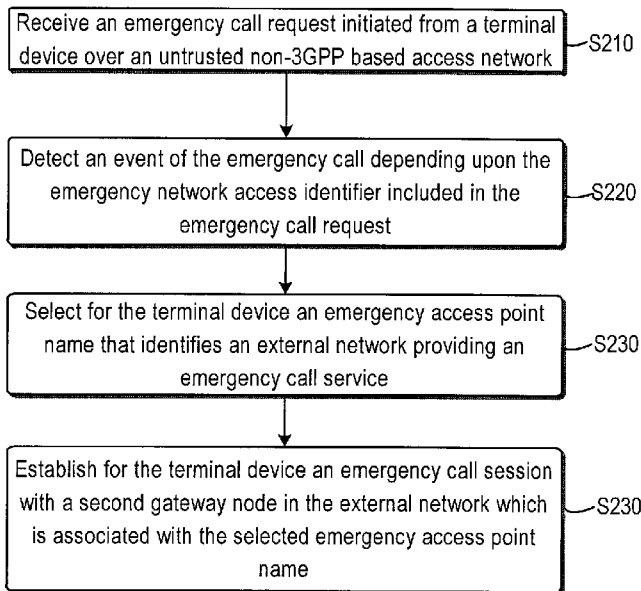




- (51) International Patent Classification: **H04L 12/24** (2006.01)
- (21) International Application Number: **PCT/CN2015/075612**
- (22) International Filing Date: **31 March 2015 (31.03.2015)**
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; Stockholm, SE-164 83 (SE).
- (72) Inventor; and
- (71) Applicant (for SC only): **WANG, Chunbo** [CN/CN]; 302#, No. 25, Lane 99, Jinhe Road, Pudong New Area, Shanghai 200127 (CN).
- (72) Inventors: **LI, Xiaoming**; Building Z, Floor 9, 1068 Tianshan Road West, Shanghai 200335 (CN). **WANG, Lu**; Room 26-1901, No. 388 Furongjiang Road, Shanghai 200051 (CN).
- (74) Agent: **KING & WOOD MALLESONS**; 20th Floor, East Tower, World Financial Centre, No.1 Dongsanhuan Zhonglu, Chaoyang District, Beijing 100020 (CN).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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,

[Continued on next page]

(54) Title: METHODS AND DEVICES FOR FACILITATING EMERGENCY CALLS OVER WIRELESS COMMUNICATION SYSTEMS



(57) Abstract: One embodiment of the present disclosure relates to a method implemented by a first gateway node for processing an emergency call from an untrusted non-3GPP access network. The method comprises: receiving an emergency call request initiated from a terminal device over an untrusted non-3GPP based access network; detecting an event of the emergency call depending upon the emergency network access identifier included in the request message; selecting for the terminal device an emergency access point name that identifies an external network providing an emergency call service; and establishing for the terminal device an emergency call session with a second gateway node interfacing with the external network which is identified by the selected emergency access point name. According to an aspect of the present disclosure, there are provided corresponding methods and devices.

Fig. 2

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))

METHODS AND DEVICES FOR FACILITATING EMERGENCY CALLS OVER
WIRELESS COMMUNICATION SYSTEMS

5 TECHNICAL FIELD

[0001] The present disclosure generally relates to wireless communication, particularly to methods and devices for facilitating emergency calls over an untrusted non-3GPP based access network.

10

BACKGROUND

[0002] This section is intended to provide a background to the various embodiments of the invention that are described in this disclosure. The description herein may include concepts
15 that could be pursued, but are not necessarily ones that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the description and/or claims of this disclosure and is not admitted to be prior art by the mere
20 inclusion in this section.

[0003] Universal Mobile Telecommunications System (UMTS) is the 3rd Generation (3G) mobile communication system standardized by 3rd Generation Partnership Project (3GPP). The 3GPP launched a study item known as "Long Term Evolution
25 (LTE)". The study will investigate means of achieving major leaps in performance in order to improve service provisioning, and to reduce user and operator costs. Out of that and because interworking with other radio access technologies should be possible, the need arose for a new evolved Packet Core Network.

30 [0004] In general, in such mobile communication systems, a

terminal device (also called User Equipment (UE)) has access to communication services (including basic services such as in particular providing IP connectivity) via a network comprising a Core Network (CN) accessed by an Access Network (AN) .

[0005] An example of 3GPP-based mobile communication system is Evolved Packet System (EPS), a description of which can be found in particular in 3GPP standards such as for example 3GPP TS 23.401 and 3GPP TS 23.402 series.

10 [0006] According to the 3GPP standards, EPS includes Evolved Packet Core (EPC) that can be accessed by various access networks, including 3GPP based access networks and non-3GPP based access networks. Examples of 3GPP based access networks include UMTS Terrestrial Radio Access Network (UTRAN),
15 evolved UTRAN (E-UTRAN), GSM EDGE Radio Access Network (GERAN), etc. Examples of non-3GPP based access networks include CDMA2000, Wireless Fidelity (WiFi) Access Network (specified by IEEE, in particular in 802.11 specifications), Worldwide Interoperability for Microwave Access (WiMAX) Access Network
20 (specified by IEEE, in particular in 802.16 specifications).

[0007] Two different types of non-3GPP based access networks are involved in the 3GPP standards, i.e. untrusted non-3GPP based access networks and trusted non-3GPP based access network, and normally whether a non-3GPP based access network
25 is trusted or not is left to specific 3GPP operators. During initial attach or handover attach a UE needs to discover the trust relationship (whether it is a trusted or untrusted non-3GPP access network) of the non-3GPP access network in order to know which non-3GPP IP access procedure to initiate.

30 [0008] Some calling solutions enable mobile subscribers to make voice calls (initially) from an untrusted non-3GPP based access environment, such as from residential WiFi. The calls

are managed by IP Multimedia Subsystem (IMS) Core, and the solution is sometimes referred to as Voice over Wi-Fi. Those solutions also enable the user to maintain session continuity or IP address persistency when they handover between 3GPP based access (such as for example LTE) to untrusted non-3GPP based access (such as for example WiFi).

[0009] The procedures of non-3GPP Packet Data Network (PDN) connection establishment over untrusted non-3GPP access and the handover between 3GPP based accesses and untrusted non-3GPP accesses are defined in 3GPP TS 23.402 and TS 23.401 series.

[0010] However, as to the emergency call service, the current 3GPP standards do not support emergency calls over an untrusted non-3GPP accesses (e.g., WiFi) and emergency session continuity for the handover between a 3GPP based access network and an untrusted non-3GPP based access network. Specifically, in the current 3GPP standard: IMS Emergency Session setup over untrusted non-3GPP based access (e.g., WiFi) is not supported; IMS Emergency Session Support for non-3GPP accesses connected to EPC is limited to support of handover of emergency sessions from E-UTRAN access to High Rate Packet Data (HRPD) access (which is normally configured as a trusted access by operators); handover of IMS Emergency Sessions from non-3GPP access to 3GPP based access (e.g., E-UTRAN) is not supported.

SUMMARY

[0011] One or more method and apparatus embodiments according to the present disclosure aim to provide one or more solutions for facilitating emergency calls over an untrusted non-3GPP based access network.

[0012] According to the first aspect of the present disclosure, there is provided a method implemented by a first gateway node for processing an emergency call. The method comprises receiving an emergency call request initiated from a terminal device over an untrusted non-3GPP based access network. The emergency call request includes an emergency network access identifier constructed by the terminal device. The method further comprises detecting an event of the emergency call depending upon the emergency network access identifier; selecting for the terminal device an emergency access point name that identifies an external network providing an emergency call service; and establishing for the terminal device an emergency call session with a second gateway node interfacing with the external network which is identified with the selected emergency access point name.

[0013] According to one or more embodiments of the first aspect of the present disclosure, the method further comprises informing the terminal device of the selected emergency access point name. In this way, the terminal device may store the emergency access point name so as to facilitate potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

[0014] According to the second aspect of the present disclosure, there is provided a method implemented by a terminal device for initiating an emergency call over an untrusted non-3GPP based access network. The method comprises constructing an emergency network access identifier; sending to a first gateway node an emergency call request including the constructed emergency network access identifier; and establishing, via the first gateway node, an emergency call session with a second gateway node interfacing with an external network providing an emergency call service.

[0015] According to one or more embodiments of the second aspect of the present disclosure, the method further comprises receiving from the first gateway node an emergency access point name. In this way, the terminal device may then store
5 the emergency access point name that identifies the external network providing the emergency call service, so as to facilitate potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

[0016] According to the third aspect of the present disclosure,
10 there is provided a method implemented by a network node of a 3GPP based access network for facilitating emergency call handover from an untrusted non-3GPP based access network to the 3GPP based access network. The method comprises: receiving a request message sent from a terminal device that are
15 currently performing an emergency call over the untrusted non-3GPP based access network. The request message includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call. The method further comprises: detecting an event of the
20 emergency call handover based on the handover indication and the emergency access point name; establishing an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name; and switching the emergency call of the
25 terminal device from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network.

[0017] According to the fourth aspect of the present disclosure, there is provided a method implemented by a network node of a 3GPP based access network for processing an emergency call.
30 The method comprises: receiving an emergency call request initiated from a terminal device over a 3GPP based access network; selecting for the terminal device an emergency access point name that identifies an external network providing an

emergency call service; establishing an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name.

5 [0018] According to one or more embodiments of the fourth aspect of the present disclosure, the method further comprises informing the terminal device of the selected emergency access point name. In this way, the terminal device may store the emergency access point name that identifies the external
10 network providing the emergency call service, so as to facilitate potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

[0019] According to the fifth aspect of the present disclosure, there provides a method implemented by a first gateway node
15 for facilitating emergency call handover from a 3GPP based access network to an untrusted 3GPP based access network. The method comprises receiving a request message sent from a terminal device that is currently performing an emergency call over the 3GPP based access network. The request message
20 includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call. The method further comprises: detecting an event of the emergency call handover based on the handover indication and the emergency network access identifier; and
25 establishing an emergency call session with a second gateway node interfacing with the external network that is identified by the emergency access point name included in the request message.

[0020] According to the sixth aspect of the present disclosure,
30 there provides a first gateway node operably for processing an emergency call. The first gateway node comprises: a receiving unit configured to receive an emergency call request

initiated from a terminal device over an untrusted non-3GPP based access network. The emergency call request includes an emergency network access identifier constructed by the terminal device. The first gateway node further comprises a
5 detecting unit configured to detect an event of the emergency call depending upon the emergency network access identifier; a selecting unit configured to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service; and a session
10 establishing unit configured to establish for the terminal device an emergency call session with a second gateway node interfacing with the external network which is identified by the selected emergency access point name.

[0021] According to the seventh aspect of the present
15 disclosure, there provides a terminal device operably for initiating an emergency call over an untrusted non-3GPP based access network. The terminal device comprises: an identifier constructing unit configured to construct an emergency network access identifier; a transmitting unit configured to
20 send to a first gateway node an emergency call request including the constructed emergency network access identifier; and a session establishing unit configured to establish, via the first gateway node, an emergency call session with a second gateway node interfacing with an external network providing
25 an emergency call service.

[0022] According to the eighth aspect of the present disclosure, there provides a network node of a 3GPP based access network operably for facilitating emergency call handover from an untrusted non-3GPP based access network to the 3GPP based
30 access network. The network node comprises: a receiving unit configured to receive a request message sent from a terminal device that is currently performing an emergency call over the untrusted non-3GPP based access network. The request

message includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call. The network node comprises: a detecting unit configured to detect an event of the emergency call handover based on the handover indication and the emergency access point name; a session establishing unit configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name; and a switching unit configured to switch the emergency call of the terminal device from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network.

[0023] According to the ninth aspect of the present disclosure, there provides a network node of a 3GPP based access network operably for processing an emergency call. The network node comprises: a receiving unit configured to receive an emergency call request initiated from a terminal device over a 3GPP based access network; a selecting unit configured to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service; and a session establishing unit configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name.

[0024] According to the tenth aspect of the present disclosure, there provides a first gateway node operably for facilitating emergency call handover from a 3GPP based access network to an untrusted non-3GPP based access network. The first gateway node comprises: a receiving unit configured to receive a request message sent from a terminal device that is currently performing an emergency call over the 3GPP based access network. The request message includes a handover indication

and an emergency access point name which identifies an external network used to establish the emergency call. The first gateway node further comprises: a detecting unit configured to detect an event of the emergency call handover
5 based on the handover indication and the emergency network access identifier; and a session establishing unit configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the emergency access point name included in the request
10 message.

[0025] According to the eleventh aspect of the present disclosure, there provides a first gateway node operably for processing an emergency call. The first gateway node comprises processing means adapted to cause to receive an emergency call
15 request initiated from a terminal device over an untrusted non-3GPP based access network, wherein the emergency call request includes an emergency network access identifier constructed by the terminal device; cause to detect an event of the emergency call depending upon the emergency network access identifier; cause to select for the terminal device
20 an emergency access point name that identifies an external network providing an emergency call service; cause to establish for the terminal device an emergency call session with a second gateway node interfacing with the external network which is identified by the selected emergency access
25 point name.

[0026] According to the twelfth aspect of the present disclosure, there provides a terminal device operably for initiating an emergency call over an untrusted non-3GPP based
30 access network. The terminal device comprises processing means adapted to: cause to construct an emergency network access identifier; cause to send to a first gateway node an emergency call request including the constructed emergency

network access identifier; cause to establish, via the first gateway node, an emergency call session with a second gateway node interfacing with an external network providing an emergency call service.

5 [0027] According to the thirteenth aspect of the present disclosure, there provides a network node of a 3GPP based access network for facilitating emergency call handover from an untrusted non-3GPP based access network to the 3GPP based access network. The network node comprises processing means
10 adapted to: cause to receive a request message sent from a terminal device that is currently performing an emergency call over the untrusted non-3GPP based access network, wherein the request message includes a handover indication and an emergency access point name which identifies an external
15 network used to establish the emergency call; cause to detect an event of the emergency call handover based on the handover indication and the emergency access point name; cause to establish an emergency call session with a second gateway node interfacing with the external network that is identified by
20 the selected emergency access point name; cause to switch the emergency call of the terminal device from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network.

[0028] According to the fourteenth aspect of the present
25 disclosure, there provides a network node of a 3GPP based access network operably for processing an emergency call. The network node comprises processing means adapted to: cause to receive an emergency call request initiated from a terminal device over a 3GPP based access network; cause to select for
30 the terminal device an emergency access point name that identifies an external network providing an emergency call service; cause to establish an emergency call session with a second gateway node interfacing with the external network

that is identified by the selected emergency access point name.

[0029] According to the fifteenth aspect of the present disclosure, there provides a first gateway node operably for
5 facilitating emergency call handover from a 3GPP based access network to an untrusted non-3GPP based access network. The first gateway node comprises processing means adapted to:
cause to receive a request message sent from a terminal device that is currently performing an emergency call over the 3GPP
10 based access network, wherein the request message includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call;
cause to detect an event of the emergency call handover based on the handover indication and the emergency network
15 access identifier; cause to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the emergency access point name included in the request message.

[0030] According to one or more embodiments of the present
20 disclosure, a user is allowed to make an emergency call even over an untrusted non-3GPP based access network, for example, a WiFi residential environment. In a meanwhile, the continuity of the emergency call session can be maintained by appropriately handing over between the untrusted non-3GPP
25 based access network and a 3GPP based access network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] Inventive features regarded as the characteristics of the present invention are set forth in the appended claims.
30 However, the present invention, its implementation mode, other objectives, features and advantages will be better understood through reading the following detailed description

on the exemplary embodiments with reference to the accompanying drawings, where in the drawings:

[0032] Fig. 1 is a diagram schematically illustrating a network architecture, on which various embodiments of the present disclosure can be practiced;

[0033] Fig. 2 is a diagram schematically illustrating an exemplary flow chart of a method implemented by a first gateway node according to one or more embodiments of the present disclosure;

[0034] Fig. 3 is a diagram schematically illustrating an exemplary flow chart of a method implemented by a terminal device according to one or more embodiments of the present disclosure;

[0035] Fig. 4 is an example signaling diagram illustrating an embodiment where an emergency call is initiated over an untrusted non-3GPP based access network;

[0036] Fig. 5 is a diagram schematically illustrating an exemplary flow chart of a method implemented by a network node of a 3GPP based access network according to one or more embodiments of the present disclosure;

[0037] Fig. 6 is an example signaling diagram illustrating an embodiment where a handover of an emergency call is performed from an untrusted non-3GPP based access network to a 3GPP based access network;

[0038] Fig. 7 is a diagram schematically illustrating an exemplary flow chart of a method implemented by a network node of a 3GPP based access network according to one or more embodiments of the present disclosure;

[0039] Fig. 8 is an example signaling diagram illustrating an embodiment where an emergency call is initiated over a 3GPP

based access network;

[0040] Fig. 9 is a diagram schematically illustrating an exemplary flow chart of a method implemented by a first gateway node according to one or more embodiments of the present disclosure;

[0041] Fig. 10 is an example signaling diagram illustrating an embodiment where a handover of an emergency call is performed from a 3GPP based access network to an untrusted non-3GPP based access network;

[0042] Fig. 11 is a schematic block diagram depicting a first gateway node operably for processing an emergency call according to an embodiment of the present disclosure;

[0043] Fig. 12 is a schematic block diagram depicting a terminal device operably for processing an emergency call according to an embodiment of the present disclosure;

[0044] Fig. 13 is a schematic block diagram depicting a 3GPP network node operably for facilitating emergency call handover from an untrusted non-3GPP based access network to a 3GPP based access network according to an embodiment of the present disclosure;

[0045] Fig. 14 is a schematic block diagram depicting a 3GPP network node operably for processing an emergency call according to an embodiment of the present disclosure;

[0046] Fig. 15 is a schematic block diagram depicting a first gateway node operably for facilitating emergency call handover from a 3GPP based access network to an untrusted non-3GPP based access network according to an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0047] Hereinafter, embodiments of the present disclosure will be described with reference to the accompanying drawings. In the following description, many specific details are illustrated so as to understand the present disclosure more comprehensively. However, it is apparent to the skilled in the art that implementation of the present invention may not have these details. Additionally, it should be understood that the present invention is not limited to the particular embodiments as introduced here. On the contrary, any combination of the following features and elements may be considered to implement and practice the present invention, regardless of whether they involve different embodiments. For example, while it is described below in the context of 5G cellular communication system for illustrative purposes, those skilled in the art will recognize that one or more embodiments of the present disclosure can also be applied to various other types of cellular communication systems. Thus, the following aspects, features, embodiments and advantages are only for illustrative purposes, and should not be understood as elements or limitations of the appended claims, unless otherwise explicitly specified in the claims.

[0048] Fig. 1 is a diagram schematically illustrating a network architecture, on which various embodiments of the present disclosure can be practiced.

[0049] As shown in Fig. 1, the system 100 is for example an EPS including an untrusted non-3GPP based network 110 (e.g., a WiFi access network) and a 3GPP based access network 130 (a LTE access network).

[0050] UE 120, which is attached to an access point (not shown) of the untrusted non-3GPP access network 110, has an access to external networks 170 (which provide IP services) via a first gateway node 140 (e.g., an evolved Packet Data Gateway

(ePDG)) and a second gateway node 150 (e.g., a Packet Data Network Gateway (PDN Gateway, PGW)).

[0051] The first gateway node 140 interfaces with the untrusted nono-3GPP based access network 110 enabling routing packet
5 from/to the second gateway node 150 to/from UE 120 in the untrusted non-3GPP based access network 110. The first gateway node 140 is also capable of relaying Authentication, Authorization and Accounting (AAA) messages between the UE
10 120 and a 3GPP AAA server 180/ Home Subscriber Server (HSS) 190 to perform 3GPP AAA procedures for the UE 120 in the untrusted non-3GPP based access network 110. For implementation of the above functionalities, different interfaces may be used by the first gateway node 140, as defined particular in 3GPP TS 23.402 v13.1.0:

- 15 • S2b It provides the user plane with related control and mobility support between the ePDG and the PGW;
- SWn This is the reference point between the untrusted Non-3GPP IP Access and the ePDG. Traffic on this interface for a UE-initiated tunnel has to be forced towards the ePDG;
- 20 • SWm This reference point is located between 3GPP AAA Server/Proxy and the ePDG and is used for AAA signalling (transport of mobility parameters, tunnel authentication and authorization data).

[0052] The second gateway node 150 (e.g., a PGW of the EPS)
25 provides connectivity for UEs (in both the 3GPP based access network 130 and the untrusted non-3GPP based access network 110) to the external packet data networks 170 by being the point of exit and entry of traffic for the UE. The second gateway node 150 is to act as the anchor for mobility between
30 3GPP and non-3GPP technologies. For implementation of the above functionalities, different interfaces may be used by

the second gateway node 150, as defined particular in 3GPP TS 23.402 v13.1.0:

- SGi It is the reference point between the PGW and the packet data network (shown as "External networks 170" in Fig. 1). Packet data network may be an operator external public or private packet data network or an intra-operator packet data network, e.g. for provision of IMS services.
- S5 It provides user plane tunnelling and tunnel management between the Serving GW (shown as "Serving Gateway 160" in Fig. 1) and PGW. It is used for Serving GW relocation due to UE mobility and in case the Serving GW needs to connect to a non-located PDN GW for the required PDN connectivity.
- S6b It is the reference point between PDN Gateway and 3GPP AAA server/proxy (shown as "3GPP AAA server 180" in Fig. 1) for mobility related authentication if needed. This reference point may also be used to retrieve and request storage of mobility parameters. This reference point may also be used to retrieve static QoS profile for a UE for non-3GPP access in case dynamic PCC is not supported.

[0053] The Serving Gateway (SGW) 160 routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNB handovers and as the anchor for mobility between LTE and other 3GPP technologies.

[0054] Although not shown in Fig. 1, it should be appreciated by the person skilled in the art that the 3GPP based access network 130 comprises different functional network elements, for example, Node Bs (eNB or eNode B), Mobility Management Entities (MME).

[0055] The eNode B provides the E-UTRA user plane and control plane protocol terminations towards the UE in the 3GPP based

access network 130.

[0056] The MME is the key control-node for the 3GPP based access network 130. It is responsible for idle mode UE tracking and paging procedure including retransmissions. It is involved
5 in the bearer activation/deactivation process and is also responsible for choosing the SGW for UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation. It is responsible for authenticating the user by interacting with the HSS 190. It checks the authorization
10 of the UE to camp on the service provider's Public Land Mobile Network (PLMN) and enforces UE roaming restrictions.

[0057] A more detailed description of the network architecture can be found in 3GPP TS 23.402 v13.1.0.

[0058] In the present disclosure, terminal devices also known
15 as mobile terminals, wireless terminals and/or User Equipment (UE) are enabled to communicate wirelessly with a network node in a wireless communication system, sometimes also referred to as a cellular radio system. For instance, a terminal device may include but is not limited to: mobile phone, smart phone,
20 sensor device, meter, vehicle, household appliance, medical appliance, media player, camera, or any type of consumer electronic, for instance, but not limited to, television, radio, lighting arrangement, tablet computer, laptop, or PC. The communication device may be a portable, pocket-storable,
25 hand-held, computer-comprised, or vehicle-mounted mobile device, enabled to communicate voice and/or data, via a wireless connection.

[0059] With reference to Figs. 2-17, various embodiments of the present disclosure are described in details.

30 [0060] Fig. 2 is a diagram schematically illustrating an exemplary flow chart of a method 200 implemented by a first gateway node for processing an emergency call according to

one or more embodiments of the present disclosure.

[0061] As shown in Fig. 2, the method 200 begins at step S210. In step S210, the first gateway node (e.g., the first gateway node 140) receives an emergency call request initiated from a terminal device (e.g., the UE 120) over an untrusted non-3GPP based access network (e.g., the untrusted non-3GPP based access network 110). In order to indicate the emergency call, the emergency call request includes an emergency network access identifier constructed by the terminal device. Depending upon the emergency network access identifier (NAI) in the call request, the first gateway node detects, in step S220, an event of the emergency call. In step S230, an emergency access point name (APN) is selected by the first gateway node, which identifies a particular external packet data network (one of the external networks 170) that provides the emergency call service requested by the terminal device. The first gateway node then establishes, in step S240, for the terminal device an emergency call session with a second gateway node (e.g., the second gateway node 150) interfacing with the external network which is identified by the selected emergency access point name.

[0062] In one or more embodiments of the present disclosure, the method 200 may further comprises the following step (not shown in Fig.1): the first gateway node may inform the terminal device of the selected emergency access point name. The terminal device may locally store the selected access point name associated with the external network providing the emergency call service, thereby facilitating potential handover procedure from the untrusted non-3GPP based access network to a 3GPP based access network, for example, due to its mobility.

[0063] According to one or more embodiments of the present

disclosure, during the establishment of an emergency call session for the terminal device, the first gateway node may send to the second gateway node a create session request including the selected emergency access point name, thereby
5 enabling the second network node to identify the emergency call session. Since the terminal device is communicatively interfacing with the untrusted non-3GPP based environment, the first gateway node may also need to perform authentication procedure for the terminal device based on an equipment
10 identity of the terminal device.

[0064] Fig. 3 is a diagram schematically illustrating an exemplary flow chart of a method 300 implemented by a terminal device for processing an emergency call according to one or more embodiments of the present disclosure.

15 [0065] As shown in Fig. 3, when initiating an emergency call over an untrusted non-3GPP based access network (e.g., the untrusted non-3GPP based access network 110), a terminal device (e.g., the UE 120) constructs, in step S310, an emergency network access identifier for example in response
20 to a user dialing an emergency number. The emergency network access identifier may include a predefined indicator of the emergency call, for example, a character string "SOS". In step S320, the terminal device sends to a first gateway node (e.g., the first gateway node 140) an emergency call request
25 including the constructed emergency network access identifier. An emergency call session with a second gateway node (e.g., the second gateway node 150) is established via the first gateway node in step S330. The second gateway node interfaces with an external network that provides the requested emergency
30 call service.

[0066] According to one or more embodiments of the present disclosure, the terminal device may receive from the first

gateway node an emergency access point name and store it locally, thereby facilitating potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

5 [0067] Fig. 4 is an example signaling diagram illustrating an embodiment where an emergency call is initiated over an untrusted non-3GPP based access network.

[0068] As shown in Fig. 4, the UE communicates wirelessly with an access point (AP) of the untrusted non-3GPP based access network (for example, a WiFi network) and accesses to the
10 external networks (e.g., public Internet, Intranet, operator's IMS networks). In the example of Fig. 4, the first gateway node may be an ePDG and the second gateway node may be a PGW.

15 [0069] In step S401, the UE and the ePDG may exchange the first pair of IKE_SA_INIT messages, in which the ePDG and the UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie-Hellman exchange, as specified in 3GPP TS 33.402 V12.5.0.

20 [0070] In step S402, the UE constructs an emergency network access identifier. The emergency network access identifier includes a predetermined indicator of the emergency call and may be compliant to the definition of 3GPP TS 23.003 series.

[0071] In step S403, the UE may send a request message IKE
25 AUTH_REQ for the emergency call to the ePDG. The emergency network access identifier constructed by the UE is included in the IKE AUTH_REQ message. More detailed description of IKE AUTH_REQ is provided in Chapter 6.5 of 3GPP TS 33.402 series.

[0072] In some implementations, the UE may also include an
30 emergency access point name in the IKE AUTH_REQ, if it has been already configured by the network.

[0073] In step S404, the ePDG detects depending upon the emergency network access identifier that the current request is directed to an emergency call. In some implementations, the ePDG may not treat the request as an emergency call request, if the ePDG only receives an emergency access point name but without the emergency network access identifier from the UE.

[0074] In step S405, the ePDG may select an appropriate emergency access point name for the UE, for example, by load balancing mechanism. The emergency access point name identifies an external network which will provide the emergency call service for the UE.

[0075] In step S406, the ePDG may perform the local Extensible Authentication Protocol (EAP) authentication or the remote EAP authentication with an AAA server (not shown) based on UE Identity (e.g., International Mobile Equipment Identity (IMEI) or International Mobile Subscriber Identification Number (IMSI)) and configuration information. If the UE identity is based on IMEI, then only local EAP authentication needs to be performed.

[0076] In step S407, the UE may send the AUTH parameter to the ePDG.

[0077] In steps S408 and S409, the ePDG establishes for the UE an emergency call session with the PGW that interfaces with the external network identified by the selected emergency access point name. Specifically, the ePDG may send (S408) a Create Session Request including the UE's IMSI or IMEI, the emergency access point name to the PGW. Upon receipt of the Create Session Request, the PGW may detect the emergency call request based on the emergency APN included in the Request, then handle accordingly and return (S409) a Create Session Response.

[0078] In step S410, the ePDG may send the selected emergency

access point name and other parameters received from the PGW (e.g., UE IP address) to the UE.

[0079] In step S411, the UE may locally store the selected emergency access point name, so as to facilitate potential
5 handover from the untrusted non-3GPP based access network to a 3GPP based access network.

[0080] Fig. 5 is a diagram schematically illustrating an exemplary flow chart of a method 500 implemented by a network node of a 3GPP based access network according to one or more
10 embodiments of the present disclosure.

[0081] As shown in Fig. 5, the method 500 begins at step S510, where the network node (e.g., MME) of the 3GPP based access network (e.g., the 3GPP based access network 130) receives a request message (e.g., a packet data network connectivity
15 request message or an attach request message) sent from a terminal device (e.g., the UE 120) that is currently performing an emergency call over the untrusted non-3GPP based access network (e.g., the untrusted non-3GPP based access network 110). The request message includes a handover
20 indication and an emergency access point name which identifies an external network (e.g., one of the external networks 170) used to establish the emergency call. The network node detects in step S520 an event of the emergency call handover based on the handover indication and the emergency access
25 point name and then establishes in step S530 an emergency call session with a second gateway node (e.g., the second gateway node 150) interfacing with the external network that is identified by the selected emergency access point name. After the establishment of the emergency session with the second
30 gateway node, the network node switches in step S540 the emergency call of the terminal device from the bearer of the untrusted non-3GPP based access network to the bearer of the

3GPP based access network.

[0082] According to one or more embodiments, during the establishment of the emergency call session with the second gateway node, the network node may send to the second gateway node a create session request including the emergency access point name, thereby enabling the second gateway node to identify the emergency call session.

[0083] Fig. 6 is an example signaling diagram illustrating an embodiment where a handover of an emergency call is performed from an untrusted non-3GPP based access network to a 3GPP based access network.

[0084] As shown in Fig. 6, the UE communicates wirelessly with an eNodeB of the 3GPP based access network and accesses to the external networks (e.g., public Internet, Intranet, operator's IMS networks). In the example of Fig. 6, the network node of the 3GPP based access network mainly handling the emergency call handover procedure may be a MME; the first gateway node may be an ePDG and the second gateway node may be a PGW.

[0085] In step S601, the UE may discover the 3GPP based access (e.g., E-UTRAN access) and determine to transfer its emergency session from the currently used the untrusted non-3GPP based access network (e.g., WiFi access) to the 3GPP based access network. The UE sends an Attach Request message or PDN Connectivity Request message to the MME with Request Type indicating "Handover". The UE also includes the related emergency access point name in the request message, which was received from the ePDG in step S410 in Fig.4. More detailed description of the message routed from the UE to the MME may be provided for example in 3GPP TS 23.401 series.

[0086] In one or more embodiments of the present disclosure, if the UE is connected to both the 3GPP based access network

and the untrusted non-3GPP based access network before the emergency handover is triggered, the UE may set the "Request Type" as "Handover" and include the relevant emergency access point name in a PDN Connectivity Request message. If the UE
5 is only connected to the untrusted non-3GPP based access network before the emergency call handover is triggered, the UE may set the "Attach Type" as "Emergency", the "Request Type" to "Handover" and include the relevant emergency access point name in an Attach Request message.

10 [0087] In step S602, the MME detects that this is an emergency call handover from the untrusted non-3GPP based access network depending upon the "emergency access point name" and the request type "Handover", and then selects the PGW associated with the emergency access point name included in the request
15 message.

[0088] According to one or more implementations of the present disclosure, to ensure that the same right PGW can be selected in both 3GPP and untrusted non-3GPP based access networks, the MME configuration may preferably be consistent with the
20 ePDG side, which means that one PGW is associated with one emergency access point name. Multiple emergency access point names may be configured to achieve load balancing among multiple PGWs and the PGW high availability.

[0089] In steps S603 and S604, the MME establishes an emergency
25 call session with the PGW that is connected with the external network identified by the selected emergency access point name. Specifically, in step S603, the MME sends a Create Session Request message including the PGW address, the handover indication and the emergency access point name to a
30 corresponding Serving gateway (SGW), which then forwards the Create Session Request towards the selected PGW. The PGW may detect the emergency call handover from the untrusted non-3GPP

based access network depending upon the "Handover Indication" and the "emergency access point name" included in the Create Session Request message, then return (S604) a Create Session Response with the IP address of the UE. The SGW may forward
5 the Create Session Response message to the MME. This message may also serve as an indication to the MME that the S5 bearer setup has been successful. The messaging among the MME, SGW and PGW for creating a session may be compliant with 3GPP TS 23.401 series.

10 [0090] From step S605 to step S608, the MME switches the emergency call of the UE from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network. Specifically, in step S605, Radio and Access bearers are established in the 3GPP based access network, as specified
15 in 3GPP TS 23.401 series. The MME may send in step S606 a Modify Bearer Request message to the SGW, which includes eNodeB address, eNodeB TEID, and the Handover Indication. The SGW forwards the Modify Bearer Request message to the PGW. The PGW may switch the data path to the SGW, and then in step S607,
20 return a Modify Bearer Response. The SGW may forward the Modify Bearer Response message to the MME. In step S608, resource allocation deactivation procedure in the untrusted non-3GPP based access network may be initiated to delete the untrusted non-3GPP bearer.

25 [0091] Fig. 7 is a diagram schematically illustrating an exemplary flow chart of a method 700 implemented by a network node of a 3GPP based access network according to one or more embodiments of the present disclosure.

[0092] As shown in Fig. 7, the method 700 begins at step S710,
30 where the network node (e.g., a MME) receives an emergency call request initiated from a terminal device (e.g., UE in the 3GPP based access network 130) over a 3GPP based access

network (e.g., the 3GPP based access network 130). In step S720, the network node selects for the terminal device an emergency access point name that identifies an external network (e.g., one of the external networks 170) providing an emergency call service. The network node establishes, in step S730, an emergency call session with a second gateway node (e.g., the second gateway 150) interfacing with the external network that is identified by the selected emergency access point name.

[0093] According to one or more embodiments of the present disclosure, the network node may inform the terminal device of the selected emergency access point name, thereby facilitating potential handover from the 3GPP based access network to an untrusted non-3GPP based access network (e.g., the untrusted non-3GPP based access network 110).

[0094] Fig. 8 is an example signaling diagram illustrating an embodiment where an emergency call is initiated over a 3GPP based access network.

[0095] As shown in Fig. 8, the UE may communicate wirelessly with an eNodeB of the 3GPP based access network and access to the external networks (e.g., public Internet, Intranet, operator's IMS networks). In the example of Fig. 8, the network node of the 3GPP based access network operably processing an emergency call may be a MME; the first gateway node may be an ePDG and the second gateway node may be a PGW.

[0096] In step S801, the UE initiates the Attach procedure for an emergency call by the transmission, to the eNodeB, of an Attach Request message with the "Attach Type" as "Emergency". In some embodiments, an emergency access point name may also be included in a PDN connectivity Request message and sent to the MME.

[0097] In step S802, The MME may check if the user is allowed

to perform handover to non-3GPP accesses, then for such an emergency call, an emergency access point name is selected which is associated with a PGW.

[0098] In steps S803 and S804, the MME establishes an emergency call session with the PGW connected with the external network that is identified by the selected emergency access point name. Specifically, the MME sends (S803) to a corresponding SGW a Create Session Request message including the emergency access point name, IMSI or IMEI of the UE, and the PGW address. The SGW may forward the Create Session Request message to the PGW. The PGW may detect the emergency call request depending upon the emergency access point name, handle accordingly, and return (S804) a Create Session Response message with the IP address of the UE. This message may also serve as an indication to the MME that the S5 bearer setup has been successful. The messaging among the MME, SGW and PGW for creating a session may be compliant with the description of 3GPP TS 23.401 series.

[0099] In step S805, radio and access bearers are established in the 3GPP based access network, for example, as specified in TS 23.401. According to one or more embodiments of the present disclosure, the selected emergency access point name may be included in Activate Default EPS bearer Request message to inform the UE.

[00100] In step S806, the MME may send a Modify Bearer Request message including eNodeB address, eNodeB TEID to the SGW. The SGW acknowledges by sending, in step S807, Modify Bearer Response message including EPS Bearer Identity to the MME.

[00101] In step S809, the UE may store the related emergency access point name received in step 805 for potential use in following emergency handover to the untrusted non-3GPP based access network.

[00102] Fig. 9 is a diagram schematically illustrating an

exemplary flow chart of a method 900 implemented by a first gateway node according to one or more embodiments of the present disclosure.

[00103] As shown in Fig. 9, the method 900 begins at step S910 where the first gateway node (e.g., the first gateway node 110) receives a request message sent from a terminal device (e.g., the UE 120) that is currently performing an emergency call over the 3GPP based access network (130). The request message includes a handover indication and an emergency access point name which identifies an external network (one of the external networks 170) used to establish the emergency call. In some implementation, the request message may further include an emergency network access identifier constructed by the terminal device. The first gateway node detects, in step S920, an event of the emergency call handover based on the handover indication and the emergency network access identifier and then establishes, in step S930, an emergency call session with a second gateway node (e.g., the second gateway node 150) interfacing with the external network that is identified by the emergency access point name included in the request message.

[00104] According to one or more embodiments of the present disclosure, during the establishment of the emergency call session, the first gateway node may send to the second gateway node a create session request including the handover indication and the emergency access point name, thereby enabling the second gateway node to identify the emergency call session and perform the emergency call handover. The first gateway node may also need to perform authentication procedure for the terminal device based on an equipment identity of the terminal device.

[00105] Fig. 10 is an example signaling diagram illustrating

an embodiment where a handover of an emergency call is performed from a 3GPP based access network to an untrusted non-3GPP based access network.

[00106] As shown in Fig. 10, the UE communicates wirelessly with an eNodeB of the 3GPP based access network and accesses to the external networks (e.g., public Internet, Intranet, operator's IMS networks) over the 3GPP based access network (for example, a LTE network). In the example of Fig. 10, the first gateway node may be an ePDG and the second gateway node may be a PGW.

[00107] In step S1001, the UE may discover the untrusted non-3GPP based access network (e.g., a WiFi network) and determine to handover its emergency call session from the currently used 3GPP based access network to the untrusted non-3GPP based access network. The UE and the ePDG may exchange the first pair of IKE_SA_INIT messages, in which the ePDG and the UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie-Hellman exchange, for example, as specified in 3GPP TS 33.402 V12.5.0.

[00108] In step S1002, the UE may send a request message IKE AUTH_REQ for the handover of the emergency call to the ePDG. The emergency call handover request includes a Handover Indication and the emergency access point name the UE received, for example, at step S805 of Fig. 8. In some implementations, according to the current standard, the UE may indicate "Handover" by including its preserved IP address in the IKE AUTH_REQ message. Alternatively or additionally, the emergency call handover request may further include an emergency network access identifier, which may include a predetermined indicator of the emergency call and may be compliant with the definition of 3GPP TS 23.003 series.

[00109] In step S1003, the ePDG detects the emergency call

handover request depending upon the emergency network access identifier and the handover indication. The ePDG selects the corresponding PGW based on the emergency access point name included in the IKE AUTH_REQ message. The ePDG emergency APN configuration must be consistent with the ones in MME to ensure the same PGW selected in the emergency handover between 3GPP and non-3GPP.

[00110] In step 1004, the ePDG may perform the local EAP authentication or the remote EAP authentication with an AAA server (not shown in Fig. 10) based on UE Identity (e.g., International Mobile Equipment Identity (IMEI) or International Mobile Subscriber Identification Number (IMSI)) and configuration. For IMEI case, only local EAP authentication needs to be performed.

[00111] In step S1005, the UE may send the AUTH parameter to the ePDG.

[00112] In steps S1006 and S1007, the ePDG establishes for the UE an emergency call session with the PGW that interfaces with the external network identified by the emergency access point name included in the IKE AUTH_REQ message. Specifically, the ePDG may send (S1006) a Create Session Request including the UE's IMSI or IMEI, the emergency access point name and the handover indication to the PGW. Upon receipt of the Create Session Request, the PGW may detect the emergency call handover request from 3GPP based on the emergency access point name and the handover indication, then handles accordingly and return (S1007) a Create Session Response.

[00113] In step S1008, the ePDG may send the parameters received from PGW (e.g., UE IP address) to the UE in an IKE AUTH_RSP message.

[00114] Fig. 11 is a schematic block diagram depicting a first gateway node 1100 operably for processing an emergency call

according to an embodiment of the present disclosure.

[00115] As shown in Fig. 11, the first gateway node 1100 is configured to process an emergency call over an untrusted non-3GPP based access network. The first gateway 1100
5 comprises a receiving unit 1110, a detecting unit 1120, a selecting unit 1130 and a session establishing unit 1140. The first gateway node 1100 may comprise multiple suitable network communications interfaces for communications with corresponding network elements, as described with reference
10 to Fig. 1.

[00116] The first gateway node 1100 comprises a processor 11, which may include one or more microprocessor or microcontrollers, as well as other digital hardware, which may include digital signal processors (DSPs), special-purpose
15 digital logic, and the like. The processor 11 may be configured to execute program code stored in memory (not shown in Fig. 11), which may include one or several types of memory such as read-only memory (ROM), random-access memory, cache memory, flash memory devices, optical storage devices, etc.
20 Program code stored in memory includes program instructions for executing one or more telecommunications and/or data communications protocols as well as instructions for carrying out one or more of the techniques described herein, in several embodiments. In some implementations, the processor 11 may
25 be used to cause the receiving unit 1110, the detecting unit 1120, the selecting unit 1130 and the session establishing unit 1140 to perform corresponding functions according one or more embodiments of the present disclosure.

[00117] The receiving unit 1110 is configured to receive an
30 emergency call request initiated from a terminal device over an untrusted non-3GPP based access network. The emergency call request includes an emergency network access identifier

constructed by the terminal device. The detecting unit 1120 is configured to detect an event of the emergency call depending upon the emergency network access identifier. The selecting unit 1130 is configured to select for the terminal
5 device an emergency access point name that identifies an external network providing an emergency call service. The session establishing unit 1140 is configured to establish for the terminal device an emergency call session with a second gateway node interfacing with the external network which is
10 identified by the emergency access point name selected by the selecting unit 1130.

[00118] According to one or more embodiments of the present disclosure, the first gateway node 1100 may further comprise a transmitting unit (not shown in Fig. 11) configured to inform
15 the terminal device of the selected emergency access point name for following potential use of handover from the untrusted non-3GPP based access network to a 3GPP based access network.

[00119] According to one or more embodiments of the present disclosure, the session establishing unit 1140 may be further
20 configured to send to the second gateway node a create session request including the selected emergency access point name, thereby enabling the second network node to identify the emergency call session. The session establishing unit 1140
25 may be further configured to authenticate the terminal device based on an equipment identity of the terminal device.

[00120] Fig. 12 is a schematic block diagram depicting a terminal device 1200 operably for processing an emergency call according to an embodiment of the present disclosure.

30 [00121] As shown in Fig. 12, the terminal device 1200 is configured to initiate an emergency call over an untrusted non-3GPP based access network. The terminal device 1200

comprises: an identifier constructing unit 1210, a transmitting unit 1220, a session establishing unit 1230. The terminal device 1200 may also comprise multiple suitable radio frequency transceivers (not shown in Fig. 12) that may be
5 selectively coupled with one or more antenna(s) (not shown in Fig. 12) which are used to transmit signals to, and receive signals from, other radio nodes such as an eNodeB or a WiFi AP.

[00122] The terminal device 1200 comprises a processor 12,
10 which may include one or more microprocessor or microcontrollers, as well as other digital hardware, which may include digital signal processors (DSPs), special-purpose digital logic, and the like. The processor 12 may be configured to execute program code stored in memory (not shown
15 in Fig. 12), which may include one or several types of memory such as read-only memory (ROM), random-access memory, cache memory, flash memory devices, optical storage devices, etc. Program code stored in memory includes program instructions for executing one or more telecommunications and/or data
20 communications protocols as well as instructions for carrying out one or more of the techniques described herein, in several embodiments. In some implementations, the processor 12 may be used to cause the identifier unit 1210, the transmitting unit 1220, the session establishing unit 1230 to perform
25 corresponding functions according one or more embodiments of the present disclosure.

[00123] The identifier constructing unit 1210 is configured to construct an emergency network access identifier. According to one or more embodiments of the present disclosure,
30 the emergency network access identifier may include a predetermined indicator of the emergency call. The transmitting unit 1220 is configured to send to a first gateway node an emergency call request including the constructed

emergency network access identifier. The session establishing unit 1230 is configured to establish, via the first gateway node, an emergency call session with a second gateway node interfacing with an external network providing an emergency call service.

[00124] According to one or more embodiments of the present disclosure, the terminal device 1200 may further comprise a receiving unit (not shown in Fig. 12) configured to receive from the first gateway node an emergency access point name, thereby facilitating potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

[00125] Fig. 13 is a schematic block diagram depicting a 3GPP network node 1300 operably for facilitating emergency call handover from an untrusted non-3GPP based access network to the 3GPP based access network according to an embodiment of the present disclosure.

[00126] As shown in Fig. 13, the network node 1300 of a 3GPP based access network is configured to facilitate emergency call handover from an untrusted non-3GPP based access network to the 3GPP based access network. The network node 1300 comprises a receiving unit 1310, a detecting unit 1320, a session establishing unit 1330, a switching unit 1340. The network node 1300 may comprise multiple suitable network communications interfaces for communications with corresponding network elements, as described with reference to Fig. 1.

[00127] The network node 1300 comprises a processor 13, which may include one or more microprocessor or microcontrollers, as well as other digital hardware, which may include digital signal processors (DSPs), special-purpose digital logic, and the like. The processor 13 may be configured to execute program code stored in memory (not shown in Fig. 13), which

may include one or several types of memory such as read-only memory (ROM), random-access memory, cache memory, flash memory devices, optical storage devices, etc. Program code stored in memory includes program instructions for executing one or more telecommunications and/or data communications protocols as well as instructions for carrying out one or more of the techniques described herein, in several embodiments. In some implementations, the processor 13 may be used to cause the receiving unit 1310, the detecting unit 1320, the session establishing unit 1330 and the switching unit 1340 to perform corresponding functions according one or more embodiments of the present disclosure.

[00128] The receiving unit 1310 is configured to receive a request message sent from a terminal device that is currently performing an emergency call over the untrusted non-3GPP based access network. The request message includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call. According to one or more embodiments of the present disclosure, the request message may be a packet data network connectivity request message or an attach request message. The detecting unit 1320 is configured to detect an event of the emergency call handover based on the handover indication and the emergency access point name. The session establishing unit 1330 is configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name. The switching unit 1340 is configured to switch the emergency call of the terminal device from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network.

[00129] According to one or more embodiments of the present disclosure, the session establishing unit 1330 may be further

configured to send to the second gateway node a create session request including the emergency access point name, thereby enabling the second gateway node to identify the emergency call session.

5 [00130] Fig. 14 is a schematic block diagram depicting a 3GPP network node 1400 operably for processing an emergency call according to an embodiment of the present disclosure.

[00131] As shown in Fig. 14, the network node 1400 is configured to process an emergency call over a 3GPP based
10 access network. The network node 1400 comprises a receiving unit 1410, a selecting unit 1420, a session establishing unit 1430. The network node 1400 may comprise multiple suitable network communications interfaces for communications with corresponding network elements, as described with reference
15 to Fig. 1.

[00132] The network node 1400 comprises a processor 14, which may include one or more microprocessor or microcontrollers, as well as other digital hardware, which may include digital signal processors (DSPs), special-purpose digital logic, and
20 the like. The processor 14 may be configured to execute program code stored in memory (not shown in Fig. 14), which may include one or several types of memory such as read-only memory (ROM), random-access memory, cache memory, flash memory devices, optical storage devices, etc. Program code
25 stored in memory includes program instructions for executing one or more telecommunications and/or data communications protocols as well as instructions for carrying out one or more of the techniques described herein, in several embodiments. In some implementations, the processor 14 may be used to cause
30 the receiving unit 1410, the selecting unit 1420, the session establishing unit 1430 to perform corresponding functions according one or more embodiments of the present disclosure.

[00133] The receiving unit 1410 is configured to receive an emergency call request initiated from a terminal device over a 3GPP based access network. The selecting unit 1420 is configured to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service; the session establishing unit 1430 is configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the emergency access point name selected by the selecting unit 1420.

[00134] According to one or more embodiments of the present disclosure, the network node 1400 may further comprise a transmitting unit configured to inform the terminal device of the selected emergency access point name.

[00135] Fig. 15 is a schematic block diagram depicting a first gateway node 1500 operably for facilitating emergency call handover from a 3GPP based access network to an untrusted non-3GPP based access network according to an embodiment of the present disclosure.

[00136] As shown in Fig. 15, the first gateway node 1500 is configured to facilitate emergency call handover from a 3GPP based access network to an untrusted non-3GPP based access network. The first gateway 1500 comprises a receiving unit 1510, a detecting unit 1520 and a session establishing unit 1530. The first gateway node 1500 may comprise multiple suitable network communications interfaces for communications with corresponding network elements, as described with reference to Fig. 1.

[00137] The first gateway node 1500 comprises a processor 15, which may include one or more microprocessor or microcontrollers, as well as other digital hardware, which may include digital signal processors (DSPs), special-purpose

digital logic, and the like. The processor 15 may be configured to execute program code stored in memory (not shown in Fig. 15), which may include one or several types of memory such as read-only memory (ROM), random-access memory, cache
5 memory, flash memory devices, optical storage devices, etc. Program code stored in memory includes program instructions for executing one or more telecommunications and/or data communications protocols as well as instructions for carrying out one or more of the techniques described herein, in several
10 embodiments. In some implementations, the processor 15 may be used to cause the receiving unit 1510, the detecting unit 1520, and the session establishing unit 1540 to perform corresponding functions according one or more embodiments of the present disclosure.

15 [00138] The receiving unit 1510 is configured to receive a request message sent from a terminal device that is currently performing an emergency call over the 3GPP based access network. The request message includes a handover indication and an emergency access point name which identifies an
20 external network used to establish the emergency call. According to one or more embodiments of the present disclosure, the request message received by the receiving unit may further include an emergency network access identifier constructed by the terminal device. The detecting unit 1520 is configured
25 to detect an event of the emergency call handover based on the handover indication and the emergency network access identifier. The session establishing unit 1530 is configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified
30 by the emergency access point name included in the request message.

[00139] According to one or more embodiments of the present disclosure, the session establishing unit 1530 may be

configured to send to the second gateway node a create session request including the handover indication and the emergency access point name, thereby enabling the second gateway node to identify the emergency call session and perform the emergency call handover. The session establishing unit 1530 may be further configured to authenticate the terminal device based on an equipment identity of the terminal device.

[00140] According to one or more embodiments of the present disclosure, a user is allowed to make an emergency call even over an untrusted non-3GPP based access network, for example, a WiFi residential environment. In a meanwhile, the continuity of the emergency call session can be maintained by appropriately handing over between the untrusted non-3GPP based access network and a 3GPP based access network.

[00141] In general, the various exemplary embodiments may be implemented in hardware or special purpose circuits, software, logical or any combination thereof. For example, some aspects may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device, although the disclosure is not limited thereto. While various aspects of the exemplary embodiments of this disclosure may be illustrated and described as block and signaling diagrams, it is well understood that these blocks, apparatus, systems, techniques or methods described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logical, general purpose hardware or controller or other computing devices, or some combination thereof.

[00142] As such, it should be appreciated that at least some aspects of the exemplary embodiments of the disclosure may be practiced in various components such as integrated circuit

chips and modules. As well known in the art, the design of integrated circuits is by and large a highly automated process.

[00143] The present disclosure may also be embodied in the computer program product which comprises all features capable of implementing the method as depicted herein and may implement the method when loaded to the computer system.

[00144] The present disclosure has been specifically illustrated and explained with reference to the preferred embodiments. The skilled in the art should understand various changes thereto in form and details may be made without departing from the spirit and scope of the present disclosure.

WHAT IS CLAIMED IS:

1. A method (200) implemented by a first gateway node (140) for processing an emergency call, comprising:

5 receiving (S210) an emergency call request initiated from a terminal device (120) over an untrusted non-3GPP based access network (110), wherein the emergency call request includes an emergency network access identifier constructed by the terminal device (120);

10 detecting (S220) an event of the emergency call depending upon the emergency network access identifier;

selecting (S230) for the terminal device (120) an emergency access point name that identifies an external network (170) providing an emergency call service;

15 establishing (S240) for the terminal device (120) an emergency call session with a second gateway node (150) interfacing with the external network (170) which is identified by the selected emergency access point name.

20 2. The method according to Claim 1, further comprising informing the terminal device of the selected emergency access point name, thereby facilitating potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

25

3. The method according to any of Claims 1-2, wherein establishing an emergency call session for the terminal device comprises:

30 sending to the second gateway node a create session request including the selected emergency access point name,

thereby enabling the second network node to identify the emergency call session.

4. The method according to any of Claims 1-3, wherein
5 establishing an emergency call session for the terminal device comprises:

authenticating the terminal device based on an equipment identity of the terminal device.

10 5. A method (300) implemented by a terminal device (120) for initiating an emergency call over an untrusted non-3GPP based access network (110), comprising:

constructing (S310) an emergency network access identifier;

15 sending (S320) to a first gateway node (140) an emergency call request including the constructed emergency network access identifier;

establishing (S330), via the first gateway node (140), an emergency call session with a second gateway node (150)
20 interfacing with an external network (170) providing an emergency call service.

6. The method according to Claim 5, wherein the emergency network access identifier includes a predetermined indicator
25 of the emergency call.

7. The method according to any of Claim 5-6, further comprising:

receiving from the first gateway node an emergency access

point name, thereby facilitating potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

5 8. A method (500) implemented by a network node of a 3GPP based access network (130) for facilitating emergency call handover from an untrusted non-3GPP based access network (110) to the 3GPP based access network (130), comprising:

 receiving (S510) a request message sent from a terminal
10 device (120) that is currently performing an emergency call over the untrusted non-3GPP based access network (110), wherein the request message includes a handover indication and an emergency access point name which identifies an external network (170) used to establish the emergency call;

15 detecting (S520) an event of the emergency call handover based on the handover indication and the emergency access point name;

 establishing (S530) an emergency call session with a second gateway node (150) interfacing with the external
20 network (170) that is identified by the selected emergency access point name;

 switching (S540) the emergency call of the terminal
25 device (120) from bearer of the untrusted non-3GPP based access network (110) to the bearer of the 3GPP based access network (130).

 9. The method according to Claim 8, wherein the request message is a packet data network connectivity request message or an attach request message.

10. The method according to any of Claims 8-9, wherein establishing an emergency call session with a second gateway node comprises:

5 sending to the second gateway node a create session request including the emergency access point name, thereby enabling the second gateway node to identify the emergency call session.

11. A method (700) implemented by a network node of a 10 3GPP based access network (130) for processing an emergency call, comprising:

receiving (S710) an emergency call request initiated from a terminal device (120) over a 3GPP based access network (130);

15 selecting (S720) for the terminal device (120) an emergency access point name that identifies an external network (170) providing an emergency call service;

20 establishing (S730) an emergency call session with a second gateway node (150) interfacing with the external network (170) that is identified by the selected emergency access point name.

12. The method according to Claim 11, further comprising:

25 informing the terminal device of the selected emergency access point name, thereby facilitating potential handover from the 3GPP based access network to an untrusted non-3GPP based access network.

13. A method (900) implemented by a first gateway node 30 (140) for facilitating emergency call handover from a 3GPP

based access network (130) to an untrusted 3GPP based access network (110), comprising:

receiving (S910) a request message sent from a terminal device (120) that is currently performing an emergency call over the 3GPP based access network (130), wherein the request message includes a handover indication and an emergency access point name which identifies an external network (170) used to establish the emergency call;

detecting (S920) an event of the emergency call handover based on the handover indication and the emergency network access identifier;

establishing (S930) an emergency call session with a second gateway node (150) interfacing with the external network (170) that is identified by the emergency access point name included in the request message.

14. The method according to Claim 13, wherein establishing an emergency call session for the terminal device comprises:

sending to the second gateway node a create session request including the handover indication and the emergency access point name, thereby enabling the second gateway node to identify the emergency call session and perform the emergency call handover.

25

15. The method according to any of Claims 13-14, wherein establishing an emergency call session for the terminal device comprises:

authenticating the terminal device based on an equipment identity of the terminal device.

30

16. The method according to any of Claims 13-15, wherein the request message further includes an emergency network access identifier constructed by the terminal device.

5

17. A first gateway node (1100) operably for processing an emergency call, comprising:

10 a receiving unit (1110) configured to receive an emergency call request initiated from a terminal device over an untrusted non-3GPP based access network, wherein the emergency call request includes an emergency network access identifier constructed by the terminal device;

15 a detecting unit (1120) configured to detect an event of the emergency call depending upon the emergency network access identifier;

a selecting unit (1130) configured to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service;

20 a session establishing unit (1140) configured to establish for the terminal device an emergency call session with a second gateway node interfacing with the external network which is identified by the selected emergency access point name.

25 18. The first gateway node according to Claim 17, further comprising:

30 a transmitting unit configured to inform the terminal device of the selected emergency access point name, thereby facilitating potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

19. The first gateway node according to any of Claims 17-18, wherein the session establishing unit (1140) is further configured to send to the second gateway node a create session request including the selected emergency access point name, thereby enabling the second network node to identify the emergency call session.

20. The first gateway node according to any of Claims 17-19, wherein the session establishing unit (1140) is further configured to authenticate the terminal device based on an equipment identity of the terminal device.

21. A terminal device (1200) operably for initiating an emergency call over an untrusted non-3GPP based access network, comprising:

an identifier constructing unit (1210) configured to construct an emergency network access identifier;

a transmitting unit (1220) configured to send to a first gateway node an emergency call request including the constructed emergency network access identifier;

a session establishing unit (1230) configured to establish, via the first gateway node, an emergency call session with a second gateway node interfacing with an external network providing an emergency call service.

22. The terminal device according to Claim 21, wherein the emergency network access identifier includes a predetermined indicator of the emergency call.

23. The terminal device according to any of Claim 21-22, further comprising:

a receiving unit configured to receive from the first gateway node an emergency access point name, thereby
5 facilitating potential handover from the untrusted non-3GPP based access network to a 3GPP based access network.

24. A network node (1300) of a 3GPP based access network operably for facilitating emergency call handover from an
10 untrusted non-3GPP based access network to the 3GPP based access network, comprising:

a receiving unit (1310) configured to receive a request message sent from a terminal device that is currently performing an emergency call over the untrusted non-3GPP based
15 access network, wherein the request message includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call;

a detecting unit (1320) configured to detect an event
20 of the emergency call handover based on the handover indication and the emergency access point name;

a session establishing unit (1330) configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by
25 the selected emergency access point name;

a switching unit (1340) configured to switch the emergency call of the terminal device from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network.

25. The network node according to Claim 24, wherein the request message is a packet data network connectivity request message or an attach request message.

5 26. The network node according to any of Claims 24-25, wherein the session establishing unit (1330) is further configured to send to the second gateway node a create session request including the emergency access point name, thereby enabling the second gateway node to identify the emergency
10 call session.

27. A network node (1400) of a 3GPP based access network operably for processing an emergency call, comprising:

15 a receiving unit (1410) configured to receive an emergency call request initiated from a terminal device over a 3GPP based access network;

 a selecting unit (1420) configured to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service;

20 a session establishing unit (1430) configured to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name.

25 28. The network node according to Claim 27, further comprising:

 a transmitting unit configured to inform the terminal device of the selected emergency access point name, thereby facilitating potential handover from the 3GPP based access
30 network to an untrusted non-3GPP based access network.

29. A first gateway node (1500) operably for facilitating emergency call handover from a 3GPP based access network to an untrusted non-3GPP based access network, comprising:

5 a receiving unit (1510) configured to receive a request message sent from a terminal device that is currently performing an emergency call over the 3GPP based access network, wherein the request message includes a handover indication and an emergency access point name which identifies
10 an external network used to establish the emergency call;

a detecting unit (1520) configured to detect an event of the emergency call handover based on the handover indication and the emergency network access identifier;

a session establishing unit (1530) configured to
15 establish an emergency call session with a second gateway node interfacing with the external network that is identified by the emergency access point name included in the request message.

20 30. The first gateway node according to Claim 29, wherein the session establishing unit is configured to send to the second gateway node a create session request including the handover indication and the emergency access point name, thereby enabling the second gateway node to identify the
25 emergency call session and perform the emergency call handover.

31. The first gateway node according to any of Claims 29-30, wherein the session establishing unit is further
30 configured to authenticate the terminal device based on an equipment identity of the terminal device.

32. The first gateway node according to any of Claims 29-31, wherein the request message received by the receiving unit further includes an emergency network access identifier
5 constructed by the terminal device.

33. A first gateway node (1100) operably for processing an emergency call, comprising processing means adapted to:

cause to receive an emergency call request initiated from
10 a terminal device over an untrusted non-3GPP based access network, wherein the emergency call request includes an emergency network access identifier constructed by the terminal device;

cause to detect an event of the emergency call depending
15 upon the emergency network access identifier;

cause to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service;

cause to establish for the terminal device an emergency
20 call session with a second gateway node interfacing with the external network which is identified by the selected emergency access point name.

34. The first gateway node according to Claim 33, wherein
25 the processing means may comprise a processor (11) and a memory and the memory may contain instructions executable by the processor.

35. A terminal device (1200) operably for initiating an
30 emergency call over an untrusted non-3GPP based access network,

comprising processing means adapted to:

cause to construct an emergency network access identifier;

5 cause to send to a first gateway node an emergency call request including the constructed emergency network access identifier;

cause to establish, via the first gateway node, an emergency call session with a second gateway node interfacing with an external network providing an emergency call service.

10

36. The terminal device node according to Claim 35, wherein the processing means may comprise a processor (12) and a memory and the memory may contain instructions executable by the processor.

15

37. A network node (1300) of a 3GPP based access network for facilitating emergency call handover from an untrusted non-3GPP based access network to the 3GPP based access network, comprising processing means adapted to:

20 cause to receive a request message sent from a terminal device that is currently performing an emergency call over the untrusted non-3GPP based access network, wherein the request message includes a handover indication and an emergency access point name which identifies an external
25 network used to establish the emergency call;

cause to detect an event of the emergency call handover based on the handover indication and the emergency access point name;

30 cause to establish an emergency call session with a second gateway node interfacing with the external network that

is identified by the selected emergency access point name;

cause to switch the emergency call of the terminal device from bearer of the untrusted non-3GPP based access network to the bearer of the 3GPP based access network.

5

38. The network node according to Claim 33, wherein the processing means may comprise a processor (13) and a memory and the memory may contain instructions executable by the processor.

10

39. A network node (1400) of a 3GPP based access network operably for processing an emergency call, comprising processing means adapted to:

15 cause to receive an emergency call request initiated from a terminal device over a 3GPP based access network;

cause to select for the terminal device an emergency access point name that identifies an external network providing an emergency call service;

20 cause to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the selected emergency access point name.

40. The network node according to Claim 39, wherein the processing means may comprise a processor (14) and a memory and the memory may contain instructions executable by the processor.

41. A first gateway node (1500) operably for facilitating emergency call handover from a 3GPP based access network to

an untrusted non-3GPP based access network, comprising processing means adapted to:

cause to receive a request message sent from a terminal device that is currently performing an emergency call over the 3GPP based access network, wherein the request message includes a handover indication and an emergency access point name which identifies an external network used to establish the emergency call;

cause to detect an event of the emergency call handover based on the handover indication and the emergency network access identifier;

cause to establish an emergency call session with a second gateway node interfacing with the external network that is identified by the emergency access point name included in the request message.

42. The first gateway node according to Claim 41, wherein the processing means may comprise a processor (15) and a memory and the memory may contain instructions executable by the processor.

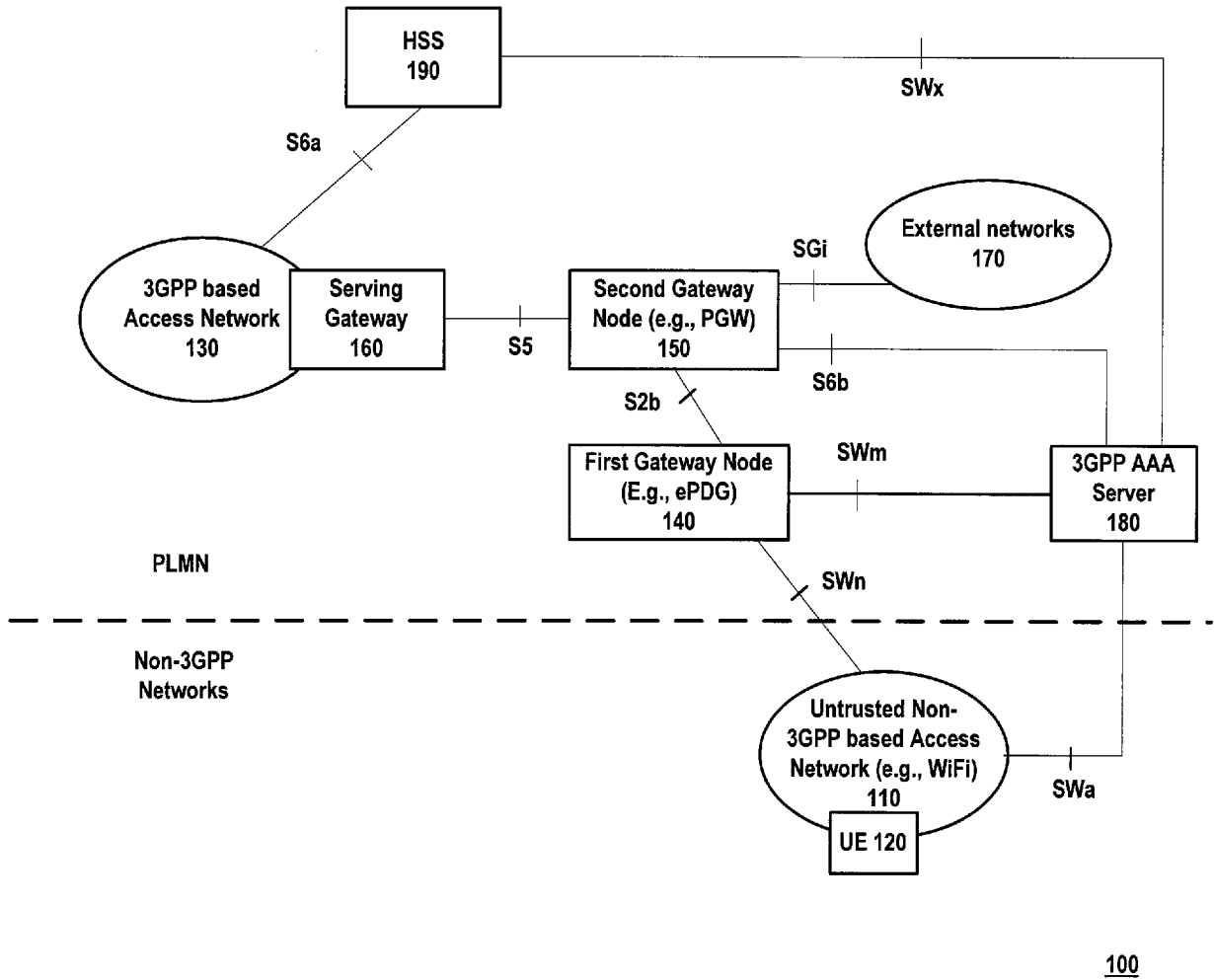
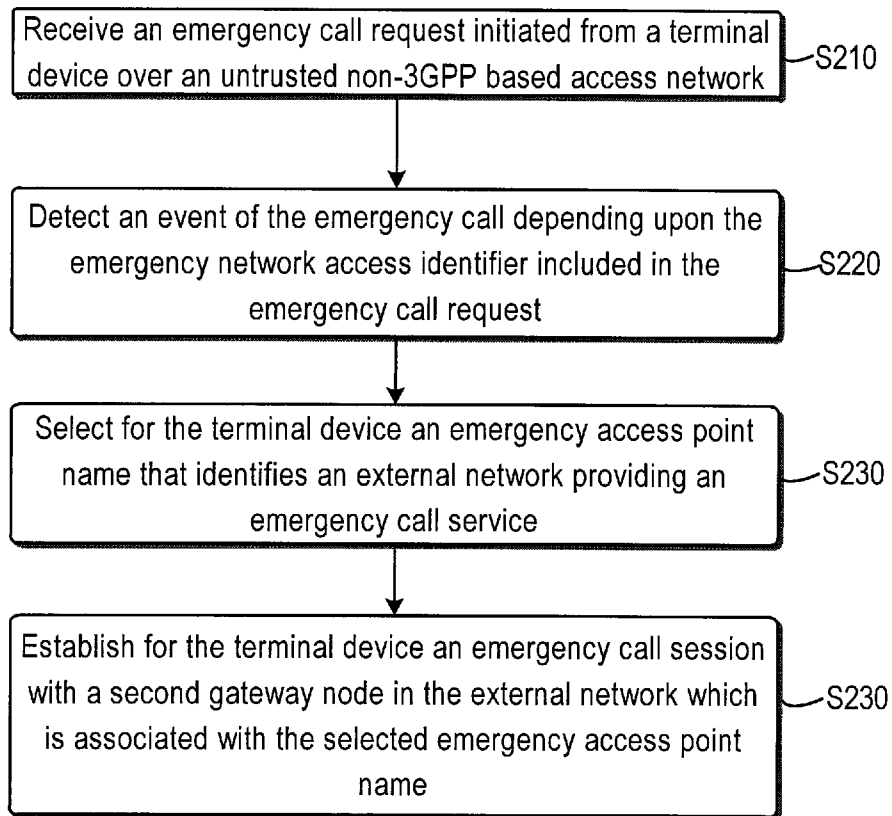


Fig. 1

200**Fig. 2**

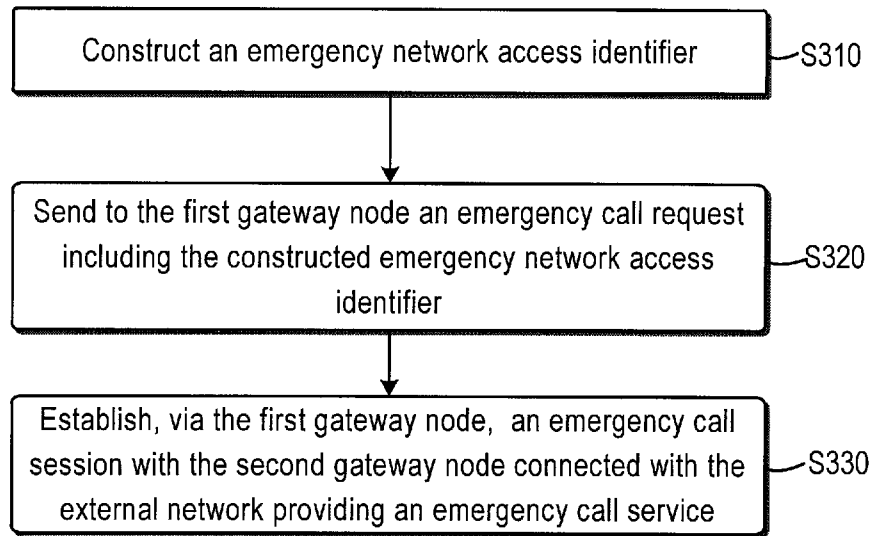


Fig. 3

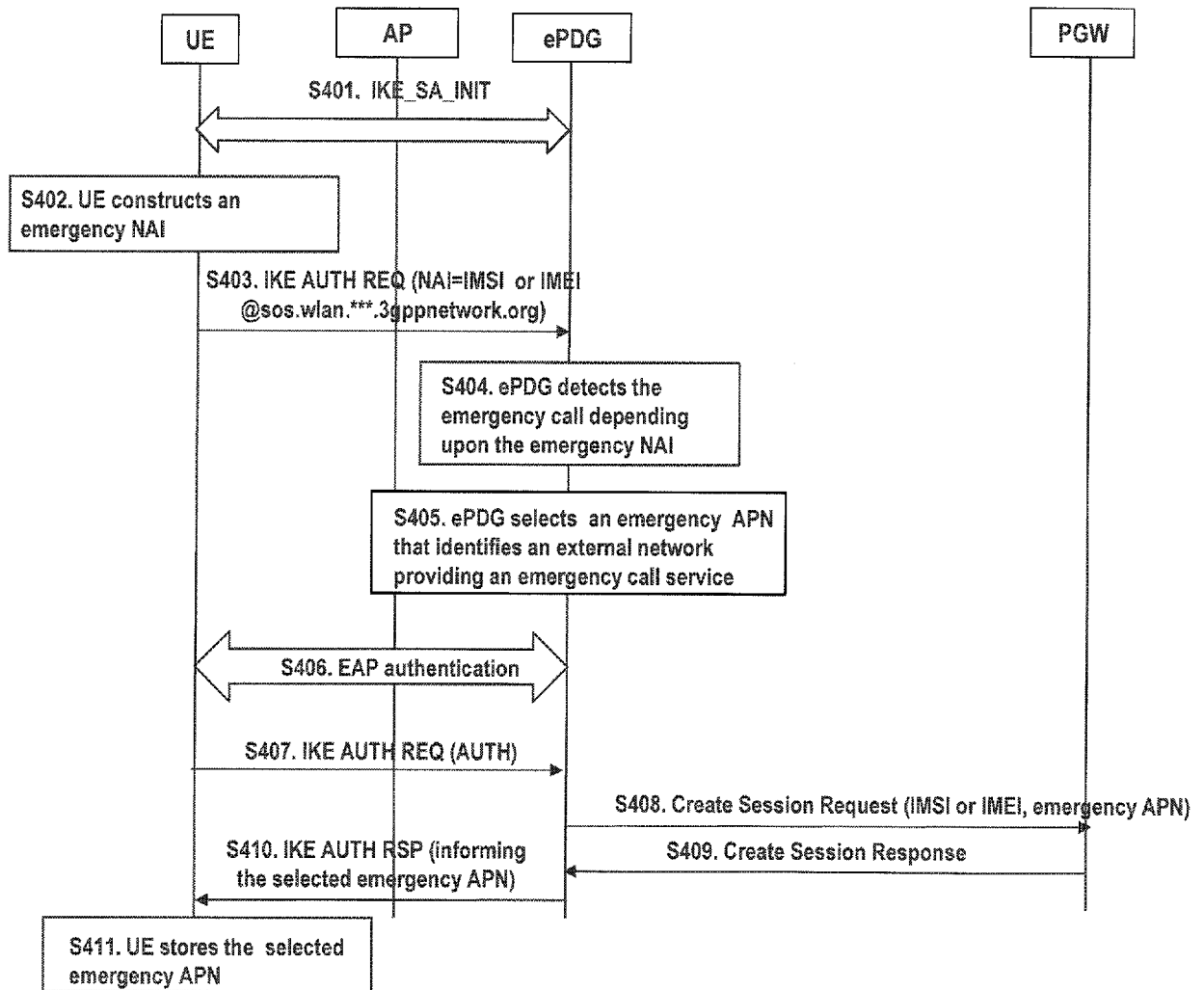


Fig. 4

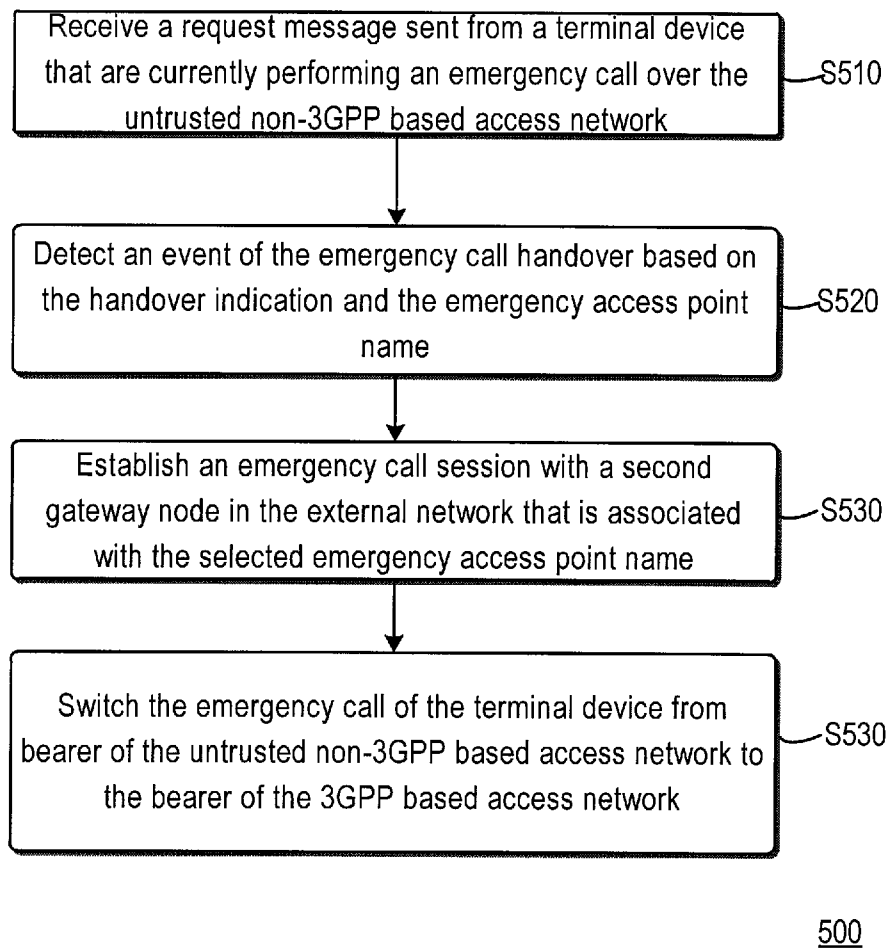


Fig. 5

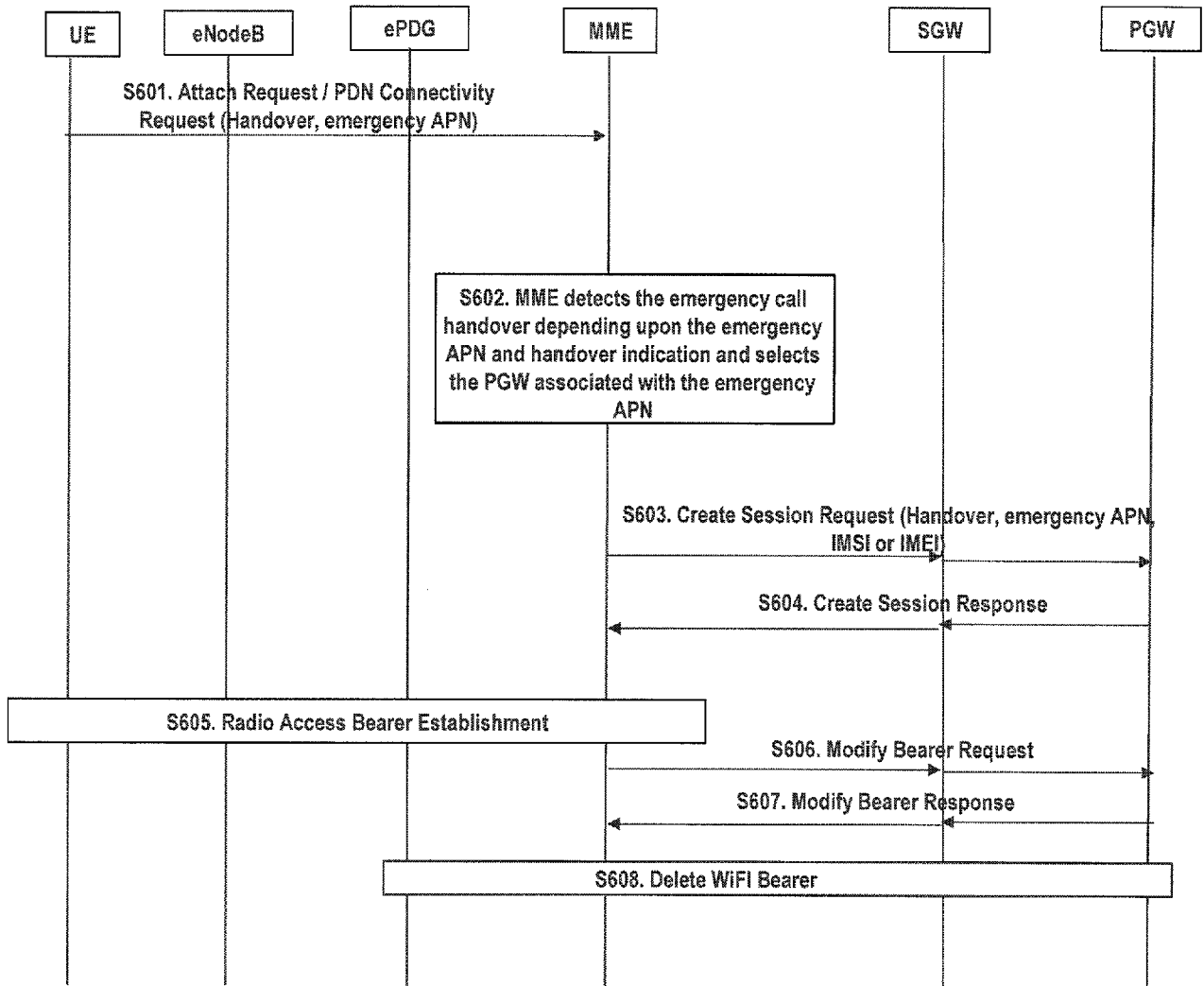


Fig. 6

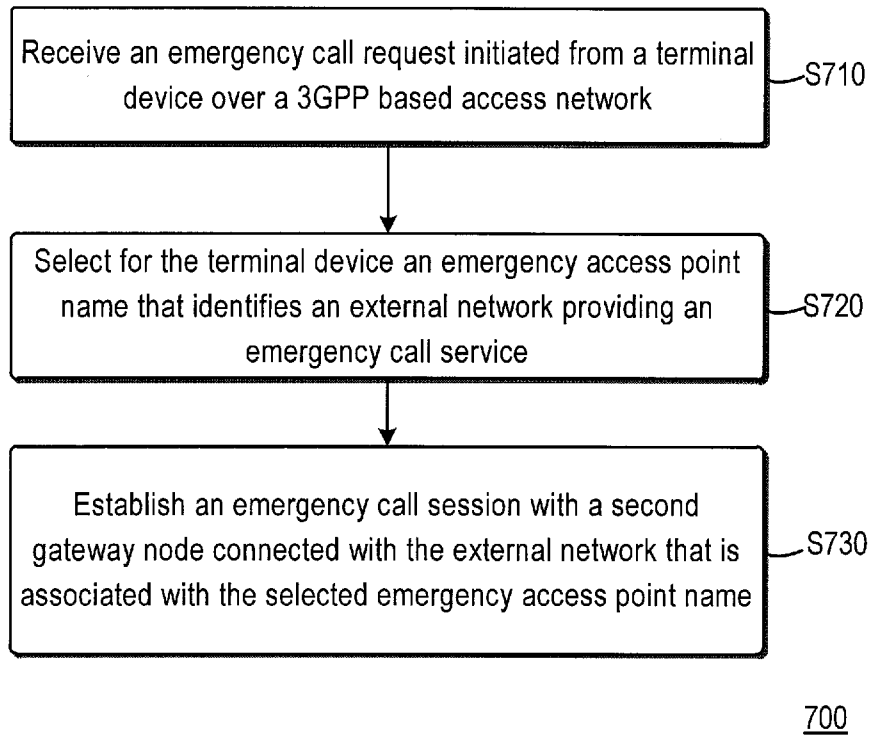


Fig. 7

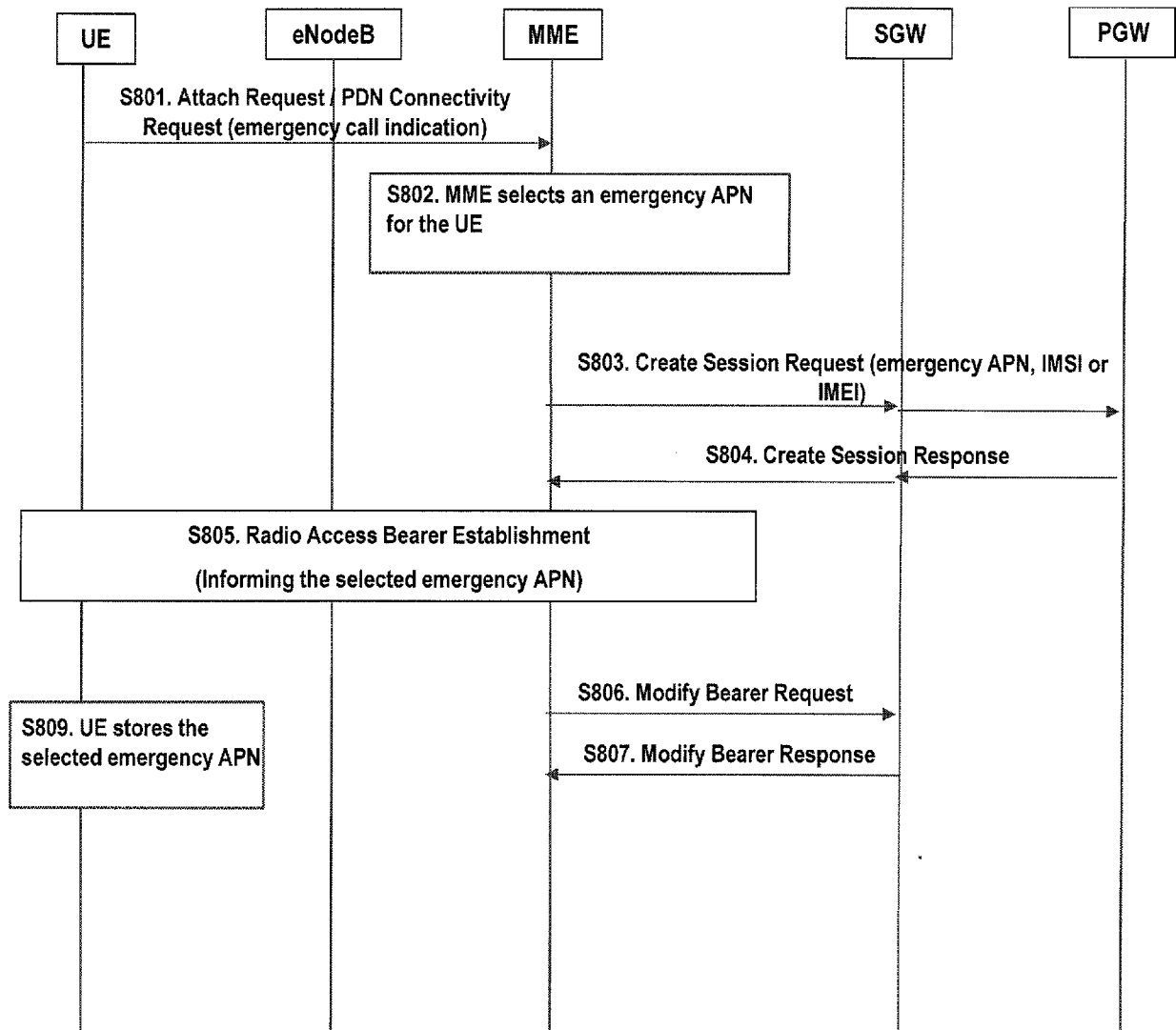
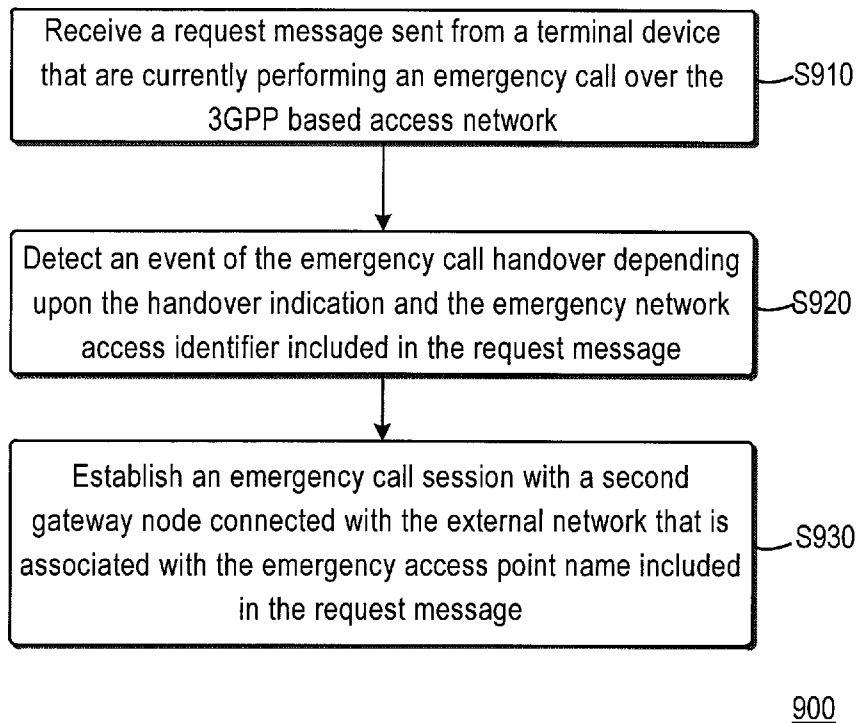


Fig. 8

**Fig. 9**

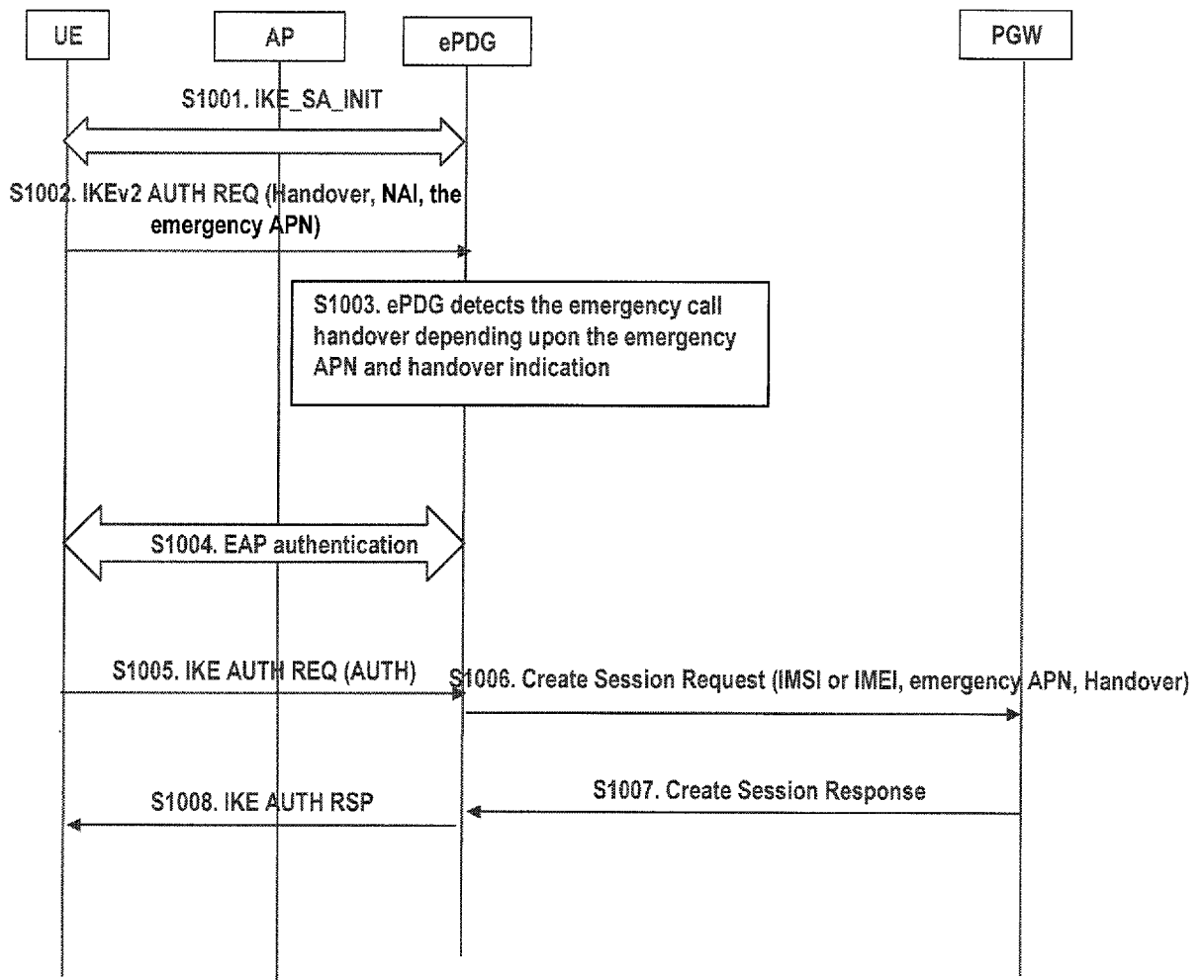


Fig. 10

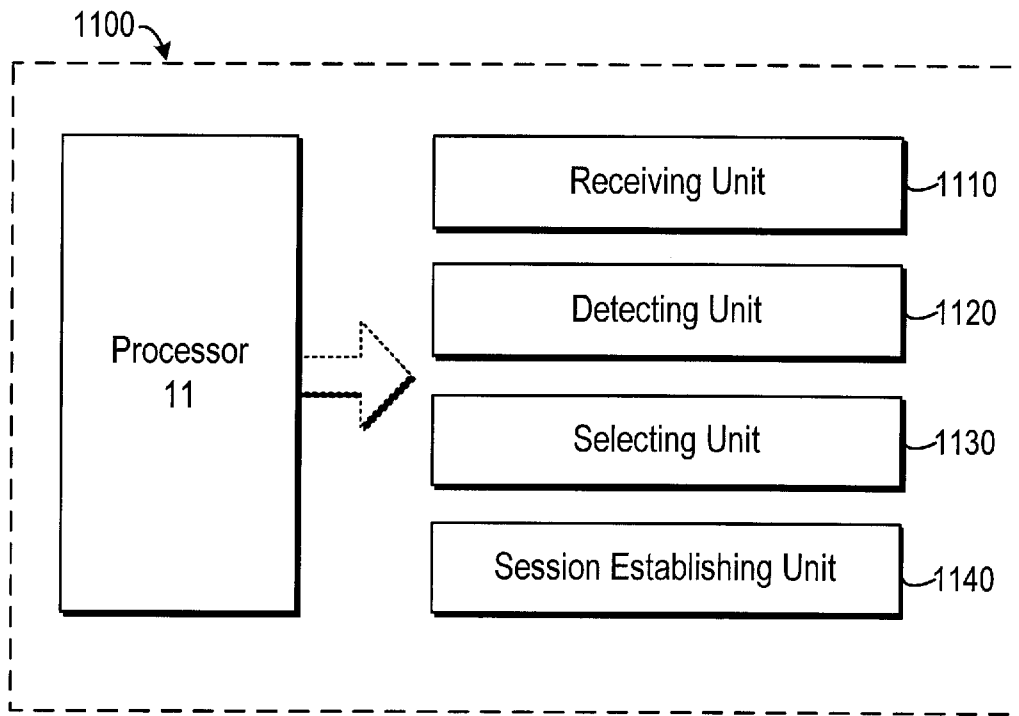


Fig. 11

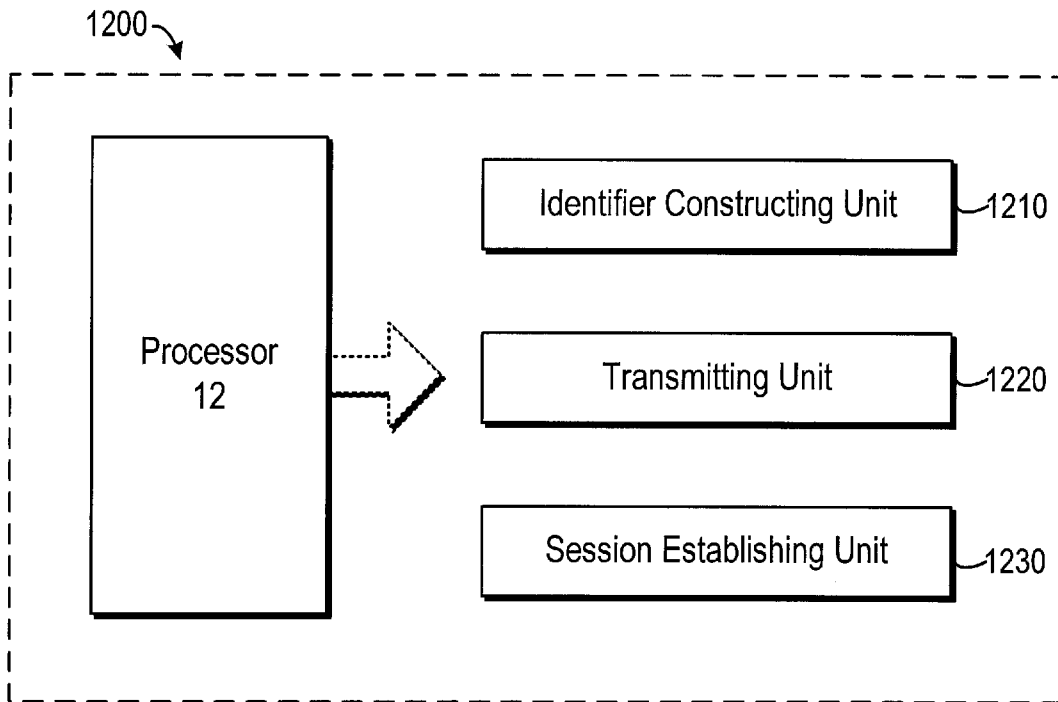


Fig. 12

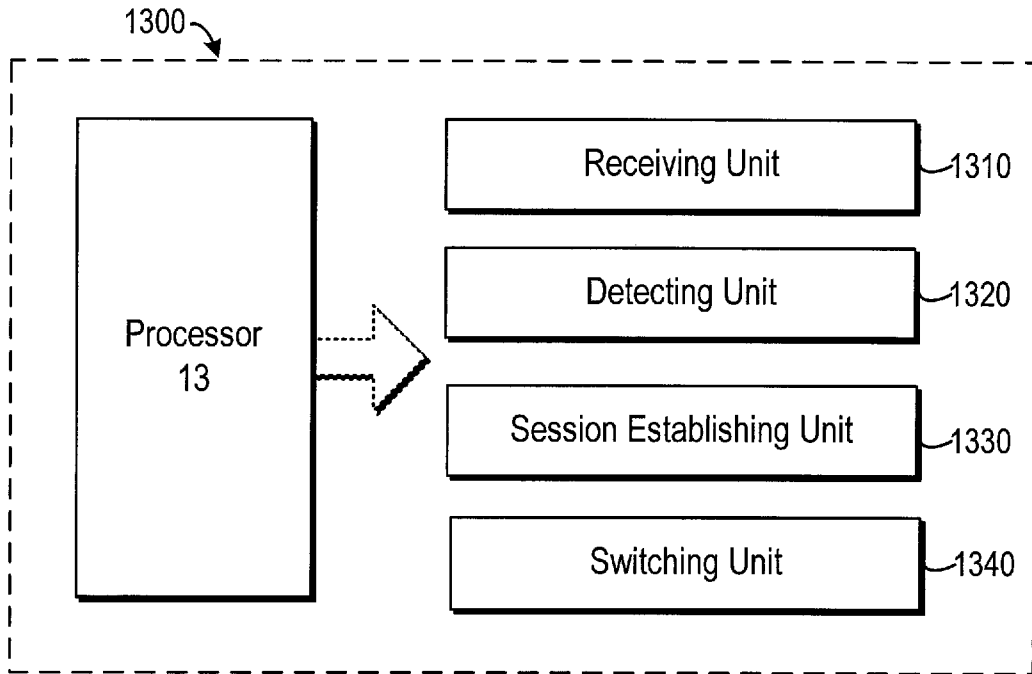


Fig. 13

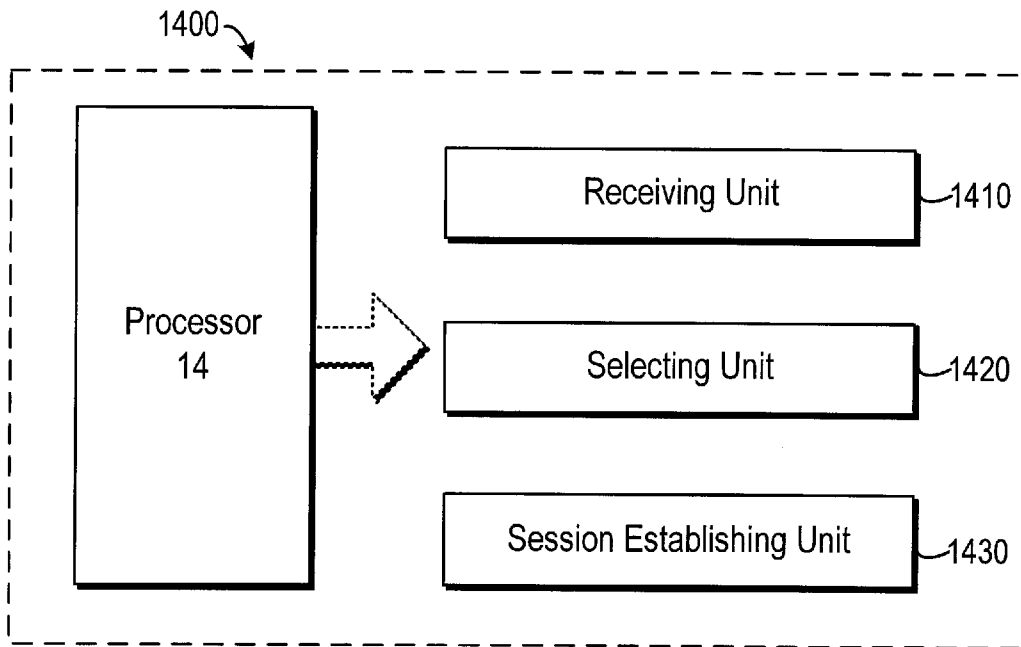


Fig. 14

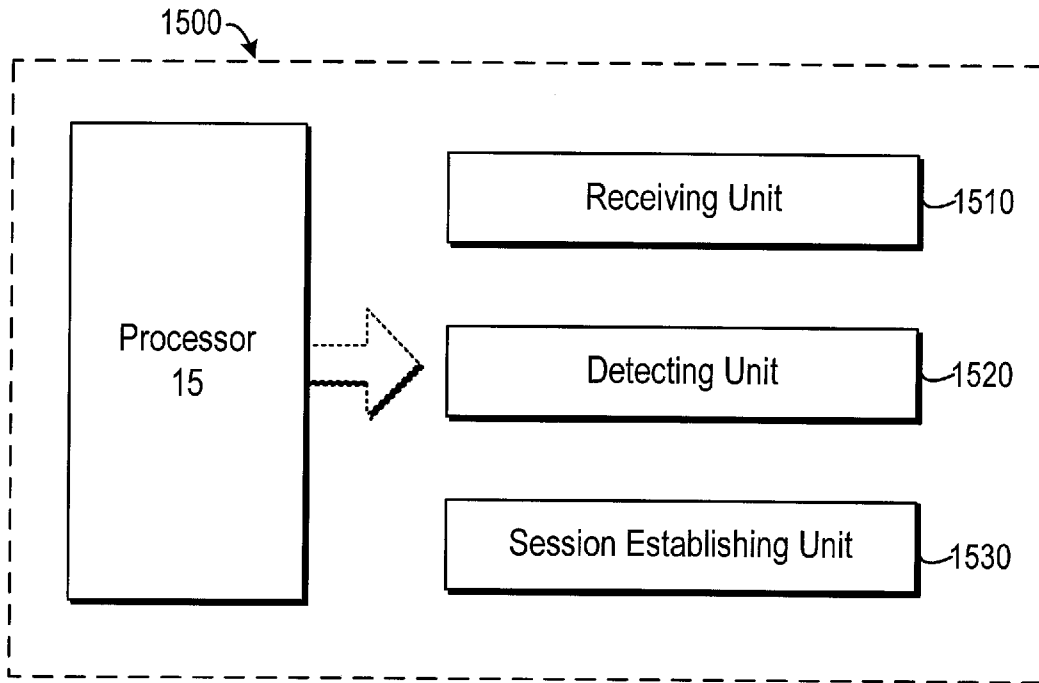


Fig. 15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/075612

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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)

CNABS,CNTXT,VEN,CNKI,IEEE: emergency, node, access, id, call, access, gateway, node, wifi, wimax, cdma, external, untrusted, session

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104247549 A (HUAWEI TECH CO LTD) 24 December 2014 (2014-12-24) the whole document	1-42
A	CN 101110758 A (HUAWEI TECH CO LTD) 23 January 2008 (2008-01-23) the whole document	1-42
A	US 2012314625 A1 (VERIZON PATENT & LICENSING INC) 13 December 2012 (2012-12-13) the whole document	1-42

 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

23 December 2015

Date of mailing of the international search report

07 January 2016

Name and mailing address of the ISA/CN

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

ZHANG, Xinyu

Telephone No. (86-10)62089388

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/075612

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104247549	A	24 December 2014	WO	2014090338	A1	19 June 2014
				EP	2932781	A1	21 October 2015
CN	101110758	A	23 January 2008	US	9001835	B2	07 April 2015
				CN	102291395	B	05 November 2014
				US	8040905	B2	18 October 2011
				CN	102291395	A	21 December 2011
				US	2009122793	A1	14 May 2009
				US	2011310774	A1	22 December 2011
				CN	101317493	B	03 August 2011
				WO	2008011833	A1	31 January 2008
				CN	101317493	A	03 December 2008
US	2012314625	A1	13 December 2012	US	9042298	B2	26 May 2015