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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2019 (14.02.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/032236 A1

(51) International Patent Classification:
H04W 60/00 (2009.01) *H04W 8/06* (2009.01)
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/US2018/041815

(22) International Filing Date:
12 July 2018 (12.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/543,473 10 August 2017 (10.08.2017) US
16/031,803 10 July 2018 (10.07.2018) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, ATTN: International IP Administration, San Diego, California 92121-1714 (US).

(72) Inventors: **SESHADRI, Swathi**; 5775 Morehouse Drive, San Diego, California 92121 (US). **TINA, Cogol**; 5775 Morehouse Drive, San Diego, California 92121 (US). **BHATNAGAR, Abhishek**; 5775 Morehouse Drive, San Diego, California 92121 (US). **AGRAWAL, Mona**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agent: **MYUNG, Hyung G.**; 5775 Morehouse Drive, ATTN: International IP Administration, San Diego, California 92121-1714 (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, JO, 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).

(54) Title: FORBIDDEN NETWORK LIST MANAGEMENT

(57) Abstract: Methods, systems, and devices for wireless communication are described. A user equipment (UE) may be configured to include procedures to mitigate denial of service (DoS) attack by a rogue base station when the initial non-access stratum (NAS) messages between the UE and a mobility management entity (MME) is unprotected. UE may maintain a temporary forbidden network list, which resides outside a subscriber identity module (SIM), and update a forbidden network list, which resides on the SIM, only under certain conditions. For example, a visited network, from which the UE receives a reject message, may be added to the forbidden network list on the SIM only when a counter associated with the visited network is equal to a maximum counter value, which is configured by the UE.

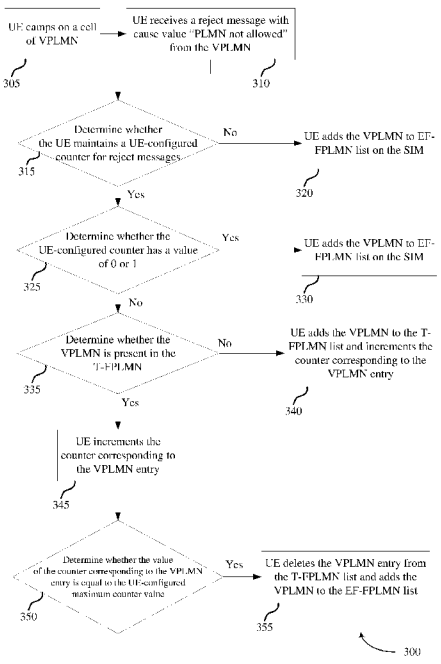

FIG. 3

[Continued on next page]

WO 2019/032236 A1

Published:
— *with international search report (Art. 21(3))*

FORBIDDEN NETWORK LIST MANAGEMENT

[0001] This application claims the benefit of U.S. Provisional Application No. 62/543,473, filed August 10, 2017, and Application No. 16/031,803, filed July 10, 2018, the entire content of which is hereby incorporated by reference.

BACKGROUND

FIELD OF THE DISCLOSURE

[0002] The following relates generally to wireless communication, and more specifically to management of a forbidden network list for a user equipment (UE).

DESCRIPTION OF RELATED ART

[0003] Wireless communications systems are widely deployed to provide various types of communication content such as voice, video, packet data, messaging, broadcast, and so on. These systems may be capable of supporting communication with multiple users by sharing the available system resources (e.g., time, frequency, and power). Examples of such multiple-access systems include fourth generation (4G) systems such as a Long Term Evolution (LTE) systems or LTE-Advanced (LTE-A) systems, and fifth generation (5G) systems which may be referred to as New Radio (NR) systems. A wireless multiple-access communications system may include a number of base stations or network access nodes, each simultaneously supporting communication for multiple communication devices, which may be otherwise known as user equipment (UE).

[0004] A non-access stratum (NAS) layer is a set of protocols used to convey non-radio signaling between a UE and a mobility management entity (MME) for access to a network (such as a Long Term Evolution (LTE) network or an evolved universal mobile telephone system (UMTS) terrestrial radio access network (E-UTRAN)). The main functions of the protocols that are a part of the NAS may include the support of UE mobility, evolved packet system (EPS) bearer management, authentication, security control, and connection management. A UE may communicate with the NAS via messages transmitted between the UE and the NAS. Typically, a first NAS message between a UE and an MME may be an attach request, though other message types may include a service request or a connectivity request message.

[0005] The initial messages sent between a UE and an MME may be unprotected. Thus, the unprotected NAS messages may be intercepted and exploited by attackers such as a rogue base station. In another instance, the rogue base station may launch a denial of service (DoS) attack on the UE.

SUMMARY

[0006] The described techniques relate to improved methods, systems, devices, or apparatuses that support management of a forbidden network list on a subscriber identity module (SIM) in a user equipment (UE) in accordance with various aspects of the present disclosure.

[0007] A method of wireless communication is described. The method may include receiving a message from a visited network, determining that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on the UE, outside a subscriber identity module (SIM), determining a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list, incrementing the counter associated with the visited network in response to the visited network being in the first forbidden network, in response to the value of the counter being equal to a maximum counter value: deleting the visited network from the first forbidden network list and adding the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

[0008] An apparatus for wireless communication is described. The apparatus may include means for receiving a message from a visited network, means for determining that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on a user equipment (UE), outside a subscriber identity module (SIM), means for determining a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list, means for incrementing the counter associated with the visited network in response to the visited network being in the first forbidden network, in response to the value of the counter being equal to a maximum counter value: means for deleting the visited network from the first forbidden network list and means for adding the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

[0009] Another apparatus for wireless communication is described. The apparatus may include a processor, memory in electronic communication with the processor, and

instructions stored in the memory. The instructions may be executable by the processor to cause the apparatus to receive a message from a visited network, determine that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on a user equipment (UE), outside a subscriber identity module (SIM), determine a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list, increment the counter associated with the visited network in response to the visited network being in the first forbidden network; in response to the value of the counter being equal to a maximum counter value: delete the visited network from the first forbidden network list and add the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

[0010] A non-transitory computer readable medium storing code for wireless communication is described. The code may include instructions executable by a processor receive a message from a visited network, determine that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on a user equipment (UE), outside a subscriber identity module (SIM), determine a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list, increment the counter associated with the visited network in response to the visited network being in the first forbidden network; in response to the value of the counter being equal to a maximum counter value: delete the visited network from the first forbidden network list and add the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 illustrates an example of a system for wireless communication.

[0012] FIG. 2 shows block diagrams of a device that supports management of a forbidden network list on a SIM in a UE in accordance with aspects of the present disclosure.

[0013] FIG. 3 illustrates methods for management of a forbidden network list on a SIM in a UE in accordance with aspects of the present disclosure.

[0014] FIG. 4 illustrates methods for management of a forbidden network list when the UE powered off or the SIM is removed in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0015] A non-access stratum (NAS) layer is a set of protocols used to convey non-radio signaling between a UE and a mobility management entity (MME) for access to a network (such as a Long Term Evolution (LTE) network or an evolved universal mobile telephone system (UMTS) terrestrial radio access network (E-UTRAN)). The main functions of the protocols that are a part of the NAS may include the support of UE mobility, evolved packet-switched system (EPS) bearer management, authentication, security control, and connection management. A UE may communicate with the NAS via messages transmitted between the UE and the NAS. Typically, a first NAS message between a UE and an MME may be an attach request, though other message types may include a service request or a connectivity request message. If the UE is new to the network the MME may also ask for the UE's identity (e.g., an international mobile subscriber identify (IMSI)).

[0016] When a UE is switched on, it attempts to make contact with a public land mobile network (PLMN). A PLMN may be identified by a mobile country code (MCC) and a mobile network code (MNC). The particular PLMN to be contacted may be selected either automatically or manually. The UE looks for a suitable cell of the chosen PLMN and chooses that cell to provide available services and tunes to its control channel. This choosing, or selection, is known as "camping on the cell". The term "cell" refers to a logical communication entity used for communication with a base station (e.g., over a carrier) and may be associated with an identifier for distinguishing neighboring cells (e.g., a physical cell identifier (PCID), a virtual cell identifier (VCID)) operating via the same or a different carrier. The UE may then register its presence in the registration area of the chosen cell if necessary, by means of a location registration (LR), general packet radio service (GPRS) attach, or IMSI attach procedure. If the UE loses coverage of a cell, or find a more suitable cell, it reselects onto the most suitable cell of the selected PLMN and camps on that cell. If the new cell is in a different registration area, an LR request is performed. If the UE loses coverage of a PLMN,

either a new PLMN is selected automatically, or an indication of which PLMNs are available is given to the user, so that a manual selection can be made.

[0017] The UE normally operates on its home PLMN (HPLMN) or equivalent home PLMN (EHPLMN). However, a visited PLMN (VPLMN) may be selected, e.g., if the UE loses coverage from HPLMN or EHPLMN. VPLMN is a PLMN different from the HPLMN (if the EHPLMN list is not present or is empty) or different from an EHPLMN (if the EHPLMN list is present). To prevent repeated attempts to have roaming service on a not allowed area, for example, local area (LA) or tracking area (TA), when the UE is informed that an area is forbidden, the LA or TA is added to a list of "forbidden location areas for roaming" or "forbidden tracking areas for roaming" respectively which is stored in the UE. These lists, if existing, are deleted when the UE is switched off or when the SIM is removed. If a message with cause value "PLMN not allowed" is received by the UE in response to an LR request from a VPLMN, that VPLMN is added to a list of "forbidden PLMNs" in the SIM of the UE and thereafter that VPLMN will not be accessed by the UE, for example, when in automatic mode. Cause value “PLMN not allowed” is also referred to as EPS mobility management (EMM) cause #11, which is sent to the UE if the UE requests service, or if the network initiates a detach request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate. That PLMN is removed from the "forbidden PLMNs" list if, after a subsequent manual selection of the PLMN, there is a successful LR. This list is retained when the UE is switched off or the SIM is removed. The HPLMN (if the EHPLMN list is not present or is empty) or the EHPLMN (if the EHPLMN list is present) shall not be stored on the list of forbidden PLMNs.

[0018] The initial messages sent between a UE and an MME may be unprotected. Thus, the unprotected NAS messages may be intercepted and exploited by attackers such as a rogue base station. In another instance, the rogue base station may launch a denial of service (DoS) attack on the UE. For example, a rogue base station may receive a tracking area update (TAU) request message in message and the rogue base station may reject the TAU request from the UE in reject message which may cause the UE to consider a subscriber identity module (SIM) as invalid for EPS services and non-EPS services until the UE switches off or the card containing the SIM is removed.

[0019] Accordingly, the UE may include procedures to mitigate such DoS attack by a rogue base station. UE may maintain a temporary forbidden network list, such as temporary forbidden PLMN (T-FPLMN) list, which resides outside the SIM, and update a forbidden network list, such as elementary file forbidden PLMN (EF-FPLMN) list, which resides on the SIM, only under certain conditions.

[0020] Aspects of the disclosure are initially described in the context of a wireless communications system. Specific examples are described for managing a forbidden network list on a subscriber identity module (SIM) in a user equipment (UE). Aspects of the disclosure are further illustrated by and described with reference to apparatus diagrams, system diagrams, and flowcharts that relate to management of a forbidden network list on a SIM in a UE.

[0021] **FIG. 1** illustrates an example of a wireless communications system 100 that supports management of a forbidden network list on a subscriber identity module (SIM) in a user equipment (UE) in accordance with various aspects of the present disclosure. The wireless communications system 100 includes base stations 105, UEs 115, and a core network 130. In some examples, the wireless communications system 100 may be a Global System for Mobile (GSM) network, a Universal Mobile Telecommunications System (UMTS) network, a Long Term Evolution (LTE) network, an LTE-Advanced (LTE-A) network, or a New Radio (NR) network. In some cases, wireless communications system 100 may support enhanced broadband communications, ultra-reliable (e.g., mission critical) communications, low latency communications, or communications with low-cost and low-complexity devices.

[0022] Base stations 105 may wirelessly communicate with UEs 115 via one or more base station antennas. Base stations 105 described herein may include or may be referred to by those skilled in the art as a base transceiver station, a radio base station, an access point, a radio transceiver, a NodeB, an eNodeB (eNB), a next-generation Node B or giga-nodeB (either of which may be referred to as a gNB), a Home NodeB, a Home eNodeB, or some other suitable terminology. Wireless communications system 100 may include base stations 105 of different types (e.g., macro or small cell base stations). The UEs 115 described herein may be able to communicate with various types of base stations 105 and network equipment including macro eNBs, small cell eNBs, gNBs, relay base stations, and the like.

[0023] Each base station 105 may be associated with a particular geographic coverage area 110 in which communications with various UEs 115 is supported. Each base station 105 may provide communication coverage for a respective geographic coverage area 110 via communication links 125, and communication links 125 between a base station 105 and a UE 115 may utilize one or more carriers. Communication links 125 shown in wireless communications system 100 may include uplink transmissions from a UE 115 to a base station 105, or downlink transmissions, from a base station 105 to a UE 115. Downlink transmissions may also be called forward link transmissions while uplink transmissions may also be called reverse link transmissions.

[0024] The geographic coverage area 110 for a base station 105 may be divided into sectors making up only a portion of the geographic coverage area 110, and each sector may be associated with a cell. For example, each base station 105 may provide communication coverage for a macro cell, a small cell, a hot spot, or other types of cells, or various combinations thereof. In some examples, a base station 105 may be movable and therefore provide communication coverage for a moving geographic coverage area 110. In some examples, different geographic coverage areas 110 associated with different technologies may overlap, and overlapping geographic coverage areas 110 associated with different technologies may be supported by the same base station 105 or by different base stations 105. The wireless communications system 100 may include, for example, a heterogeneous LTE/LTE-A or NR network in which different types of base stations 105 provide coverage for various geographic coverage areas 110.

[0025] UEs 115 may be dispersed throughout the wireless communications system 100, and each UE 115 may be stationary or mobile. A UE 115 may also be referred to as a mobile device, a wireless device, a remote device, a handheld device, or a subscriber device, or some other suitable terminology, where the "device" may also be referred to as a unit, a station, a terminal, or a client. A UE 115 may also be a personal electronic device such as a cellular phone, a personal digital assistant (PDA), a tablet computer, a laptop computer, or a personal computer. In some examples, a UE 115 may also refer to a wireless local loop (WLL) station, an Internet of Things (IoT) device, an Internet of Everything (IoE) device, or a Machine-Type Communication (MTC) device, or the like, which may be implemented in various articles such as appliances, vehicles, meters, or the like.

[0026] Base stations 105 may communicate with the core network 130 and with one another. For example, base stations 105 may interface with the core network 130 through backhaul links 132 (e.g., via an S1 or other interface). Base stations 105 may communicate with one another over backhaul links 134 (e.g., via an X2 or other interface) either directly (e.g., directly between base stations 105) or indirectly (e.g., via core network 130).

[0027] The core network 130 may provide user authentication, access authorization, tracking, Internet Protocol (IP) connectivity, and other access, routing, or mobility functions. The core network 130 may be an evolved packet core (EPC), which may include at least one mobility management entity (MME), at least one serving gateway (S-GW), and at least one Packet Data Network (PDN) gateway (P-GW). The MME may manage non-access stratum (e.g., control plane) functions such as mobility, authentication, and bearer management for UEs 115 served by base stations 105 associated with the EPC. User IP packets may be transferred through the S-GW, which itself may be connected to the P-GW. The P-GW may provide IP address allocation as well as other functions. The P-GW may be connected to the network operators IP services. The operators IP services may include access to the Internet, Intranet(s), an IP Multimedia Subsystem (IMS), or a Packet-Switched (PS) Streaming Service.

[0028] Communications between a UE 115 and a core network 130 may include non-access stratum (NAS) communications. As explained herein, a NAS layer is a functional layer used in the protocol stacks between a UE 115 and a core network 130, and may be implemented by an MME located at the core network 130. In some examples, a first NAS message between a UE 115 and an MME may be an attach request. The initial messages sent between a UE and an MME may be unprotected. Thus, the unprotected NAS messages may be intercepted and exploited by attackers such as a rogue base station. In another instance, the rogue base station may launch a denial of service (DoS) attack on the UE. For example, a rogue base station may receive a tracking area update (TAU) request message in message and the rogue base station may reject the TAU request from the UE in reject message which may cause the UE to consider a subscriber identity module (SIM) as invalid for EPS services and non-EPS services until the UE switches off or the card containing the SIM is removed.

[0029] **FIG. 2** shows a block diagram 200 of a wireless device 205 that supports management of a forbidden network list on a subscriber identity module (SIM) in a user equipment (UE) in accordance with aspects of the present disclosure. Wireless device 205 may be an example of aspects of a UE 115 as described herein. Wireless device 205 may include memory 210, processor 220, transceiver 225, antenna 230 and SIM 235. Each of these modules may communicate, directly or indirectly, with one another (e.g., via one or more buses).

[0030] The memory 210 may include random access memory (RAM) and read only memory (ROM). The memory 210 may store computer-readable, computer-executable software including instructions that, when executed, cause the processor to perform various functions described herein. In some cases, the software 215 may not be directly executable by the processor but may cause a computer (e.g., when compiled and executed) to perform functions described herein.

[0031] The transceiver 225 may communicate bi-directionally, via one or more antennas, wired, or wireless links, with one or more networks, as described above. For example, the transceiver 225 may communicate bi-directionally with a base station 105 or a UE 115. The transceiver 225 may also include a modem to modulate the packets and provide the modulated packets to the antennas for transmission, and to demodulate packets received from the antennas.

[0032] The processor 220 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a central processing unit (CPU), a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some cases, processor 220 may be configured to operate a memory array using a memory controller. In other cases, a memory controller may be integrated into processor 220. Processor 220 may be configured to execute computer-readable instructions stored in a memory to perform various functions (e.g., functions or tasks supporting management of a forbidden network list on a SIM in a UE in accordance with aspects of the present disclosure). The term processor is used herein in accordance with its meaning as structure.

[0033] The software 215 may include code to implement aspects of the present disclosure, including code to support management of a forbidden network list on a SIM

in a UE in accordance with aspects of the present disclosure. Software 215 may be stored in a non-transitory computer-readable medium such as system memory or other memory. In some cases, the software 215 may not be directly executable by the processor but may cause a computer (e.g., when compiled and executed) to perform functions described herein.

[0034] In some cases, the wireless device may include a single antenna 230. However, in some cases the device may have more than one antenna 230, which may be capable of concurrently transmitting or receiving multiple wireless transmissions.

[0035] The SIM 235 may be an integrated circuit (IC) that securely stores an international mobile subscriber identify (IMSI) and the related key used to identify and authenticate a UE 115. SIM 235 may also contain a unique serial number, e.g., an integrated circuit card identification (ICCID), security authentication and ciphering information, temporary information related to the local network, a list of the services, a personal identification number (PIN), and a PIN unblocking key (PUK) for PIN unlocking. In some cases, SIM 235 may be a circuit embedded in a removable card or directly embedded on the UE. SIM may be also referred to as universal subscriber identity module (USIM) in LTE network.

[0036] **FIG. 3** shows a flowchart illustrating a method 300 for management of a forbidden network list on a subscriber identity module (SIM) in a user equipment (UE) in accordance with aspects of the present disclosure. The operations of method 300 may be implemented by a UE 115 or its components as described herein. For example, the operations of method 300 may be performed by a processor as described with reference to FIG. 2. In some examples, a UE 115 may execute a set of codes to control the functional elements of the device to perform the functions described below. Additionally or alternatively, the UE 115 may perform aspects of the functions described below using special-purpose hardware.

[0037] At block 305 the UE 115 may camp on a cell of a visited PLMN (VPLMN). Camping on a cell of a VPLMN refers to the UE searching for a suitable cell of the VPLMN, choosing (or selecting) that cell to provide available services, and tuning to its control channel.

[0038] At block 310 the UE receives a reject message with cause value "PLMN not allowed" (also referred to as EMM cause #11), which indicates that the VPLMN is not

allowed, from the VPLMN. The reject message may include Attach Reject, tracking area update (TAU) Reject, or Service Reject messages. Further, the reject message may be a non-integrity protected or plain reject message.

[0039] At block 315 the UE determines whether it maintains a UE-configured counter for reject messages. The UE-configured counter may be any PLNM-specific counter maintained by the UE. At block 320, if the UE does not maintain a UE-configured counter for reject messages, the UE adds the VPLMN to an elementary file forbidden PLMN (EF-FPLMN) list, which resides on the SIM of the UE. For example, the UE may electronically store or write the VPLMN identification in the EF-FPLMN list.

[0040] At block 325, after the UE determines that it maintains a UE-configured counter for reject messages, the UE determines whether the UE-configured counter has a value of 0 or 1. At block 330, if the UE-configured counter has a value of 0 or 1, the UE adds the VPLMN to the EF-FPLMN list, which resides on the SIM of the UE. For example, the UE may electronically store or write the VPLMN identification in the EF-FPLMN list on the SIM of the UE. At block 335, if the UE-configured counter has a value of 2 or greater, the UE determines whether the VPLMN is present in the temporary forbidden PLMN (T-FPLMN) list in the UE's memory outside the SIM. For example, the UE may electronically search for the VPLMN identification in the T-FPLMN list in the UE's memory.

[0041] At block 340, if the VPLMN is not found in the T-FPLMN list in the UE's memory, the UE adds the VPLMN to the T-FPLMN list in the UE's memory and increments the counter corresponding to that VPLMN entry. At block 345, if the VPLMN is found in the T-FPLMN list in the UE's memory, the UE increments the counter corresponding to that VPLMN entry.

[0042] At block 350 the UE determines whether the value of the counter corresponding to the VPLMN entry is equal to the UE-configured maximum counter value. If the value of the counter corresponding to the VPLMN entry is not equal to the UE-configured maximum counter value, no action is further taken. At block 355, if the value of the counter corresponding to the VPLMN entry is equal to the UE-configured maximum counter value, the UE deletes the VPLMN entry from the T-FPLMN list in the UE's memory and adds the VPLMN to the EF-FPLMN list on the SIM.

[0043] **FIG. 4** shows a flowchart illustrating a further method 400 for management of a forbidden network list on a subscriber identity module (SIM) in a user equipment (UE) in accordance with aspects of the present disclosure. The operations of method 400 may be implemented by a UE 115 or its components as described herein. For example, the operations of method 400 may be performed by a processor as described with reference to FIG. 2. In some examples, a UE 115 may execute a set of codes to control the functional elements of the device to perform the functions described below. Additionally or alternatively, the UE 115 may perform aspects of the functions described below using special-purpose hardware.

[0044] At block 405, the SIM is removed or UE is powered off. At block 410, all entries in the T-FPLMN list in the UE's memory are cleared, or deleted, when the SIM is removed or UE is powered off. Hence, the entries in the T-FPLMN list does not get stored on the SIM's EF-FPLMN list at the time of the removal or power off, or afterwards.

[0045] Techniques described herein may be used for various wireless communications systems such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), orthogonal frequency division multiple access (OFDMA), single carrier frequency division multiple access (SC-FDMA), and other systems. A CDMA system may implement a radio technology such as CDMA2000, Universal Terrestrial Radio Access (UTRA), etc. CDMA2000 covers IS-2000, IS-95, and IS-856 standards. IS-2000 Releases may be commonly referred to as CDMA2000 1X, 1X, etc. IS-856 (TIA-856) is commonly referred to as CDMA2000 1xEV-DO, High Rate Packet Data (HRPD), etc. UTRA includes Wideband CDMA (WCDMA) and other variants of CDMA. A TDMA system may implement a radio technology such as Global System for Mobile Communications (GSM).

[0046] An OFDMA system may implement a radio technology such as Ultra Mobile Broadband (UMB), Evolved UTRA (E-UTRA), Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM, etc. UTRA and E-UTRA are part of Universal Mobile Telecommunications System (UMTS). LTE and LTE-A are releases of UMTS that use E-UTRA. UTRA, E-UTRA, UMTS, LTE, LTE-A, NR, and GSM are described in documents from the organization

named "3rd Generation Partnership Project" (3GPP). CDMA2000 and UMB are described in documents from an organization named "3rd Generation Partnership Project 2" (3GPP2). The techniques described herein may be used for the systems and radio technologies mentioned above as well as other systems and radio technologies. While aspects of an LTE or an NR system may be described for purposes of example, and LTE or NR terminology may be used in much of the description, the techniques described herein are applicable beyond LTE or NR applications.

[0047] Information and signals described herein may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0048] The various illustrative blocks and modules described in connection with the disclosure herein may be implemented or performed with a general-purpose processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA) or other programmable logic device (PLD), discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices (e.g., a combination of a DSP and a microprocessor, multiple microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration).

[0049] The functions described herein may be implemented in hardware, software executed by a processor, firmware, or any combination thereof. If implemented in software executed by a processor, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Other examples and implementations are within the scope of the disclosure and appended claims. For example, due to the nature of software, functions described above can be implemented using software executed by a processor, hardware, firmware, hardwiring, or combinations of any of these. Features implementing functions may also be physically

located at various positions, including being distributed such that portions of functions are implemented at different physical locations.

[0050] Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, non-transitory computer-readable media may comprise random-access memory (RAM), read-only memory (ROM), electrically erasable programmable read only memory (EEPROM), flash memory, compact disk (CD) ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium that can be used to carry or store desired program code means in the form of instructions or data structures and that can be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, include CD, laser disc, optical disc, digital versatile disc (DVD), floppy disk and Blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above are also included within the scope of computer-readable media.

[0051] As used herein, including in the claims, "or" as used in a list of items (e.g., a list of items prefaced by a phrase such as "at least one of" or "one or more of") indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase "based on" shall not be construed as a reference to a closed set of conditions. For example, an exemplary step that is described as "based on condition A" may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase "based on" shall be construed in the same manner as the phrase "based at least in part on."

[0052] In the appended figures, similar components or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label by a dash and a second label that distinguishes among the similar components. If just the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label, or other subsequent reference label.

[0053] The description set forth herein, in connection with the appended drawings, describes example configurations and does not represent all the examples that may be implemented or that are within the scope of the claims. The term "exemplary" used herein means "serving as an example, instance, or illustration," and not "preferred" or "advantageous over other examples." The detailed description includes specific details for the purpose of providing an understanding of the described techniques. These techniques, however, may be practiced without these specific details. In some instances, well-known structures and devices are shown in block diagram form in order to avoid obscuring the concepts of the described examples.

[0054] The description herein is provided to enable a person skilled in the art to make or use the disclosure. Various modifications to the disclosure will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other variations without departing from the scope of the disclosure. Thus, the disclosure is not limited to the examples and designs described herein, but is to be accorded the broadest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A method, by a user equipment (UE), for wireless communication, comprising:

receiving a message from a visited network;

determining that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on the UE, outside a subscriber identity module (SIM);

determining a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list;

incrementing the counter associated with the visited network in response to the visited network being in the first forbidden network;

in response to the value of the counter being equal to a maximum counter value:

deleting the visited network from the first forbidden network list; and

adding the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

2. The method of claim 1, further comprising:

deleting all entries in the first forbidden network list in response to the SIM being removed from the UE or the UE being powered off.

3. The method of claim 1, further comprising:

camping on the visited network, wherein said camping comprises:

searching for a cell in the visited network;

selecting the cell; and

tuning a control channel of the UE to the cell.

4. The method of claim 1, further comprising:

determining that the UE does not maintain a UE-configured counter; and

adding the visited network to the second forbidden network list.

5. The method of claim 1, further comprising:

determining that the UE maintains a UE-configured counter;

determining that the UE-configured counter has a value of 0 or 1; and

adding the visited network to the second forbidden network list.

6. The method of claim 1, wherein:

the visited network is different from a home network.

7. The method of claim 1, wherein:

the message comprises a non-integrity protected reject message, and further includes a cause value indicating that the visited network is not allowed.

8. The method of claim 7, wherein:

the cause value comprises an evolved packet system (EPS) mobility management (EMM) cause #11.

9. The method of claim 1, wherein:

the message comprises an attach reject message, a tracking area update (TAU) reject message, or a service reject message.

10. An apparatus for wireless communication, comprising:

a processor;

memory in electronic communication with the processor; and

instructions stored in the memory and operable, when executed by the processor, to cause the apparatus to:

receive a message from a visited network;

determine that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on a user equipment (UE), outside a subscriber identity module (SIM);

determine a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list;

increment the counter associated with the visited network in response to the visited network being in the first forbidden network;

in response to the value of the counter being equal to a maximum counter value:

delete the visited network from the first forbidden network list; and

add the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

11. The apparatus of claim 10, wherein the instructions are further executable by the processor to cause the apparatus to:

delete all entries in the first forbidden network list in response to the SIM being removed from the UE or the UE being powered off.

12. The apparatus of claim 10, wherein the instructions are further executable by the processor to cause the apparatus to:

camp on the visited network, wherein said camping comprises:

searching for a cell in the visited network;

selecting the cell; and

tuning a control channel of the UE to the cell.

13. The apparatus of claim 10, wherein the instructions are further executable by the processor to cause the apparatus to:

determine that the UE does not maintain a UE-configured counter; and

add the visited network to the second forbidden network list.

14. The apparatus of claim 10, wherein the instructions are further executable by the processor to cause the apparatus to:

determine that the UE maintains a UE-configured counter;

determine that the UE-configured counter has a value of 0 or 1; and

add the visited network to the second forbidden network list.

15. The apparatus of claim 10, wherein:

the visited network is different from a home network.

16. The apparatus of claim 10, wherein:

the message comprises a non-integrity protected reject message, and further includes a cause value indicating that the visited network is not allowed.

17. The apparatus of claim 16, wherein:

the cause value comprises an evolved packet system (EPS) mobility management (EMM) cause #11.

18. The apparatus of claim 10, wherein:

the message comprises an attach reject message, a tracking area update (TAU) reject message, or a service reject message.

19. An apparatus for wireless communication, comprising:

means for receiving a message from a visited network;

means for determining that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on a user equipment (UE), outside a subscriber identity module (SIM);

means for determining a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list;

means for incrementing the counter associated with the visited network in response to the visited network being in the first forbidden network;

in response to the value of the counter being equal to a maximum counter value:

means for deleting the visited network from the first forbidden network list; and

means for adding the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

20. The apparatus of claim 19, further comprising:

means for deleting all entries in the first forbidden network list in response to the SIM being removed from the UE or the UE being powered off.

21. The apparatus of claim 19, further comprising:

means for camping on the visited network, wherein said camping comprises:

means for searching for a cell in the visited network;

means for selecting the cell; and

means for tuning a control channel of the UE to the cell.

22. The apparatus of claim 19, further comprising:

means for determining that the UE does not maintain a UE-configured counter; and

means for adding the visited network to the second forbidden network list.

23. The apparatus of claim 19, further comprising:

means for determining that the UE maintains a UE-configured counter;

means for determining that the UE-configured counter has a value of 0 or 1; and

means for adding the visited network to the second forbidden network list.

24. The apparatus of claim 19, wherein:

the visited network is different from a home network.

25. The apparatus of claim 19, wherein:

the message comprises a non-integrity protected reject message, and further includes a cause value indicating that the visited network is not allowed.

26. The apparatus of claim 25, wherein:

the cause value comprises an evolved packet system (EPS) mobility management (EMM) cause #11.

27. The apparatus of claim 19, wherein:

the message comprises an attach reject message, a tracking area update (TAU) reject message, or a service reject message.

28. A non-transitory computer readable medium storing code for wireless communication, the code comprising instructions executable by a processor to:

receive a message from a visited network;

determine that the visited network is in a first forbidden network list, wherein the first forbidden network list resides on a user equipment (UE), outside a subscriber identity module (SIM);

determine a value of a counter associated with the visited network in response to the visited network being in the first forbidden network list;

increment the counter associated with the visited network in response to the visited network being in the first forbidden network;

in response to the value of the counter being equal to a maximum counter value:

delete the visited network from the first forbidden network list; and

add the visited network to a second forbidden network list, wherein the second forbidden network list resides in the SIM.

29. The non-transitory computer-readable medium of claim 28, wherein the instructions are further executable by the processor to cause the apparatus to:

delete all entries in the first forbidden network list in response to the SIM being removed from the UE or the UE being powered off.

30. The non-transitory computer-readable medium of claim 28, wherein the instructions are further executable by the processor to cause the apparatus to:

camp on the visited network, wherein said camping comprises:

searching for a cell in the visited network;

selecting the cell; and

tuning a control channel of the UE to the cell.

31. The non-transitory computer-readable medium of claim 28, wherein the instructions are further executable by the processor to cause the apparatus to:

determine that the UE does not maintain a UE-configured counter; and

add the visited network to the second forbidden network list.

32. The non-transitory computer-readable medium of claim 28, wherein the instructions are further executable by the processor to cause the apparatus to:

determine that the UE maintains a UE-configured counter;

determine that the UE-configured counter has a value of 0 or 1; and

add the visited network to the second forbidden network list.

33. The non-transitory computer-readable medium of claim 28, wherein:

the visited network is different from a home network.

34. The non-transitory computer-readable medium of claim 28, wherein:

the message comprises a non-integrity protected reject message, and further includes a cause value indicating that the visited network is not allowed.

35. The non-transitory computer-readable medium of claim 34, wherein:

the cause value comprises an evolved packet system (EPS) mobility management (EMM) cause #11.

36. The non-transitory computer-readable medium of claim 28, wherein:

the message comprises an attach reject message, a tracking area update (TAU) reject message, or a service reject message.

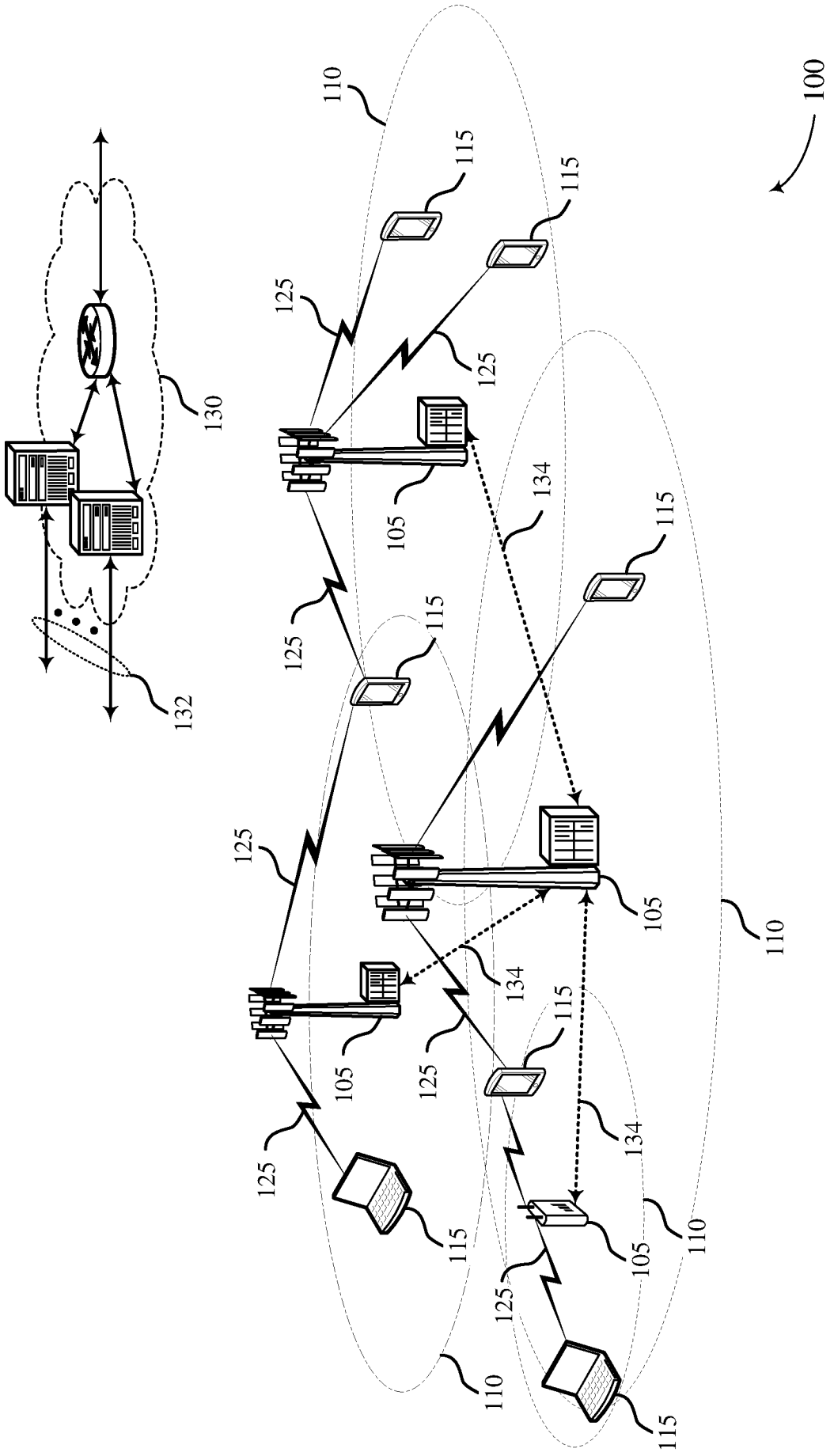

FIG. 1

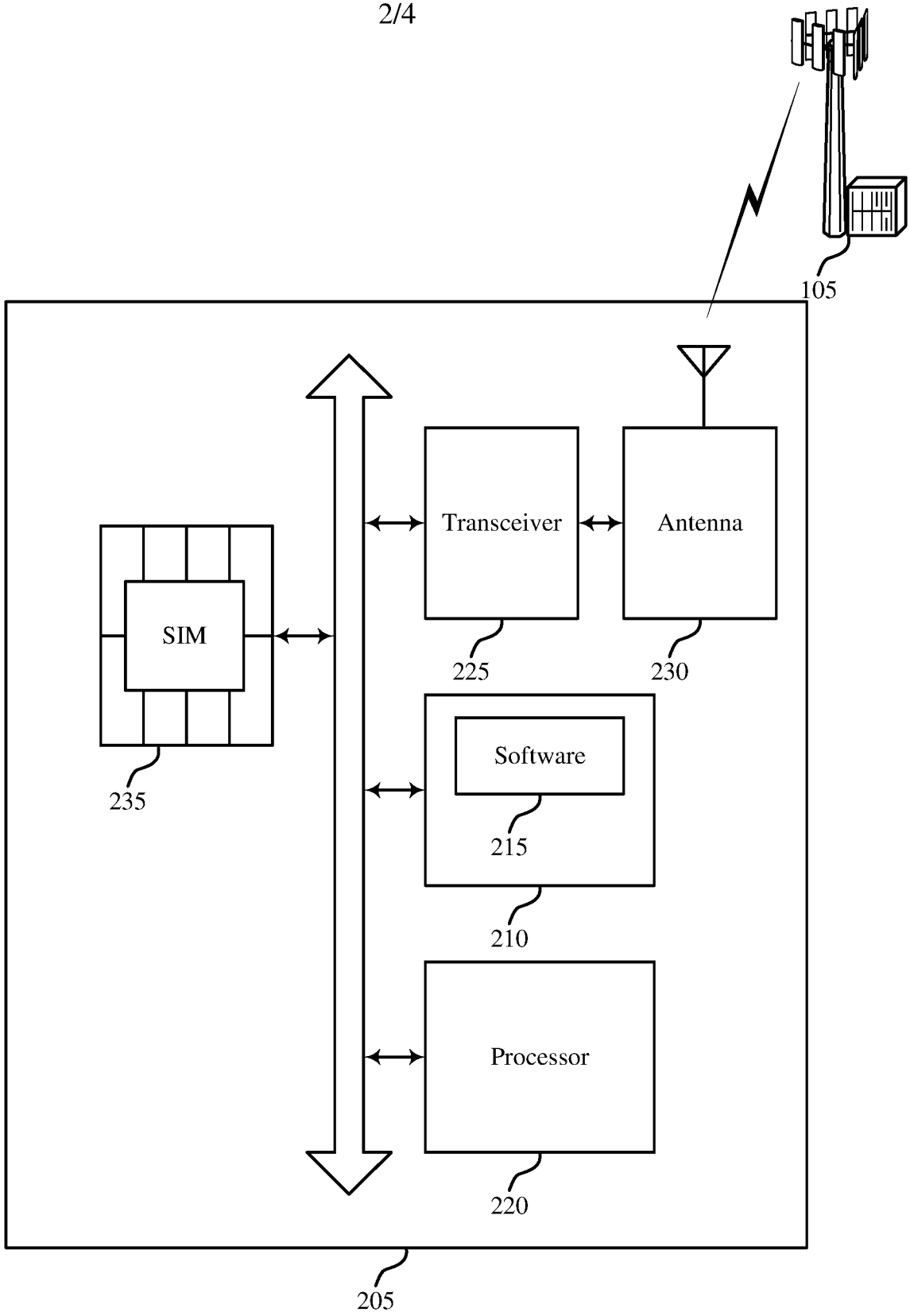
105
Transceiver
Antenna
SIM
225
230
Software
235
215
210
Processor
220
205
200

FIG. 2

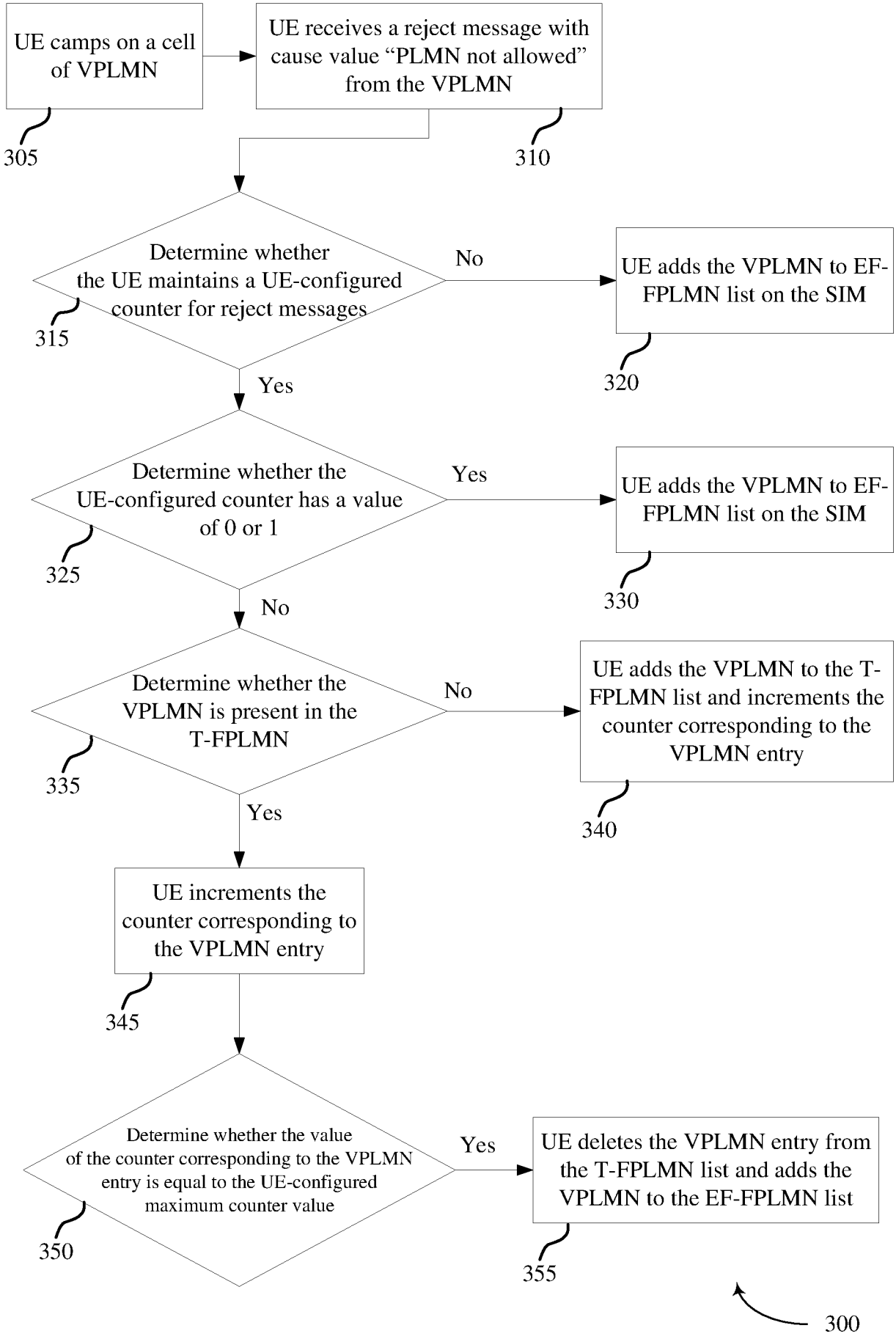
UE camps on a cell of VPLMN
305
UE receives a reject message with cause value "PLMN not allowed" from the VPLMN
310
Determine whether the UE maintains a UE-configured counter for reject messages
315
No
UE adds the VPLMN to EF-FPLMN list on the SIM
320
Yes
Determine whether the UE-configured counter has a value of 0 or 1
325
Yes
UE adds the VPLMN to EF-FPLMN list on the SIM
330
No
Determine whether the VPLMN is present in the T-FPLMN
335
No
UE adds the VPLMN to the T-FPLMN list and increments the counter corresponding to the VPLMN entry
340
Yes
UE increments the counter corresponding to the VPLMN entry
345
Determine whether the value of the counter corresponding to the VPLMN entry is equal to the UE-configured maximum counter value
350
Yes
UE deletes the VPLMN entry from the T-FPLMN list and adds the VPLMN to the EF-FPLMN list
355
300

FIG. 3

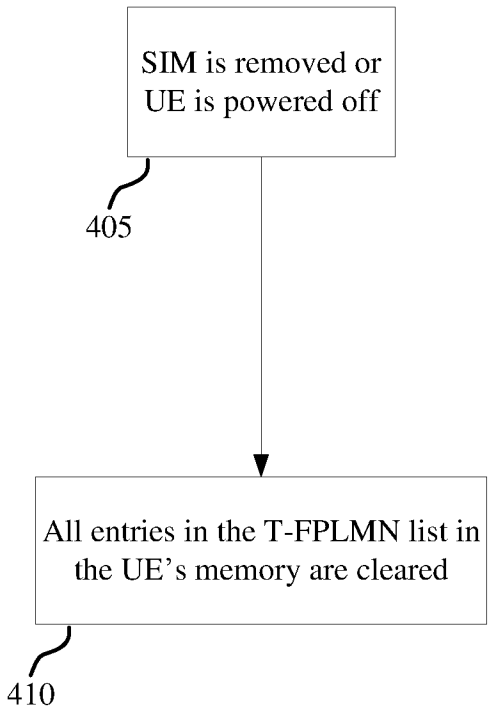
SIM is removed or UE is powered off
405
All entries in the T-FPLMN list in the UE's memory are cleared
410
400

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/041815

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W60/00
ADD. H04W12/06 H04W8/06

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)
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 practicable, search terms used)
EPO-Internal, 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	"3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 14)", 3GPP STANDARD ; TECHNICAL SPECIFICATION ; 3GPP TS 24.301, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. CT WG1, no. V14.4.0, 16 June 2017 (2017-06-16), pages 1-486, XP051298653, [retrieved on 2017-06-16] page 76 - page 78 page 112 - page 115 -/--	1-36

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 October 2018	24/10/2018

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	Tozlovanu, Ana-Delia

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	& "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (Release 14)", 3GPP STANDARD ; TECHNICAL SPECIFICATION ; 3GPP TS 23.122, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. CT WG1, no. V14.3.0, 15 June 2017 (2017-06-15), pages 1-53, XP051298505, [retrieved on 2017-06-15] page 12	1-36

A	MEDIATEK INC ET AL: "Correction of handling NAS reject messages without Integrity protection", 3GPP DRAFT; C1-161196-WAS0967, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. CT WG1, no. Jeju (Korea); 20160215 - 20160219 22 February 2016 (2016-02-22), XP051078125, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_96_Jeju/docs/ [retrieved on 2016-02-22] page 5	2,11,20, 29

X,P	QUALCOMM INCORPORATED: "Corrections to handling of EFFPLMN file in the SIM and of "forbidden PLMNs for GPRS service" list", 3GPP DRAFT; C1-173146_CORRECTIONS_FPLMN, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. CT WG1, no. Krakow (Poland); 20170821 - 20170825 20 August 2017 (2017-08-20), XP051313194, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/CT1/Docs/ [retrieved on 2017-08-20] the whole document	1-36

	-/--	

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/041815

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	WO 2017/135702 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 10 August 2017 (2017-08-10) paragraphs [0079], [0080], [0143] - paragraph [0152]	1-36
X,P	WO 2018/085427 A1 (INTEL IP CORP [US]) 11 May 2018 (2018-05-11) paragraph [0022] - paragraph [0028]	1-36

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/041815

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2017135702 A1	10-08-2017	KR 20180101439 A	12-09-2018
		WO 2017135702 A1	10-08-2017
WO 2018085427 A1	11-05-2018	NONE	