balancer **114** load balances the tapped traffic across monitoring nodes **120a-c**, e.g., to prevent any of monitoring nodes **120a-c** from being over or under utilized. In some
15 examples, monitoring node load balancer **114** extracts subscriber identifiers from the S1-MME traffic or the S6a traffic or both and distributes the tapped traffic across monitoring nodes **120a-c** using the subscriber identifiers.

For example, monitoring node load balancer **114** can distribute tapped traffic so that each monitoring node **120a-c** is handling an
20 approximately equal number of subscriber identifiers and traffic associated with those subscriber identifiers. Monitoring node load balancer **114** can use international mobile subscriber identities (IMSI) to perform the load balancing.

In some cases, UE **102** will cause network traffic to be transmitted in
25 telecommunications network **100** where the subscriber identifier for UE **102** is encrypted. For example, UE **102** may enter an idle state, releasing some but not all network resources for UE **102**. When UE **102** later re-enters an active state, network traffic for UE **102** on S1-MME interface **116** may be encrypted. In that case, monitoring load node balancer **114** may not be able
30 to perform load balancing without decrypting the network traffic for UE **102** on S1-MME interface **116** to determine that the traffic is associated with UE **102**.

To properly perform the load balancing, monitoring node load balancer **114** can be configured to decrypt some of the S1-MME traffic, e.g., only as much S1-MME traffic as is necessary to perform load balancing across monitoring nodes **120a-c**. Monitoring node load balancer **114** can
5 extract information from S6a traffic and use the extracted information to decrypt encrypted S1-MME traffic for load balancing across monitoring nodes **120a-c**.

Figure 2 is a block diagram of an example monitoring node load balancer **114**. Monitoring node load balancer **114** includes at least one
10 processor **202** and memory **204**. For example, monitoring node load balancer **114** can be implemented as an independent system of one or more computers having packet processors configured to load balance across monitoring nodes. In another example, monitoring node load balancer **114** can be implemented as a process executing in a distributed computing
15 system, e.g., executing on virtual machines or as a containerized load balancer.

Monitoring node load balancer **114** includes a traffic monitor **206** configured for monitoring S1-MME traffic and S6a traffic. Traffic monitor **206** extracts subscriber identifiers from the S1-MME traffic. Traffic monitor **206**
20 also extracts information from the S6a traffic that can be used to decrypt encrypted S1-MME traffic for the purpose of load balancing using subscriber identifiers.

Monitoring node load balancer **114** includes a decryption engine **208** configured for decrypting S1-MME traffic using information extracted from
25 S6a traffic. For example, decryption engine **208** can be configured for decrypting the S1-MME traffic using a SNOW 3G based algorithm or an AES based algorithm, as specified by the information extracted from the S6a traffic. In some examples, decryption engine **208** accepts data and key material as inputs and produces decrypted data as an output.

30 Monitoring node load balancer **114** includes a load balancer **210** configured for load balancing across monitoring nodes. Load balancer **210** distributes tapped traffic by creating bindings between subscribers and monitoring nodes and storing the bindings in a subscriber-node bindings

repository **212**. When load balancer **210** receives new traffic from a subscriber bound to a monitoring node, load balancer **210** distributes the new traffic to the bound monitoring node. Load balancer **210** can use any appropriate algorithm for distributing the bindings across the monitoring nodes, e.g., round-robin or fair queuing algorithms.

In operation, monitoring node load balancer **114** builds a table with a record for each subscriber attaching to the telecommunications network. Monitoring node load balancer **114** correlates, in each record, a first subscriber identifier extracted from an attachment request in the S1-MME traffic with a second subscriber identifier extracted from an attachment response in the S1-MME traffic. For example, the first subscriber identifier can be an IMSI and the second subscriber identifier can be a globally unique temporary UE identity (GUTI).

Storing both subscriber identifiers can be useful so that load balancer **210** can distribute traffic regardless of whether the traffic is associated with an IMSI or a GUTI. For example, suppose that a UE initially attaches to the telecommunications network and monitoring node load balancer **114** binds the UE to a monitoring node based on the IMSI of the UE, which is extracted from attachment messages by traffic monitor **206** along with the GUTI for the UE. Later, the UE enters an idle state, and some network resources are released in response to the UE entering the idle state. When the UE returns to an active state, the traffic for the UE may contain the GUTI for the UE and not the IMSI. Since monitoring node load balancer **114** has correlated the GUTI with the IMSI, monitoring node load balancer **114** can continue to send tapped traffic for the UE to the monitoring node bound to the UE.

In this case, monitoring node load balancer **114** may need to decrypt the tapped traffic to determine the GUTI. Traffic monitor **206** can store an encryption key extracted from the S6a traffic. Building the table that correlates subscriber identifiers can include storing encryption keys. For example, the encryption key can be a KASME key or a key derived from a KASME key. The KASME key can be extracted from S6a traffic.

To decrypt an encrypted message, monitoring node load balancer **114** locates a corresponding encryption for the encrypted message using a key identifier, e.g., a key set identifier for the encrypted message. Decryption engine **208** then decrypts the encrypted message using the
5 located key. Monitoring node load balancer **114** can then extract the second subscriber identifier from the decrypted message and distribute the encrypted message to the monitoring node that is bound to the second subscriber identifier in the table.

Figure 3 is a call flow diagram **300** illustrating an example exchange
10 of messages monitored by the monitoring node load balancer **114**. In a first exchange **302** of messages, eNodeB **104** and MME **106** setup a connection and then UE **102** and eNodeB **104** setup a connection. In a second exchange **304** of messages **304**, eNodeB **102** initiates an attachment request with MME **106** for UE **102**.

15 During second exchange **304**, monitoring node load balancer **114** extracts the IMSI for UE **102** and the GUTI for UE **102** on the S1-MME interface by extracting the IMSI from an attachment request message and extracting the GUTI from a responsive attachment response message. Monitoring node load balancer **114** can then add both the IMSI and the GUTI
20 to a same record in a table for correlating subscriber identifiers for UEs.

Also during second exchange **304**, monitoring node load balancer **114** stores the KASME key from HSS **108** by monitoring the authentication info request (AIR) and authentication info answer (AIA) messages exchanged between MME **106** and HSS **108**. Monitoring node load
25 balancer **114** can determine which type of decryption to use based on the security mode messages exchange during second exchange **304**.

In a third exchange **306** of messages, a connection to a packet network is setup by exchanging messages with SGW **110** and PGW **112**. Monitoring node load balancer **114** may be able to appropriately distribute
30 tapped traffic during this exchange using the IMSI. However, if UE **102** later enters an idle state, releasing network resources, and then re-enters an active state, monitoring node load balancer **114** may need to use the stored KASME key to decrypt encrypted messages and extract the GUTI for UE

102 to distribute tapped traffic for UE **102** to the monitoring node bound to UE **102**.

Figure 4 is a diagram **400** illustrating an example network stack for communications between UE **102**, eNodeB **104**, and MME **106**. The top layer of the network stack is a non-access stratum (NAS) layer **402**. The NAS protocol is used on the control plane between UE **102** and MME **106**. NAS layer **402** handles mobility related functions between UE **102** and the core network, such as attachment and tracking area update and authentication and security.

When UE **102** enters an idle state, network resources associate with the layers **404** below NAS layer **402** are released. When UE **102** re-enters an active state, UE **102** may send a service request message. The service request may include the GUTI for UE **102** or a component of the GUTI such as the M-TMSI. Monitoring node load balancer **114** decrypts the service request message, using the decryption scheme for NAS layer **402** and the stored encryption key, to recover the GUTI and distribute traffic for UE **102** to the monitoring node bound to UE **102**.

Figure 5 is a flow chart illustrating an example method **500** for distributing monitored network traffic. Method **500** is performed by a monitoring node load balancer implemented using at least one processor.

The monitoring node load balancer monitors S1-MME traffic and S6a traffic in a core network of a telecommunications network (**502**). Monitoring the S1-MME traffic and S6a traffic can include extracting subscriber identifiers for subscribers to the telecommunications network.

For example, the monitoring node load balancer can build a table with a record for each subscriber attaching to the telecommunications network. Building the table can include correlating, in each record, a first subscriber identifier extracted from an attachment request in the S1-MME traffic with a second subscriber identifier extracted from an attachment response in the S1-MME traffic. The first subscriber identifier can be an IMSI and the second subscriber identifier can be a GUTI. In general, the first subscriber identifier is a permanent subscriber identifier and the second subscriber identifier is a temporary subscriber identifier.

The monitoring node load balancer decrypts encrypted S1-MME traffic using information extracted from the S6a traffic (504). Building the table can include storing one or more encryption keys extracted from the S6a traffic. The encryption keys are stored on an HSS for UEs attaching to the telecommunications network. For example, the encryption key can be a KASME key or any other appropriate key derived from or associated with the KASME key. Decrypting an encrypted message can include locating a corresponding encryption key using a key identifier for the encrypted message and decrypting the encrypted message using the encryption key.

10 The monitoring node load balancer load balances between monitoring nodes using the decrypted S1-MME traffic (506). Load balancing can include distributing tapped traffic from the core network across the monitoring nodes using subscriber identifiers, i.e., by binding each subscriber identifier to a monitoring node. For example, the monitoring node load balancer can extract subscriber identifiers from the decrypted S1-MME traffic and use the extracted subscriber identifiers for load balancing.

Accordingly, while the methods, systems, and computer readable media have been described herein in reference to specific embodiments, features, and illustrative embodiments, it will be appreciated that the utility of the subject matter is not thus limited, but rather extends to and encompasses numerous other variations, modifications and alternative embodiments, as will suggest themselves to those of ordinary skill in the field of the present subject matter, based on the disclosure herein.

Various combinations and sub-combinations of the structures and features described herein are contemplated and will be apparent to a skilled person having knowledge of this disclosure. Any of the various features and elements as disclosed herein may be combined with one or more other disclosed features and elements unless indicated to the contrary herein. Correspondingly, the subject matter as hereinafter claimed is intended to be broadly construed and interpreted, as including all such variations, modifications and alternative embodiments, within its scope and including equivalents of the claims.

It is understood that various details of the presently disclosed subject matter may be changed without departing from the scope of the presently disclosed subject matter. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

CLAIMS

What is claimed is:

1. A method for distributing monitored network traffic, the method comprising:
 - 5 at a monitoring node load balancer implemented using at least one processor:
 - monitoring S1-MME traffic and S6a traffic in a core network of a telecommunications network;
 - decrypting encrypted S1-MME traffic using information extracted from
 - 10 the S6a traffic; and
 - load balancing between a plurality of monitoring nodes using the decrypted S1-MME traffic.
2. The method of claim 1, wherein monitoring the S1-MME traffic and S6a traffic comprises extracting subscriber identifiers for subscribers to the
- 15 telecommunications network.
3. The method of claim 2, wherein load balancing comprises distributing tapped traffic from the core network across the plurality of monitoring nodes using the subscriber identifiers.
4. The method of claim 1, wherein monitoring the S1-MME traffic and
- 20 S6a traffic comprises building a table with a record for each subscriber of a plurality of subscribers attaching to the telecommunications network.
5. The method of claim 4, wherein building the table comprises correlating, in each record, a first subscriber identifier extracted from an attachment request in the S1-MME traffic with a second subscriber identifier
- 25 extracted from an attachment response in the S1-MME traffic.
6. The method of claim 5, wherein the first subscriber identifier is an international mobile subscriber identity (IMSI) and the second subscriber identifier is a globally unique temporary UE identity (GUTI).
7. The method of claim 5, wherein building the table comprises storing
- 30 an encryption key extracted from the S6a traffic.
8. The method of claim 7, wherein the encryption key comprises a KASME key.

9. The method of claim 7, wherein decrypting the encrypted S1-MME traffic comprises locating, for an encrypted message, a corresponding encryption key using a key identifier for the encrypted message and decrypting the encrypted message using the encryption key.
- 5 10. The method of claim 9, wherein decrypting the encrypted message comprises extracting the second subscriber identifier from the encrypted message and using the second subscriber identifier for load balancing.
11. A system for distributed monitored network traffic, the system comprising:
- 10 at least one processor; and
a monitoring node load balancer implemented using the at least one processor;
- wherein the monitoring node load balancer is configured for monitoring S1-MME traffic and S6a traffic in a core network of a telecommunications network; decrypting encrypted S1-MME traffic using
15 information extracted from the S6a traffic; and load balancing between a plurality of monitoring nodes using the decrypted S1-MME traffic.
12. The system of claim 11, wherein monitoring the S1-MME traffic and S6a traffic comprises extracting subscriber identifiers for subscribers to the
20 telecommunications network.
13. The system of claim 12, wherein load balancing comprises distributing tapped traffic from the core network across the plurality of monitoring nodes using the subscriber identifiers.
14. The system of claim 11, wherein monitoring the S1-MME traffic and
25 S6a traffic comprises building a table with a record for each subscriber of a plurality of subscribers attaching to the telecommunications network.
15. The system of claim 14, wherein building the table comprises correlating, in each record, a first subscriber identifier extracted from an attachment request in the S1-MME traffic with a second subscriber identifier
30 extracted from an attachment response in the S1-MME traffic.
16. The system of claim 15, wherein the first subscriber identifier is an international mobile subscriber identity (IMSI) and the second subscriber identifier is a globally unique temporary UE identity (GUTI).

17. The system of claim 15, wherein building the table comprises storing an encryption key extracted from the S6a traffic.
18. The system of claim 17, wherein the encryption key comprises a KASME key.
- 5 19. The system of claim 17, wherein decrypting the encrypted S1-MME traffic comprises locating, for an encrypted message, a corresponding encryption key using a key identifier for the encrypted message and decrypting the encrypted message using the encryption key.
20. The system of claim 19, wherein decrypting the encrypted message
10 comprises extracting the second subscriber identifier from the encrypted message and using the second subscriber identifier for load balancing.
21. One or more non-transitory computer readable mediums storing instructions for at least one processor that, when executed by the at least one processor, cause the at least one processor to perform operations
15 comprising:
- monitoring S1-MME traffic and S6a traffic in a core network of a telecommunications network;
 - decrypting encrypted S1-MME traffic using information extracted from the S6a traffic; and
 - 20 load balancing between a plurality of monitoring nodes using the decrypted S1-MME traffic.

1/5

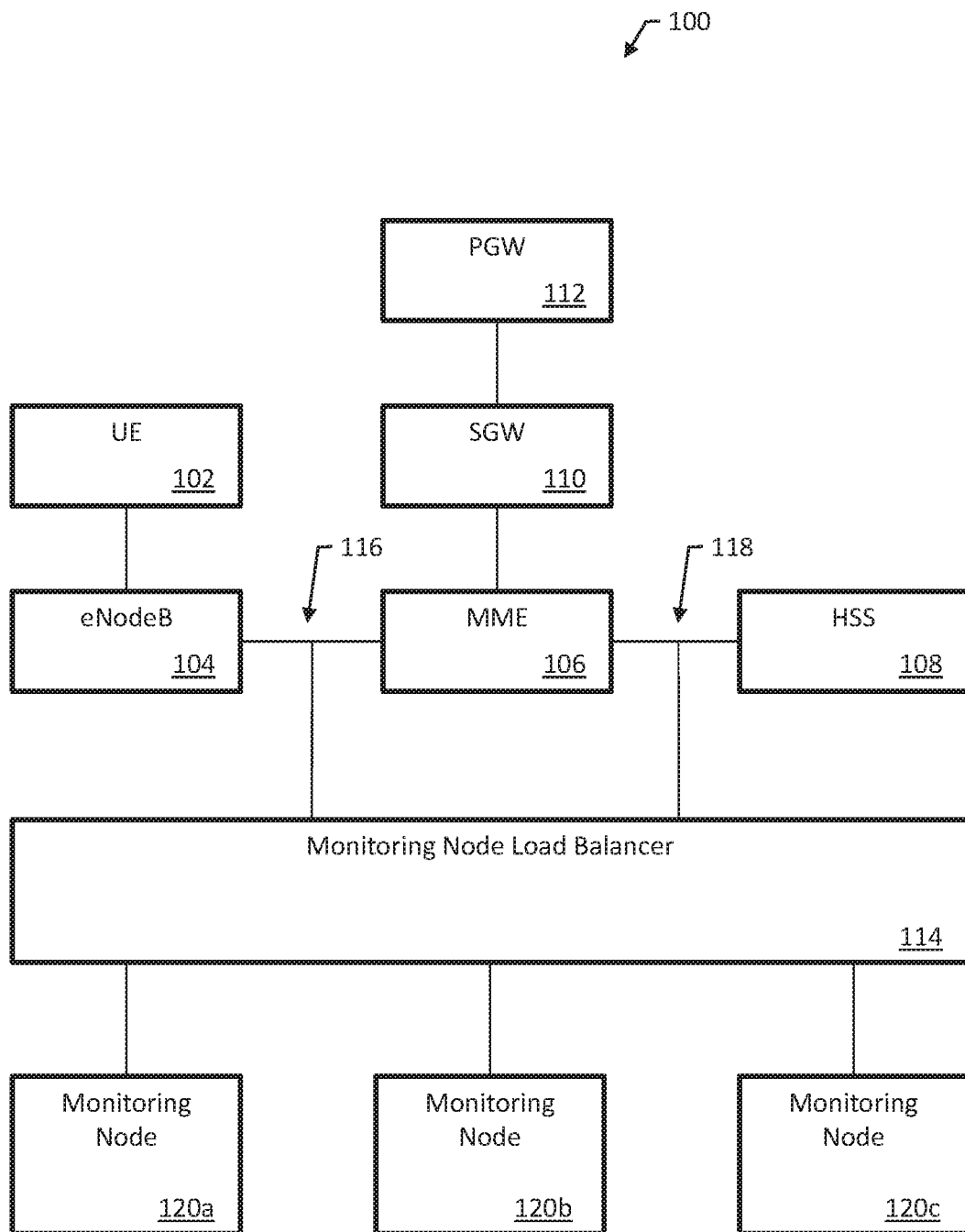


FIG. 1

2/5

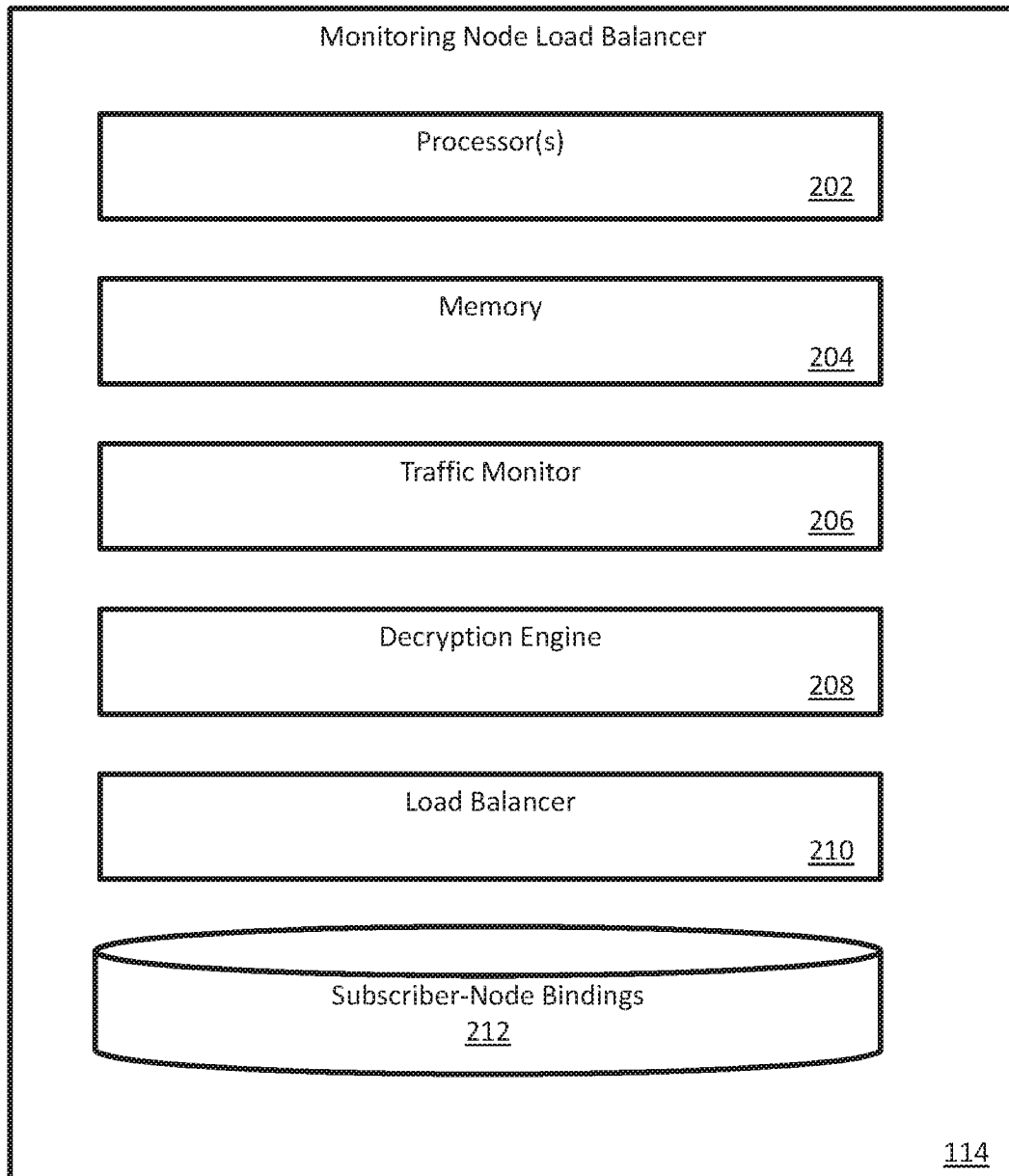


FIG. 2

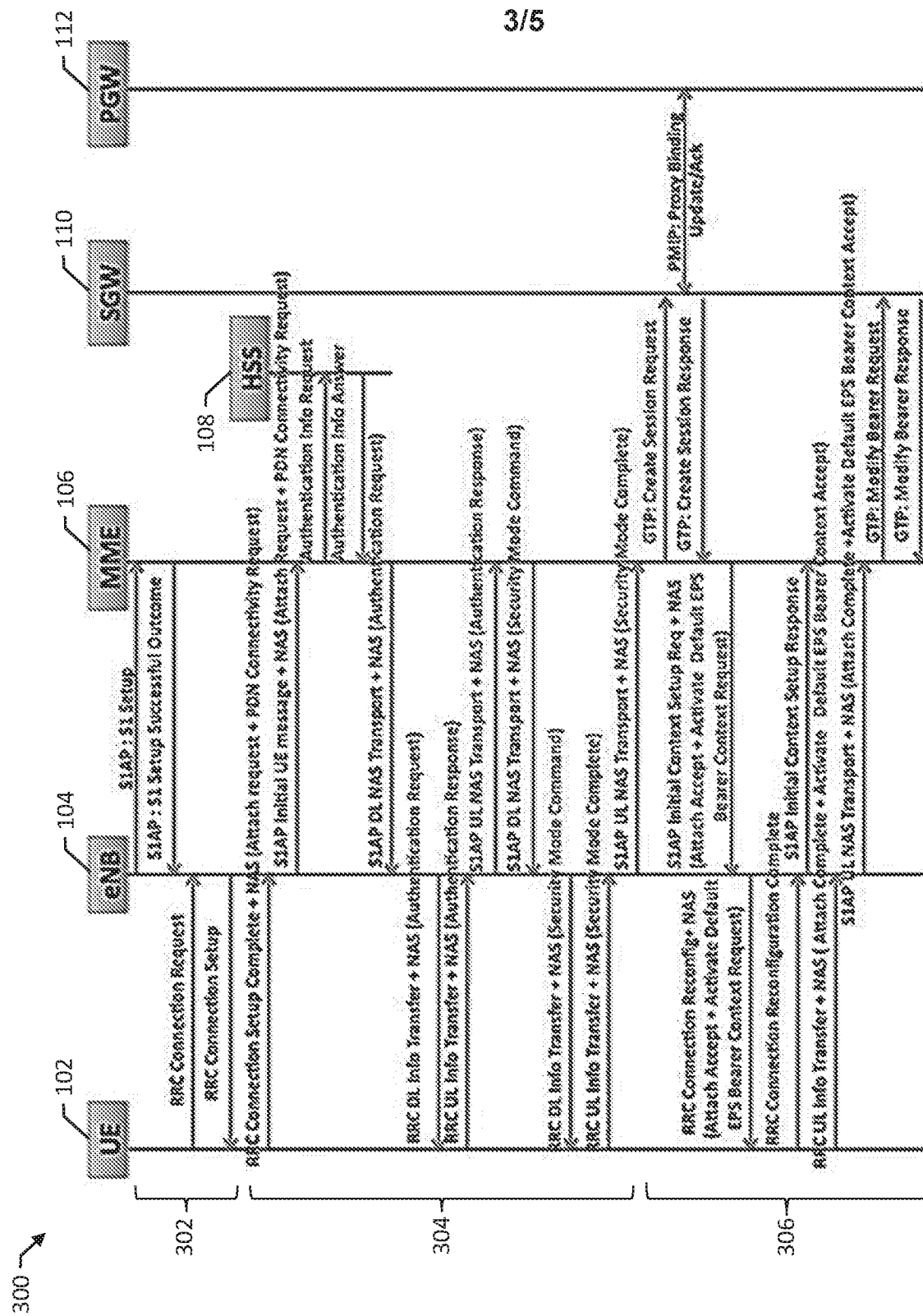


FIG. 3

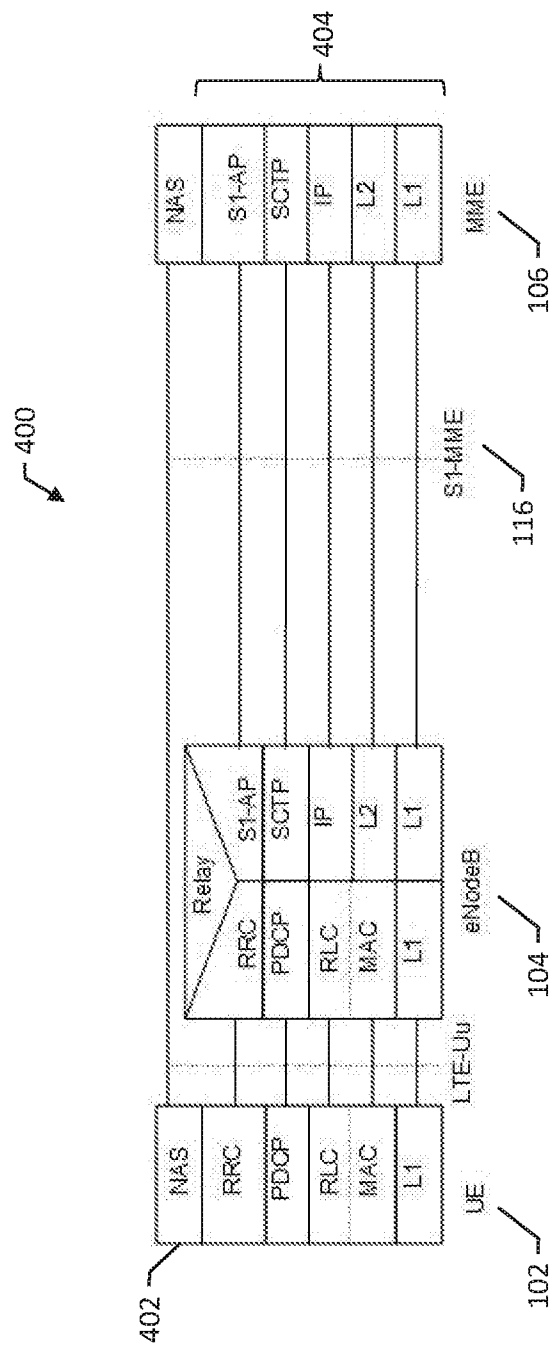


FIG. 4

5/5

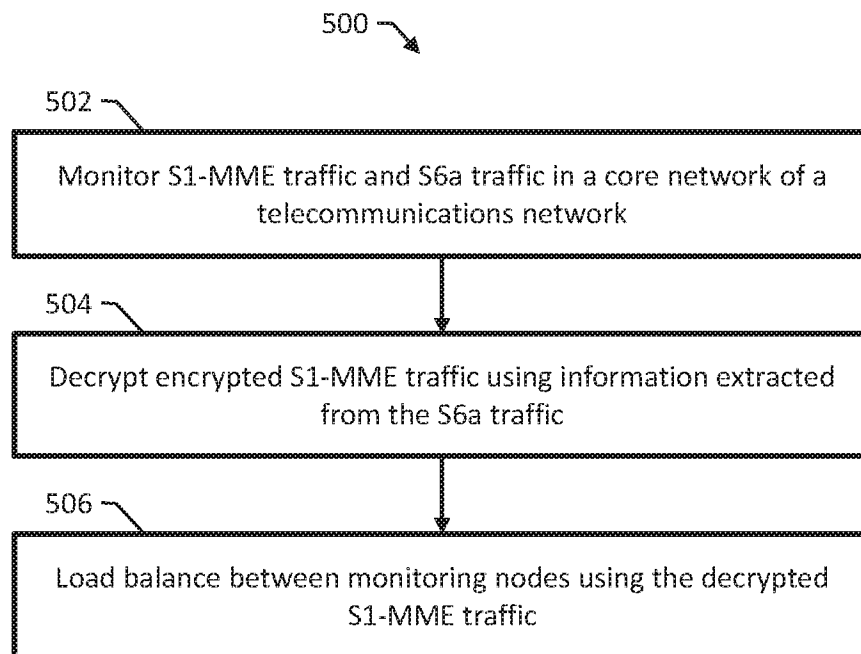


FIG. 5

A. CLASSIFICATION OF SUBJECT MATTER**H04W 28/08(2009.01)i, H04W 24/08(2009.01)i, H04W 12/08(2009.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 28/08; H04W 24/00; H04L 12/26; H04W 4/00; H04L 12/28; H04W 12/04; H04L 12/56; H04W 24/08; H04W 12/08

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: monitor, network traffic, load balance, S1-MME, S6a, decrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012-0155324 A1 (VIGNESH JANAKIRAMAN et al.) 21 June 2012 See paragraphs [0013]–[0056]; claims 1–18; and figures 1–2.	1–21
Y	US 2013-0272127 A1 (SYED MUNTAQA ALI et al.) 17 October 2013 See paragraphs [0044]–[0061]; claims 1–16; and figures 3–6.	1–21
Y	US 2013-0269001 A1 (TEKTRONIX, INC.) 10 October 2013 See paragraphs [0025]–[0042]; and claim 10.	8–10, 18–20
A	US 2012-0063300 A1 (YILDIRIM SAHIN et al.) 15 March 2012 See paragraphs [0052]–[0140]; and claims 1–11.	1–21
A	US 2015-0043353 A1 (CELLOS SOFTWARE LTD.) 12 February 2015 See paragraphs [0075]–[0144]; and claims 1–18.	1–21



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

21 April 2017 (21.04.2017)

Date of mailing of the international search report

21 April 2017 (21.04.2017)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea



Facsimile No. +82-42-481-8578

Authorized officer

YANG, Jeong Rok

Telephone No. +82-42-481-5709



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/012740

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0155324 A1	21/06/2012	CN 102685769 A EP 2469761 A1 EP 2469761 B1 JP 2012-156988 A US 8924572 B2	19/09/2012 27/06/2012 30/04/2014 16/08/2012 30/12/2014
US 2013-0272127 A1	17/10/2013	CN 103516710 A EP 2654366 A1 EP 2654366 B1 US 8902754 B2	15/01/2014 23/10/2013 19/11/2014 02/12/2014
US 2013-0269001 A1	10/10/2013	CN 102769848 A EP 2469752 A1 JP 2012-134975 A US 2012-0159151 A1 US 9071962 B2	07/11/2012 27/06/2012 12/07/2012 21/06/2012 30/06/2015
US 2012-0063300 A1	15/03/2012	CA 2811467 A1 CN 103202064 A EP 2617235 A2 EP 2617235 B1 EP 2693806 A2 EP 2693806 A3 JP 05957454 B2 JP 06063530 B2 JP 2013-537387 A JP 2015-195622 A KR 10-2013-0107302 A US 8848516 B2 WO 2012-035450 A2 WO 2012-035450 A3	22/03/2012 10/07/2013 24/07/2013 05/10/2016 05/02/2014 24/12/2014 27/07/2016 18/01/2017 30/09/2013 05/11/2015 01/10/2013 30/09/2014 22/03/2012 10/05/2012
US 2015-0043353 A1	12/02/2015	AU 2014-208273 A1 US 2016-0127933 A1 US 9277429 B2 US 9439094 B2	26/02/2015 05/05/2016 01/03/2016 06/09/2016