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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 August 2020 (27.08.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/171765 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04W 12/06* (2009.01)
H04W 12/00 (2009.01)

(21) International Application Number:
PCT/SE2020/050194

(22) International Filing Date:
19 February 2020 (19.02.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/809,328 22 February 2019 (22.02.2019) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; SE-164 83 Stockholm (SE).

(72) Inventors: **YANG, Yong**; Heljereds Byväg 111B, 428 36 Kållered (SE). **OLSSON, Tony**; Lyr-Bö 151, 474 96 Nösund (SE).

(74) Agent: **ERICSSON AB**; Patent Development, Torshamnsgatan 21-23, 164 80 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) Title: MITIGATING DOS ATTACKS

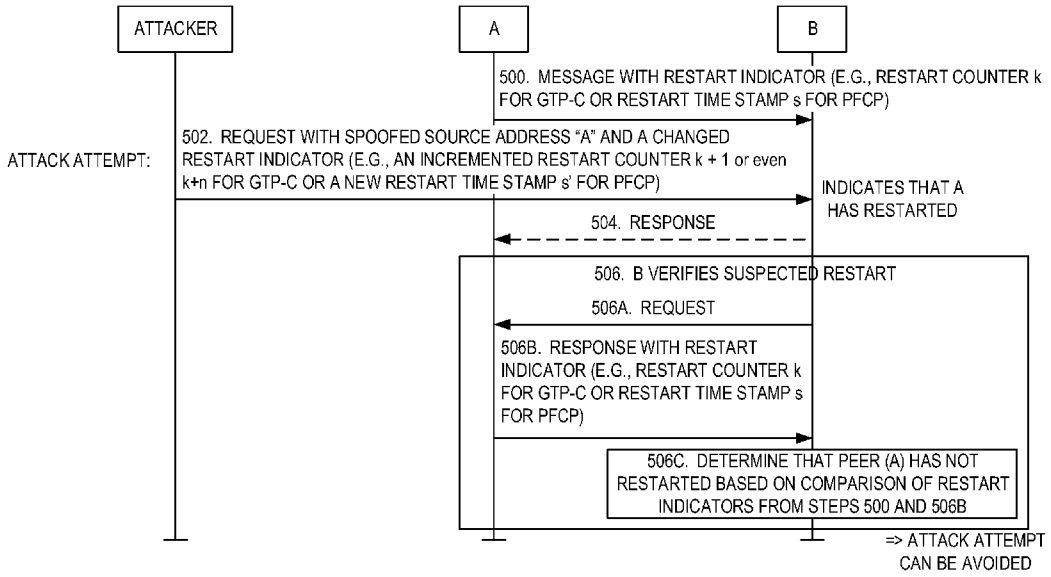

FIG. 5

(57) Abstract: Disclosed herein is a method performed by GTP-C or PFCP entity B, 200, the method comprising: receiving 500, 600, from a peer entity A, 202, a first message comprising a first restart indicator for the peer entity; receiving 502, 602 a second message comprising a changed restart indicator for the peer entity that indicates that the peer entity has restarted; and verifying that that peer entity has restarted by sending 506A, 606B towards the peer entity a request for a restart indicator of the peer entity; receiving 506B a response with an unchanged restart indicator sent by the peer entity; and determine 506C, since the first restart indicator is the same as the second restart indicator, that the peer entity has not restarted.

WO 2020/171765 A1

[Continued on next page]

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

MITIGATING DoS ATTACKS

BACKGROUND

[0001] Generally, all terms used herein are to be interpreted according to their ordinary meaning in the relevant technical field, unless a different meaning is clearly given and/or is implied from the context in which it is used. All references to a/an/the element, apparatus, component, means, step, etc. are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any methods disclosed herein do not have to be performed in the exact order disclosed, unless a step is explicitly described as following or preceding another step and/or where it is implicit that a step must follow or precede another step. Any feature of any of the embodiments disclosed herein may be applied to any other embodiment, wherever appropriate. Likewise, any advantage of any of the embodiments may apply to any other embodiments, and vice versa. Other objectives, features, and advantages of the enclosed embodiments will be apparent from the following description.

GTP-based Peer Restart Detection

[0002] The General Packet Radio Service (GPRS) Tunneling Protocol (GTP) Version 1 for Control Plane (GTPv1-C) protocol is used on the Gn/Gp interface between a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN). Details are described in Third Generation Partnership Project (3GPP) Technical Specification (TS) 29.060.

[0003] The GTP Version 2 for Control Plane (GTPv2-C) protocol is used between S4-SGSN / Mobility Management Entities (MMEs), between S4-SGSN/MME and Serving Gateway (SGW), between SGW and Packet Data Network (PDN) Gateway (PGW), between Trusted Wireless Local Area Network (WLAN) (TWAN) and PGW, and between evolved Packet Data Gateway (ePDG) and PGW. Details are described in 3GPP TS 29.274.

[0004] The GTP for User Plane (GTP-U) protocol is described in TS 29.281. It is based on GTP Version 1 (GTPv1).

[0005] In the following discussion, "GTP-C" will refer to both GTPv1-C and GTPv2-C.

[0006] The GTP-C protocol includes a mechanism by which a GTP entity can detect restarts of its peer GTP entities. The mechanism is described in 3GPP TS 23.007 chapter 18.

[0007] GTP-C messages can include a recovery Information Element (IE), in which there is a Restart Counter. The Restart Counter signaled in the GTP-C message is associated with the GTP-C entity identified by the sender's Fully Qualified Tunnel Endpoint Identifier (F-TEID) or SGSN/GGSN Internet Protocol (IP) address for control plane if present in the message; otherwise (e.g., in echo request message), the Restart Counter is associated with the GTP-C entity identified by the source IP address of the message (see, e.g., 3GPP TS 23.007 chapter 18).

[0008] A GTP-C entity should store the IP addresses to its peer GTP-C entities together with the most recently received Restart Counters for those peers. By comparing Restart Counters received in new messages from the peers with the stored Restart Counters for the same peers, it is possible to detect peer restarts. When a GTP-C entity restarts,

no Packet Data Protocol (PDP) contexts / Evolved Packet System (EPS) bearers associated with that GTP-C entity are expected to survive. Therefore, when a peer restart is detected, the standard prescribes that all sessions associated with that peer should be removed. For example:

> "When the GGSN detects a restart in an SGSN (see clause 18 "GTP-C based restart procedures") with which it has PDP context(s) activated and/or MBMS UE context(s), it shall delete all these PDP context(s) and/or MBMS UE context(s)." (3GPP TS 23.007 chapter 11.1).

The standard contains similar text for other GTP-C entities, like MME, SGW, PGW, TWAN, and ePDG (3GPP TS 23.007).

PFCP-based Peer Restart Detection

[0009] The Packet Forwarding Control Protocol (PFCP) protocol is used in Evolved Packet Core (EPC) between SGW Control Plane (SGW-C) and SGW User Plane (SGW-U) and between PGW Control Plane (PGW-C) and PGW User Plane (PGW-U). The same protocol is also used in the Fifth Generation (5G) Core Network (5GC) between the Session Management Function (SMF) and the User Plane Function (UPF) network functions. Details of the PFCP protocol are described in 3GPP TS 29.244.

[0010] The PFCP protocol uses a mechanism for detecting restarts of peer PFCP entities which is very similar to the mechanism used in GTP.

[0011] The main difference between the peer restart detection mechanisms in GTP-C and PFCP is that GTP-C uses a Restart Counter while PFCP uses a Restart Time Stamp. The Restart Counter in GTP-C is one octet. For each restart, it is incremented until it wraps around. The size of the Restart Time Stamp in PFCP is four octets. The Restart Time Stamp is set to the Coordinated Universal Time (UTC) time for the most recent restart of the PFCP entity.

SUMMARY

[0012] There currently exist certain challenge(s).

[0013] GTP-C messages can be used for Denial of Service (DoS) attacks. An attacker can, for example, spoof the IP Source Address of the User Datagram Protocol (UDP) / IP packet that carries a GTP-C message, and include a Restart Counter with a random value. The effect can be that the node that receives the message deletes all sessions that are associated with the node that has the IP address in the manipulated message.

[0014] Groupe Spéciale Mobile Association (GSMA) has reported this problem to 3GPP:

> **Denial of service on all subscribers on the same SGSN/SGW**
>
> An attacker can spoof any GTP-C message (e.g. Echo response) with increased Restart Counter and send it to the target node. The target node, since the counter has been increased, assumes a restart of the sending node and deletes all context assigned to this spoofed IP address. (C4-1900033)

[0015] The **Echo Request** message is particularly easy to manipulate. The reasons are:

- The Echo Request message does not make use of the Tunnel Endpoint Identifier (TEID) field in the GTP-C header.

- The Echo Request message contains very few IEs. The only mandatory IE is the Recovery IE, which contains the Restart Counter, and this IE can cause severe damage when misused.
- The Restart Counter is associated with the IP Source Address in the IP/UDP packet that carries the Echo Request message, and that address can easily be spoofed.

[0016] **Other GTP-C messages** can also be spoofed, especially those that are addressed to TEID=0, for example:

- "The Create PDP Context Request message and the Create MBMS Context Request message for a given MS sent to a specific GGSN shall have the Tunnel Endpoint Identifier set to all zeroes, if the SGSN has not been assigned a Tunnel Endpoint Identifier Control Plane by the GGSN." (TS 29.060 ch. 8.2)
- "Create Session Request message on S2a/S2b/S5/S8" (TS 29.274 ch. 5.5.2)
- "Create Session Request message on S4/S11, if for a given UE, the SGSN/MME has not yet obtained the Control TEID of the SGW" (TS 29.274 ch. 5.5.2)

[0017] There are good reasons to be extra careful with signaling over **roaming interfaces** (Gn and S8). Unfortunately, there is no way to detect that Echo Request/Response messages are sent over roaming interfaces (unless the roaming interfaces are separated from the interfaces used within the Public Land Mobile Network (PLMN), but that is not supported by the standard).

[0018] The only nodes that are mentioned in the paper from GSMA are SGSN and SGW. However, since Echo Request is pointed out as especially suited for DoS attacks, the problem is relevant for all GTP-based interfaces on which Echo Request/Response with a Recovery IE can be sent. Those interfaces are: Gn/Gp, S5/S8, S11, S4, S2a, and S2b. The corresponding nodes are SGSN, GGSN, PGW, SGW, S4-SGSN, MME, TWAN, and ePDG. Corresponding interfaces in the 5G system are at least the N3 and N4 interfaces with corresponding nodes/functions R(AN), SMF and UPF.

[0019] If a received Echo Request message is unreliable, it means that the Supported Node Features IE in the same message are equally unreliable. The possible effects of this problem are less severe compared with the damage that can be caused by a malicious use of an incremented Restart Counter.

[0020] Certain aspects of the present disclosure and their embodiments may provide solutions to the aforementioned or other challenges.

[0021] Systems and methods are disclosed herein that provide a mechanism to verify if a peer GTP entity or a peer PFCP entity has restarted, in a mobile network, e.g. EPS, 5GC and GPRS network. In some embodiments, when a GTP-C/PFCP entity receives a changed restart indicator in the GTP-C/PFCP message from a peer entity (i.e., an incremented Restart Counter included in a GTP-C message from the peer entity or a new Restart Time Stamp included in a PFCP message) (for example Command messages and Request messages that not have been triggered by a Command message), e.g. Echo Request, the GTP-C/PFCP entity does not take immediate action(s) and delete all sessions (PDP Contexts, PDN Connections, or PFCP Sessions) associated with the IP address of the peer entity which is included in the message. Instead, the GTP-C/PFCP entity marks these sessions with a flag or other indicator indicating that these sessions are associated with a **suspected** restarted peer entity.

[0022] Before the GTP-C/PFCP entity takes further action, e.g. deletes those said sessions, the GTP-C/PFCP verifies whether the peer entity has a real restart by taking one or more of the following measures:

1. The GTP-C/ PFCP entity sends one or more Echo Request messages to the peer entity (thus receiving corresponding Echo response message(s)), if the changed indicator (e.g., the incremented restart counter or changed restart time stamp) was included in an initial message, e.g. Command messages, and Request messages that not have been triggered by a Command message;
2. The GTP-C/PFCP entity randomly selects a number of existing sessions (PDN Connection/PDP Context/PFCP Session) which are associated with the peer entity and sends a Session-related GTP-C request message (thus receiving corresponding GTP-C response message(s)) to modify these sessions for every selected PDN connections/PDP context associated with the peer GTP entity, e.g. a modify bearer request message including a User Location Information, or an Update Bearer Request message including an Indication Flags IE with the Retrieve Location Indication set to 1 to retrieve the current UE location. Similarly for PFCP a, e.g., PFCP Session Modification Request or a PFCP Session Report request message may be used. If the peer entity has had a real restart, all these modification requests should be rejected, and the response message should be sent towards TEID=0 or SEID=0 with the rejection cause "Context not found" (or "Non-existent" for GTPv1) and the restart counter if included in these response message should be the same as received earlier; NOTE: This alternative may be used by a SGSN, GGSN, PGW (for GTP-C sessions), or a control plane function and user plane function (for PFCP session).
3. The GTP-C/PFCP entity randomly selects a number of sessions which have ongoing session related signaling towards the peer entity for requesting a new session, or for modifying an existing session. The GTP-C/PFCP entity **monitors** the corresponding response messages. NOTE: This alternative may e.g. be used by a SGSN, GGSN, SGW, PGW (for GTP-C sessions), or a control plane function and user plane function (for PFCP session). If the peer entity has had a real restart:
    a. the creation of a session should be accepted/rejected by other reason per existing specification, and the restart indicator (e.g., the restart counter for GTP-C or the restart time stamp for PFCP) if included in these response message should be the same as received earlier; and
    b. all modification requests should be rejected and the response messages should be sent towards TEID=0 or SEID=0 with the rejection cause "Context not found" (or "Non-existent" for GTPv1), and the indicator (e.g., the restart counter for GTP-C or the restart time stamp for PFCP) if included in these response message should be the same as received earlier;

[0023] Measures to delete the sessions should then be taken place only after the restart is verified.

[0024] There are, proposed herein, various embodiments which address one or more of the issues disclosed herein.

[0025] One embodiment is directed to a method performed by GTP-C or PFCP entity, the method comprising: receiving, from a peer entity, a first message comprising a first restart indicator for the peer entity; receiving a second

message comprising a changed restart indicator for the peer entity that indicates that the peer entity has restarted; and verifying whether the peer entity has restarted by sending towards the peer entity a request for a restart indicator of the peer entity; receiving a response with an unchanged restart indicator sent by the peer entity; and determine, since the first restart indicator is the same as the second restart indicator, that the peer entity has not restarted.

[0026] Another embodiment is directed to *** a network node for implementing a GTP-C or PFCP entity, the network node comprising: a network interface; and processing circuitry associated with the network interface, the processing circuitry operable to cause the network node to perform the method embodiment above.

[0027] Certain embodiments may provide one or more of the following technical advantage(s). Embodiments of the solution proposed herein will significantly reduce the risk that sessions are unintentionally deleted due to misinterpretation of received spoofed GTP-C messages due to the following reasons:

- the response message must contain the same 3 bytes sequence number as included in the request message;
- sending session related messages for randomly selected affected session and expecting receiving response at TEID=0, and a specific cause increase the complexity to be spoofed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] The accompanying drawings, which are included to provide a further understanding of the disclosure and are incorporated in a constitute a part of this application, illustrate certain non-limiting embodiments of inventive concepts. In the drawings:

Figure 1 illustrates one example of a cellular communications network 100 in which embodiments of the present disclosure may be implemented;

Figure 2 illustrates one example of the cellular communications network 100;

Figure 3 illustrates a wireless communication system represented as a 5G network architecture;

Figure 4 illustrates a 5G network architecture using service-based interfaces;

Figure 5 illustrates a procedure for avoiding a GTP-C/PFCP DoS attack in accordance with embodiments of the present disclosure;

Figure 6 illustrates a procedure for avoiding a GTP-C DoS attack in accordance with embodiments of the present disclosure;

Figure 7 is a schematic block diagram of a network node 700 according to some embodiments of the present disclosure;

Figure 8 is a schematic block diagram that illustrates a virtualized embodiment of the network node 700 according to some embodiments of the present disclosure;

Figure 9 is a schematic block diagram of the network node 700 according to some other embodiments of the present disclosure;

Figure 10 is a schematic block diagram of a UE according to some embodiments of the present disclosure;

Figure 11 is a schematic block diagram of the UE according to some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0029] Some of the embodiments contemplated herein will now be described more fully with reference to the accompanying drawings. Other embodiments, however, are contained within the scope of the subject matter disclosed herein, the disclosed subject matter should not be construed as limited to only the embodiments set forth herein; rather, these embodiments are provided by way of example to convey the scope of the subject matter to those skilled in the art.

[0030] **Radio Node:** As used herein, a "radio node" is either a radio access node or a wireless device.

[0031] **Radio Access Node:** As used herein, a "radio access node" or "radio network node" is any node in a radio access network of a cellular communications network that operates to wirelessly transmit and/or receive signals. Some examples of a radio access node include, but are not limited to, a base station (e.g., a New Radio (NR) base station (gNB) in a 3GPP 5G NR network or an enhanced or evolved Node B (eNB) in a 3GPP Long Term Evolution (LTE) network), a high-power or macro base station, a low-power base station (e.g., a micro base station, a pico base station, a home eNB, or the like), and a relay node.

[0032] **Core Network Entity:** As used herein, a "core network entity" is any type of entity in a core network. Some examples of a core network entity include, e.g., a MME, a PGW, a Service Capability Exposure Function (SCEF), or the like in an EPC. Some other examples of a core network entity include, e.g., an Access and Mobility Management Function (AMF), a Network Slice Selection Function (NSSF), an Authentication Server Function (AUSF), a Unified Data Management (UDM), a SMF, a Policy Control Function (PCF), an Application Function (AF), a Network Exposure Function (NEF), a UPF, or the like in a 5GC. A core network entity may be implemented as a physical network node (e.g., including hardware or a combination of hardware and software) or implemented as a functional entity (e.g., as software) that is, e.g., implemented on a physical network node or distributed across two or more physical network nodes.

[0033] **Wireless Device:** As used herein, a "wireless device" is any type of device that has access to (i.e., is served by) a cellular communications network by wirelessly transmitting and/or receiving signals to a radio access node(s). Some examples of a wireless device include, but are not limited to, a UE in a 3GPP network and a Machine Type Communication (MTC) device.

[0034] **Network Node:** As used herein, a "network node" is any node that is either part of the radio access network or the core network of a cellular communications network/system.

[0035] Note that the description given herein focuses on a 3GPP cellular communications system and, as such, 3GPP terminology or terminology similar to 3GPP terminology is oftentimes used. However, the concepts disclosed herein are not limited to a 3GPP system.

[0036] Note that, in the description herein, reference may be made to the term "cell"; however, particularly with respect to 5G NR concepts, beams may be used instead of cells and, as such, it is important to note that the concepts described herein are equally applicable to both cells and beams.

[0037] Systems and methods are disclosed herein that provide a mechanism to verify if a peer GTP entity or a peer PFCP entity has restarted, in a mobile network, e.g. EPS, 5GC and GPRS network.

Figure 1

[0038] In this regard, **Figure 1** illustrates one example of a cellular communications network 100 in which embodiments of the present disclosure may be implemented. In the embodiments described herein, the cellular communications network 100 is a EPS including an LTE radio access network and EPC, 5G System (5GS) including a 5G radio access network (e.g., a NR radio access network) and a 5GC, a GPRS system, or the like. In this example, the cellular communications network 100 includes base stations 102-1 and 102-2, which in LTE are referred to as eNBs and in 5G NR are referred to as gNBs, controlling corresponding macro cells 104-1 and 104-2. The base stations 102-1 and 102-2 are generally referred to herein collectively as base stations 102 and individually as base station 102. Likewise, the macro cells 104-1 and 104-2 are generally referred to herein collectively as macro cells 104 and individually as macro cell 104. The cellular communications network 100 may also include a number of low power nodes 106-1 through 106-4 controlling corresponding small cells 108-1 through 108-4. The low power nodes 106-1 through 106-4 can be small base stations (such as pico or femto base stations) or Remote Radio Heads (RRHs), or the like. Notably, while not illustrated, one or more of the small cells 108-1 through 108-4 may alternatively be provided by the base stations 102. The low power nodes 106-1 through 106-4 are generally referred to herein collectively as low power nodes 106 and individually as low power node 106. Likewise, the small cells 108-1 through 108-4 are generally referred to herein collectively as small cells 108 and individually as small cell 108. The base stations 102 (and optionally the low power nodes 106) are connected to a core network 110. For a 5GS, the core network 110 is a 5GC.

[0039] The base stations 102 and the low power nodes 106 provide service to wireless devices 112-1 through 112-5 in the corresponding cells 104 and 108. The wireless devices 112-1 through 112-5 are generally referred to herein collectively as wireless devices 112 and individually as wireless device 112. The wireless devices 112 are also sometimes referred to herein as User Equipment devices (UEs).

Figure 2

[0040] **Figure 2** illustrates one example of the cellular communications network 100 in which the cellular communications network 100 is a 3GPP LTE network. In particular, the exemplifying core network 110 is an EPC, which includes various core network nodes such as, for example, a SGW 200, a P-GW 202, a MME 204, a Home Subscriber Service (HSS) 206, and a SCEF 208, as will be appreciated by one of skill in the art.

Figure 3

[0041] **Figure 3** illustrates a wireless communication system represented as a 5G network architecture composed of core Network Functions (NFs), where interaction between any two NFs is represented by a point-to-point reference point/interface. Figure 3 can be viewed as one particular implementation of the system 100 of Figure 1.

[0042] Seen from the access side the 5G network architecture shown in Figure 3 comprises a plurality of UEs connected to either a Radio Access Network (RAN) or an Access Network (AN) as well as an AMF. Typically, the R(AN) comprises base stations, e.g. such as eNBs or gNBs or similar. Seen from the core network side, the 5G core NFs shown in Figure 3 include a NSSF, an AUSF, a UDM, an AMF, a SMF, a PCF, and an AF.

[0043] Reference point representations of the 5G network architecture are used to develop detailed call flows in the normative standardization. The N1 reference point is defined to carry signaling between the UE and AMF. The reference points for connecting between the AN and AMF and between the AN and UPF are defined as N2 and N3, respectively. There is a reference point, N11, between the AMF and SMF, which implies that the SMF is at least partly controlled by the AMF. N4 is used by the SMF and UPF so that the UPF can be set using the control signal generated by the SMF, and the UPF can report its state to the SMF. N9 is the reference point for the connection between different UPFs, and N14 is the reference point connecting between different AMFs, respectively. N15 and N7 are defined since the PCF applies policy to the AMF and SMP, respectively. N12 is required for the AMF to perform authentication of the UE. N8 and N10 are defined because the subscription data of the UE is required for the AMF and SMF.

[0044] The 5GC aims at separating user plane and control plane. The user plane carries user traffic while the control plane carries signaling in the network. In Figure 3, the UPF is in the user plane and all other NFs, i.e., the AMF, SMF, PCF, AF, AUSF, and UDM, are in the control plane. Separating the user and control planes guarantees each plane resource to be scaled independently. It also allows UPFs to be deployed separately from control plane functions in a distributed fashion. In this architecture, UPFs may be deployed very close to UEs to shorten the Round Trip Time (RTT) between UEs and data network for some applications requiring low latency.

[0045] The core 5G network architecture is composed of modularized functions. For example, the AMF and SMF are independent functions in the control plane. Separated AMF and SMF allow independent evolution and scaling. Other control plane functions like the PCF and AUSF can be separated as shown in Figure 3. Modularized function design enables the 5G core network to support various services flexibly.

[0046] Each NF interacts with another NF directly. It is possible to use intermediate functions to route messages from one NF to another NF. In the control plane, a set of interactions between two NFs is defined as service so that its reuse is possible. This service enables support for modularity. The user plane supports interactions such as forwarding operations between different UPFs.

Figure 4

[0047] **Figure 4** illustrates a 5G network architecture using service-based interfaces between the NFs in the control plane, instead of the point-to-point reference points/interfaces used in the 5G network architecture of Figure 3. However,

the NFs described above with reference to Figure 3 correspond to the NFs shown in Figure 4. The service(s) etc. that a NF provides to other authorized NFs can be exposed to the authorized NFs through the service-based interface. In Figure 4 the service based interfaces are indicated by the letter "N" followed by the name of the NF, e.g. Namf for the service based interface of the AMF and Nsmf for the service based interface of the SMF etc. The NEF and the Network Repository Function (NRF) in Figure 4 are not shown in Figure 3 discussed above. However, it should be clarified that all NFs depicted in Figure 3 can interact with the NEF and the NRF of Figure 4 as necessary, though not explicitly indicated in Figure 3.

[0048] Some properties of the NFs shown in Figures 3 and 4 may be described in the following manner. The AMF provides UE-based authentication, authorization, mobility management, etc. A UE even using multiple access technologies is basically connected to a single AMF because the AMF is independent of the access technologies. The SMF is responsible for session management and allocates IP addresses to UEs. It also selects and controls the UPF for data transfer. If a UE has multiple sessions, different SMFs may be allocated to each session to manage them individually and possibly provide different functionalities per session. The AF provides information on the packet flow to the PCF responsible for policy control in order to support Quality of Service (QoS). Based on the information, the PCF determines policies about mobility and session management to make the AMF and SMF operate properly. The AUSF supports authentication function for UEs or similar and thus stores data for authentication of UEs or similar while the UDM stores subscription data of the UE. The Data Network (DN), not part of the 5G core network, provides Internet access or operator services and similar.

[0049] An NF may be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualized function instantiated on an appropriate platform, e.g., a cloud infrastructure.

[0050] Similar system architectures exist for other types of cellular communications networks such as, e.g., a GPRS network (e.g., a Global System for Mobile Communications (GSM) network). Since these architectures are well known, they are not repeated here.

[0051] Systems and methods are disclosed herein that provide a mechanism to verify if a peer GTP entity or a peer PFCP entity has restarted, in a mobile network, e.g. EPS, 5GC and GPRS network. As used herein, a "GTP entity" or "GTP-C" entity is any entity that communicates in accordance with a GTP or GTP-C protocol. Likewise, a "PFCP entity" is any entity that communicates in accordance with the PFCP protocol. Note that the term "GTP/PFCP entity" or "GTP-C/PFCP entity" is used herein to generally refer to a GTP/GTP-C entity or a PFCP entity.

[0052] Systems and methods are disclosed herein that provide a mechanism to verify if a peer GTP entity or a peer PFCP entity has restarted, in a mobile network, e.g. EPS, 5GC and GPRS network. In some embodiments, when a GTP-C/PFCP entity receives a changed restart indicator (i.e., an incremented Restart Counter included in a GTP-C message from the peer entity or a new Restart Time Stamp included in a PFCP message) in the GTP-C/PFCP message (e.g., a Command message or a Request message that has not been triggered by a Command message or, e.g., an Echo Request) from a peer entity, the GTP-C/PFCP entity does not take immediate action(s) and delete all sessions (PDP

Contexts, PDN Connections, or PFCP Sessions) associated with the IP address of the peer entity which is included in the message. Instead, the GTP-C/PFCP entity marks these sessions with a flag or other indicator indicating that these sessions are associated with a **suspected** restarted peer entity.

[0053] Before the GTP-C/PFCP entity takes further action, e.g. deletes those said sessions, the GTP-C/PFCP verifies whether the peer entity has a real restart by taking one or more of the following measures:

1. The GTP-C/ PFCP entity sends one or more Echo Request messages to the peer entity (thus receiving corresponding Echo response message(s)), if the changed indicator (e.g., the incremented restart counter or changed restart time stamp) was included in an initial message, e.g. Command messages, and Request messages that not have been triggered by a Command message;
2. The GTP-C/PFCP entity randomly selects a number of existing sessions (PDN Connection/PDP Context/PFCP Session) which are associated with the peer entity and sends a Session-related GTP-C request message (thus receiving corresponding GTP-C response message(s)) to modify these sessions for every selected PDN connections/PDP context associated with the peer GTP entity, e.g. a modify bearer request message including a User Location Information, or an Update Bearer Request message including an Indication Flags IE with the Retrieve Location Indication set to 1 to retrieve the current UE location. Similarly for PFCP, a, e.g., PFCP Session Modification Request or a PFCP Session Report request message may be used. If the peer entity has had a real restart, all these modification requests should be rejected, and the response message should be sent towards TEID=0 or SEID=0 with the rejection cause "Context not found" (or "Non-existent" for GTPv1) and the restart counter if included in these response message should be the same as received earlier; NOTE: This alternative may be used by a SGSN, GGSN, PGW (for GTP-C sessions), or a control plane function and user plane function (for PFCP session).
3. The GTP-C/PFCP entity randomly selects a number of sessions which have ongoing session related signaling towards the peer entity for requesting a new session, or for modifying an existing session. The GTP-C/PFCP entity **monitors** the corresponding response messages. NOTE: This alternative may be used by a SGSN, GGSN, SGW, PGW (for GTP-C sessions), or a control plane function and user plane function (for PFCP session). If the peer entity has had a real restart:
    a. the creation of a session should be accepted/rejected by other reason per existing specification, and the restart indicator (e.g., the restart counter for GTP-C or the restart time stamp for PFCP) if included in these response message should be the same as received earlier; and
    b. all modification requests should be rejected and the response messages should be sent towards TEID=0 or SEID=0 with the rejection cause "Context not found" (or "Non-existent" for GTPv1), and the indicator (e.g., the restart counter for GTP-C or the restart time stamp for PFCP) if included in these response message should be the same as received earlier.

[0054] In other orders, the GTP-C/PFCP entity refrains from performing action(s) that are to be performed upon restart of the peer entity while the GTP-C/PFCP verifies whether the peer entity had a real restart. Measures to delete the sessions should then be taken place only after the restart (i.e., a real restart) is verified.

Figure 5

[0055] **Figure 5** illustrates a procedure for avoiding a GTP-C/PFCP DoS attack in accordance with embodiments of the present disclosure. As illustrated, a peer entity (denoted as "A" in Figure 5) sends a message to a GTP-C/PFCP entity (denoted as "B" in Figure 5), where the message includes a restart indicator (e.g., a restart counter k for GTP-C or a restart time stamp s for PFCP) (step 500). In this example, an attacking entity makes an attack attempt by sending a request message with a spoofed source address of the peer entity ("A") and a changed restart indicator (e.g., an incremented restart counter k+1 (or k+n, where n is an integer) for GTP-C or a new restart time stamp s' for PFCP) (step 502). Upon receiving the request message including the changed restart indicator, rather than immediately deleting all sessions associated with the peer entity (A) (e.g., associated with the IP address of the peer entity A), the GTP-C/PFCP entity (B) identifies these sessions as being associated with a suspected, or possibly, restarted peer entity. Optionally, the peer entity sends a response to peer entity A (step 504).

[0056] The GTP-C/PFCP entity then verifies whether the peer entity A has restarted (step 506). This verification can be performed by the GTP-C/PFCP entity using any one or any combination of one or more of the mechanisms described above (and denoted as mechanisms 1, 2, and 3 above). However, in this particular example, the GTP-C/PFCP entity sends a request for a restart indicator of the peer entity to the peer entity (step 506A), e.g. an Echo Request message or a GTP-C request message. The peer entity A sends a response with the (unchanged) restart indicator (e.g., the restart counter k for GTP-C or the restart time stamp s for PFCP) (step 506B), e.g. in an Echo Response message or a GTP-C response message. The GTP-C/PFCP entity then verifies that the peer entity has not restarted by comparing the restart indicator included in the response in step 506B with the original restart indicator included in the message in step 500 (step 506C). Since the restart indicator in step 506B is the same as that in step 500, the GTP-C/PFCP entity determines that the peer entity has not restarted and, as such, maintains the sessions with the peer entity A (i.e., does not delete all sessions with the peer entity A and keeps the original restart indicator in memory as the restart indicator of the peer entity A). In this manner, the DoS attack attempt can be avoided.

Figure 6

[0057] **Figure 6** illustrates a procedure for avoiding a GTP-C DoS attack in accordance with embodiments of the present disclosure. In this example, a PGW sends GTP-C a message to a SGW with a restart counter k (step 600). An attacker (i.e., an attacking entity) sends a request to the SGW with a spoofed source address of the PGW and an incremented restart counter k+1 (step 602) or even k+n, where n is an integer. Upon receiving the request message including the incremented restart counter k+1 or even or k+n, rather than immediately deleting all sessions associated

with the PGW (e.g., associated with the IP address of the PGW), the SGW identifies these sessions as being associated with a suspected, or possibly, restarted peer entity. Optionally, the SGW sends a response to PGW (step 604).

[0058] The SGW then verifies whether the PGW has restarted (step 606). This verification can be performed by the SGW entity using any one or any combination of one or more of the mechanisms described above (and denoted as mechanisms 1, 2, and 3 above). However, in this particular example, the SGW receives a session-related request from an MME or S4-SGSN (step 606A), sends the session-related request for a restart counter to the PGW (step 606B), receives a response from the PGW with the (unchanged) restart counter k (step 606C), and sends a response to the MME / S4-SGSN with a restart counter of the SGW (step 606D). The SGW verifies that the PGW has not restarted by comparing the restart counter k included in the response in step 606C with the original restart counter k included in the message in step 600 (step 606E). Since the restart counter in step 606C is the same as that in step 600, the SGW determines that the PGW has not restarted and, as such, maintains the sessions with the PGW (i.e., does not delete all sessions with the PGW and keeps the restart counter k in memory as the restart counter of the PGW). In this manner, the DoS attack attempt can be avoided.

Figure 7

[0059] **Figure 7** is a schematic block diagram of a network node 700 according to some embodiments of the present disclosure. The network node 700 may be, for example, a core network node or a network node implementing a core network entity (e.g., a SMF, UPF, NEF, or the like) and more specifically implementing a GTP-C or PFCP entity as described herein. As illustrated, the network node 700 includes one or more processors 704 (e.g., Central Processing Units (CPUs), Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs), and/or the like), memory 706, and a network interface 708. The one or more processors 704 are also referred to herein as processing circuitry. The one or more processors 704 operate to cause the network node 700 to provide one or more functions of a GTP-C or PFCP entity as described herein. In some embodiments, the function(s) are implemented in software that is stored, e.g., in the memory 706 and executed by the one or more processors 704.

Figure 8

[0060] **Figure 8** is a schematic block diagram that illustrates a virtualized embodiment of the network node 700 according to some embodiments of the present disclosure. This discussion is equally applicable to other types of network nodes. Further, other types of network nodes may have similar virtualized architectures.

[0061] As used herein, a "virtualized" network node is an implementation of the network node 700 in which at least a portion of the functionality of the network node 700 is implemented as a virtual component(s) (e.g., via a virtual machine(s) executing on a physical processing node(s) in a network(s)). As illustrated, in this example, the network node 700 includes one or more processing nodes 800 coupled to or included as part of a network(s) 802. Each processing node 800 includes one or more processors 804 (e.g., CPUs, ASICs, FPGAs, and/or the like), memory 806, and a network interface 808.

[0062] In this example, functions 810 of the network node 700 described herein (e.g., the functions of a GTP-C or PFCP entity) are implemented at the one or more processing nodes 800 in any desired manner. In some particular embodiments, some or all of the functions 810 of the network node 700 described herein are implemented as virtual components executed by one or more virtual machines implemented in a virtual environment(s) hosted by the processing node(s) 800.

[0063] In some embodiments, a computer program including instructions which, when executed by at least one processor, causes the at least one processor to carry out the functionality of core network entity (e.g., GTP-C or PFCP entity) as described herein is provided. In some embodiments, a carrier comprising the aforementioned computer program product is provided. The carrier is one of an electronic signal, an optical signal, a radio signal, or a computer readable storage medium (e.g., a non-transitory computer readable medium such as memory).

Figure 9

[0064] **Figure 9** is a schematic block diagram of the network node 700 according to some other embodiments of the present disclosure. The network node 700 includes one or more modules 900, each of which is implemented in software. The module(s) 900 provide the functionality of a GTP-C or PFCP entity as described herein.

Figure 10

[0065] **Figure 10** is a schematic block diagram of a UE 1000 according to some embodiments of the present disclosure. As illustrated, the UE 1000 includes one or more processors 1002 (e.g., CPUs, ASICs, FPGAs, and/or the like), memory 1004, and one or more transceivers 1006 each including one or more transmitters 1008 and one or more receivers 1010 coupled to one or more antennas 1012. The transceiver(s) 1006 includes radio-front end circuitry connected to the antenna(s) 1012 that is configured to condition signals communicated between the antenna(s) 1012 and the processor(s) 1002, as will be appreciated by on of ordinary skill in the art. The processors 1002 are also referred to herein as processing circuitry. The transceivers 1006 are also referred to herein as radio circuitry. In some embodiments, the functionality of the UE 1000 described above may be fully or partially implemented in software that is, e.g., stored in the memory 1004 and executed by the processor(s) 1002. Note that the UE 1000 may include additional components not illustrated in Figure 10 such as, e.g., one or more user interface components (e.g., an input/output interface including a display, buttons, a touch screen, a microphone, a speaker(s), and/or the like and/or any other components for allowing input of information into the UE 1000 and/or allowing output of information from the UE 1000), a power supply (e.g., a battery and associated power circuitry), etc.

[0066] In some embodiments, a computer program including instructions which, when executed by at least one processor, causes the at least one processor to carry out the functionality of the UE 1000 according to any of the embodiments described herein is provided. In some embodiments, a carrier comprising the aforementioned computer program product is provided. The carrier is one of an electronic signal, an optical signal, a radio signal, or a computer readable storage medium (e.g., a non-transitory computer readable medium such as memory).

Figure 11

[0067] **Figure 11** is a schematic block diagram of the UE 1000 according to some other embodiments of the present disclosure. The UE 1000 includes one or more modules 1100, each of which is implemented in software. The module(s) 1100 provide the functionality of the UE 1000 described herein.

[0068] Any appropriate steps, methods, features, functions, or benefits disclosed herein may be performed through one or more functional units or modules of one or more virtual apparatuses. Each virtual apparatus may comprise a number of these functional units. These functional units may be implemented via processing circuitry, which may include one or more microprocessor or microcontrollers, as well as other digital hardware, which may include Digital Signal Processor (DSPs), special-purpose digital logic, and the like. The processing circuitry may be configured to execute program code stored in memory, which may include one or several types of memory such as Read Only Memory (ROM), Random Access Memory (RAM), 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 some implementations, the processing circuitry may be used to cause the respective functional unit to perform corresponding functions according one or more embodiments of the present disclosure.

[0069] While processes in the figures may show a particular order of operations performed by certain embodiments of the present disclosure, it should be understood that such order is exemplary (e.g., alternative embodiments may perform the operations in a different order, combine certain operations, overlap certain operations, etc.).

Some embodiments describe above may be summarized in the following manner:

1. A method performed by GTP-C or PFCP entity (B, 200), the method comprising:

receiving (500, 600), from a peer entity (A, 202), a first message comprising a first restart indicator for the peer entity;

receiving (502, 602) a second message comprising a changed restart indicator for the peer entity that indicates that the peer entity has restarted; and

verifying whether the peer entity has restarted by

sending (506A, 606B) towards the peer entity a request for a restart indicator of the peer entity;

receiving (506B) a response with an unchanged restart indicator sent by the peer entity; and

determine (506C), since the first restart indicator is the same as the second restart indicator, that the peer entity has not restarted.

2. The method of embodiment 1 wherein, if a result of verifying that the peer entity has restarted is that the peer entity has not restarted, refraining from performing one or more actions that would have been performed if the peer entity had restarted.

3. The method of embodiment 2, wherein the one or more actions that would have been performed if the peer entity had restarted comprise deleting all sessions associated with the peer entity.

4. The method of any one of embodiment 1-3, wherein the request is an Echo Request and the response is an Echo Response, or wherein the request is a GTP-C request and the response is a GTP-C response.

5. The method of any one of embodiment 1-4 wherein the GTP-C entity is a GGSN, MME, SGW, PGW, TWAN, ePDG or UPF.

6. The method of embodiment 1-5, wherein the PFCP entity is a SGW-C, SGW-U, PGW-C, PGW-U, SMF, or UPF.

7. The method of any one of embodiment 1-6 wherein the restart indicator is a restart counter.

8. The method of any one of embodiment 1-7 wherein the restart indicator is a restart time stamp.

9. A GTP-C or PFCP entity adapted to perform the method of any one of embodiments 1 to 8.

10. A network node for implementing a GTP-C or PFCP entity, the network node comprising:
a network interface; and
processing circuitry associated with the network interface, the processing circuitry operable to cause the network node to perform the method of any one of embodiments 1 to 8.

<u>Some other embodiments describe above may be summarized in the following manner:</u>

1. A method performed by GTP-C or PFCP entity, the method comprising:
receiving, from a peer entity, a first message comprising a restart indicator for the peer entity;
receiving a second message comprising a changed restart indicator for the peer entity that indicates that the peer entity has restarted; and
verifying that that peer entity has restarted.

2. The method of embodiment 1 wherein, if a result of verifying that the peer entity has restarted is that the peer entity has not restarted, refraining from performing one or more actions that would have been performed if the peer entity had restarted.

3. The method of embodiment 2 wherein the one or more actions that would have been performed if the peer entity had restarted comprise deleting all sessions associated with the peer entity.

4. The method of embodiment 1 wherein, if a result of verifying that the peer entity has restarted is that the peer entity has restarted, performing one or more actions that are to be performed upon restart of the peer entity.

5. The method of embodiment 4 wherein the one or more actions that are to be performed upon restart of the peer entity comprise deleting all sessions associated with the peer entity.

6. The method of any one of embodiments 1 to 5 further comprising, upon receiving the second message comprising the changed restart indicator for the peer entity, refraining from performing one or more actions that are to be performed upon restart of the peer entity while verifying that the peer entity has restarted.

7. The method of any one of embodiments 1 to 6 wherein the GTP-C or PFCP entity is a GTP-C entity.

8. The method of embodiment 7 wherein the GTP-C entity is a GGSN, MME, SGW, PGW, TWAN, or ePDG.

9. The method of embodiment 7 or 8 wherein the restart indicator is a restart counter.

10. The method of any one of embodiments 1 to 6 wherein the GTP-C or PFCP entity is a PFCP entity.

11. The method of embodiment 10 wherein the PFCP entity is a SGW-C, SGW-U, PGW-C, PGW-U, SMF, or UPF.

12. The method of embodiment 10 or 11 wherein the restart indicator is a restart time stamp.

13. A GTP-C or PFCP entity adapted to perform the method of any one of embodiments 1 to 12.

14. A network node for implementing a GTP-C or PFCP entity, the network node comprising:
a network interface; and
processing circuitry associated with the network interface, the processing circuitry operable to cause the network node to perform the method of any one of embodiments 1 to 12.

Abbreviations

At least some of the following abbreviations may be used in this disclosure. If there is an inconsistency between abbreviations, preference should be given to how it is used above. If listed multiple times below, the first listing should be preferred over any subsequent listing(s).

- AF Application Function
- AMF Access and Mobility Management Function
- AN Access Network
- AUSF Authentication Server Function
- DN Data Network
- GGSN Gateway General Packet Radio Service Support Node
- GTP General Packet Radio Service Tunneling Protocol
- GTP-C General Packet Radio Service Tunneling Protocol Version 1 for Control Plane and General Packet Radio Service Tunneling Protocol Version 2 for Control Plane
- GTP-U General Packet Radio Service Tunneling Protocol for User Plane
- GTPv1 General Packet Radio Service Tunneling Protocol Version 1
- HSS Home Subscriber Server
- IE Information Element
- IP Internet Protocol
- MME Mobility Management Entity
- NEF Network Exposure Function
- NF Network Function
- NRF Network Repository Function
- NSSF Network Slice Selection Function
- PCF Policy Control Function
- PDN Packet Data Network
- PFCP Packet Forwarding Control Protocol
- PGW Packet Data Network Gateway
- PGW-C Packet Data Network Gateway Control Plane
- PGW-U Packet Data Network Gateway User Plane
- SCEF Service Capability Exposure Function
- SGSN Serving General Packet Radio Service Support Node
- SGW Serving Gateway
- SGW-C Serving Gateway Control Plane
- SGW-U Serving Gateway User Plane
- SMF Session Management Function

- TS Technical Specification
- TWAN Trusted Wireless Local Area Network
- UDM Unified Data Management
- UDP User Datagram Protocol
- UE User Equipment
- UPF User Plane Function

CLAIMS

1. A method performed by GTP-C or PFCP entity (B, 200), the method comprising:

receiving (500, 600), from a peer entity (A, 202), a first message comprising a first restart indicator for the peer entity;

receiving (502, 602) a second message comprising a changed restart indicator for the peer entity that indicates that the peer entity has restarted; and

verifying whether the peer entity has restarted by

sending (506A, 606B) towards the peer entity a request for a restart indicator of the peer entity;

receiving (506B) a response with an unchanged restart indicator sent by the peer entity; and

determine (506C), since the first restart indicator is the same as the second restart indicator, that the peer entity has not restarted.

2. The method of claim 1 wherein, if a result of verifying that the peer entity has restarted is that the peer entity has not restarted, refraining from performing one or more actions that would have been performed if the peer entity had restarted.

3. The method of claim 2, wherein the one or more actions that would have been performed if the peer entity had restarted comprise deleting all sessions associated with the peer entity.

4. The method of any one of claim 1-3, wherein the request is an Echo Request and the response is an Echo Response, or wherein the request is a GTP-C request and the response is a GTP-C response.

5. The method of any one of claim 1-4, wherein the GTP-C entity is a GGSN, MME, SGW, PGW, TWAN, ePDG or UPF.

6. The method of claim 1-5, wherein the PFCP entity is a SGW-C, SGW-U, PGW-C, PGW-U, SMF, or UPF.

7. The method of any one of claim 1-6, wherein the restart indicator is a restart counter.

8. The method of any one of claim 1-7, wherein the restart indicator is a restart time stamp.

9. A GTP-C or PFCP entity adapted to perform the method of any one of claim 1-8.

10. A network node for implementing a GTP-C or PFCP entity, the network node comprising:

a network interface; and

processing circuitry associated with the network interface, the processing circuitry operable to cause the network node to perform the method of any one of claim 1-8.

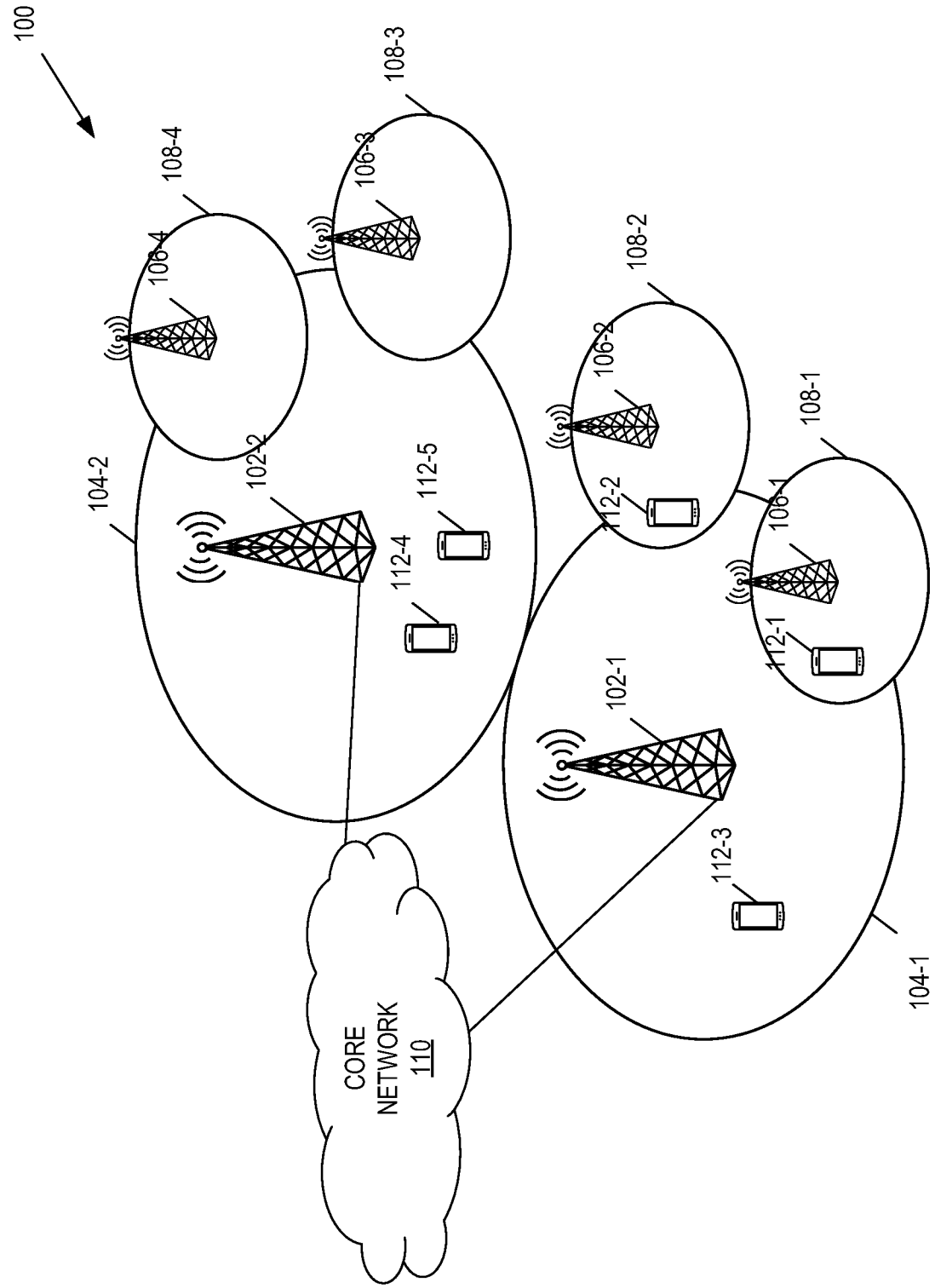
100
108-3
108-4
106-3
106-4
108-2
106-2
108-1
102-2
112-5
104-2
112-2
106-1
112-4
102-1
112-1
112-3
CORE
NETWORK
110
104-1

FIG. 1

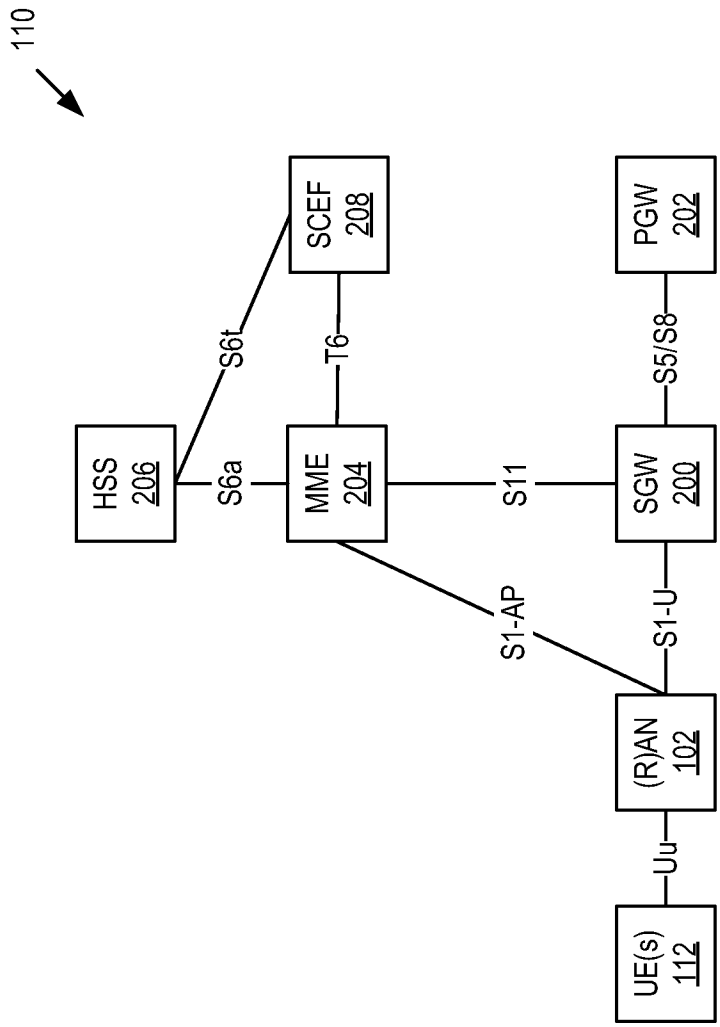
110
HSS 206
S6a
MME 204
S6t
SCEF 208
T6
S11
SGW 200
PGW 202
S5/S8
S1-AP
S1-U
(R)AN 102
Uu
UE(s) 112

FIG. 2

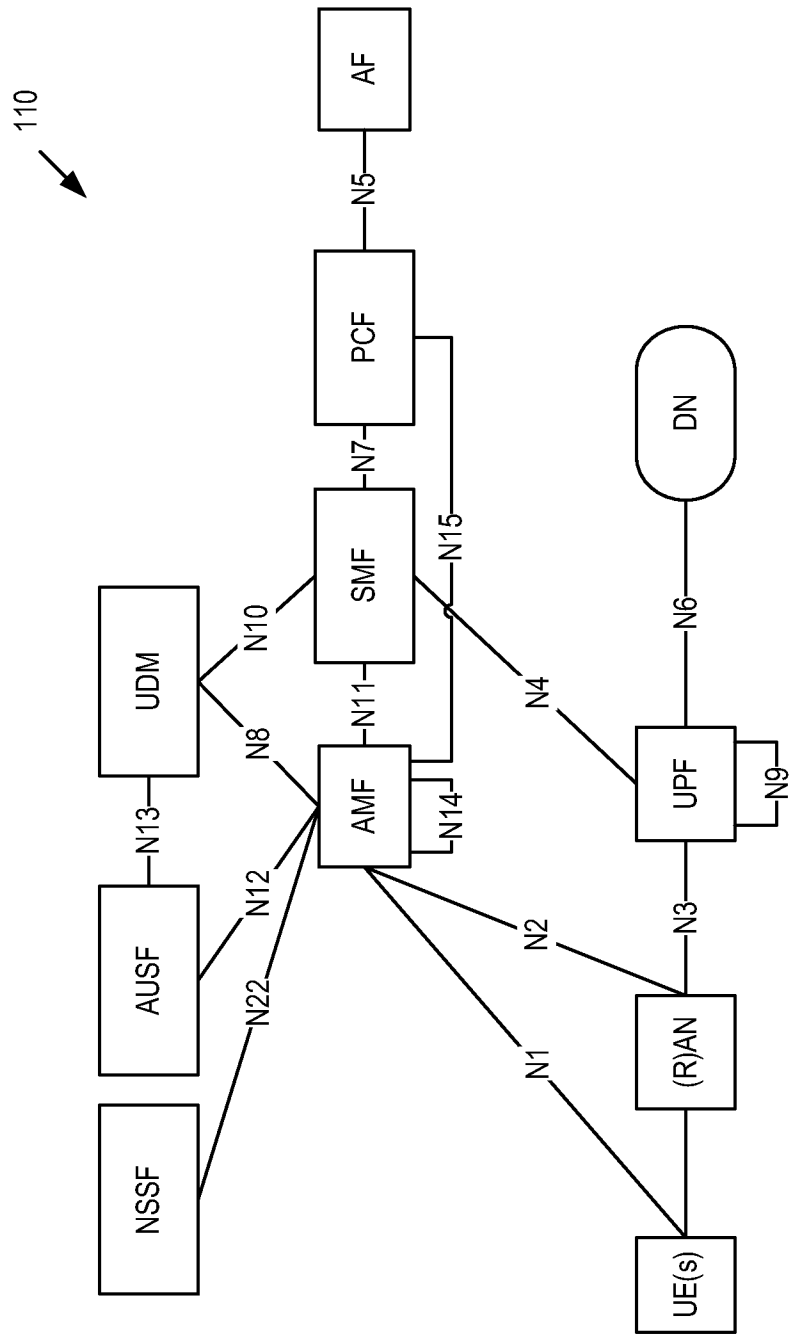
110
AF
N5
PCF
N7
SMF
N15
N10
UDM
N8
N11
AMF
N14
N4
UPF
N9
DN
N6
N13
AUSF
N12
N22
N2
N3
(R)AN
NSSF
N1
UE(s)

FIG. 3

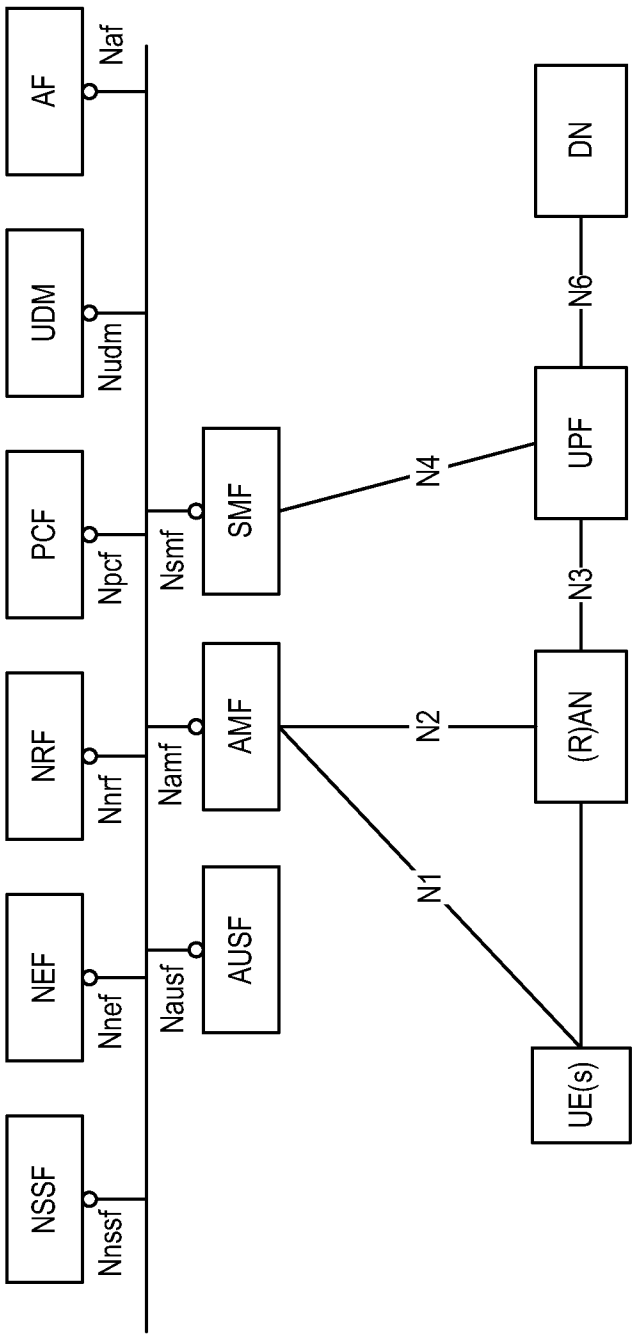
AF
Naf
UDM
Nudm
PCF
Npcf
Nsmf
SMF
N4
UPF
N6
DN
NRF
Nnrf
Namf
AMF
N2
(R)AN
N3
N1
NEF
Nnef
Nausf
AUSF
NSSF
Nnssf
UE(s)

FIG. 4

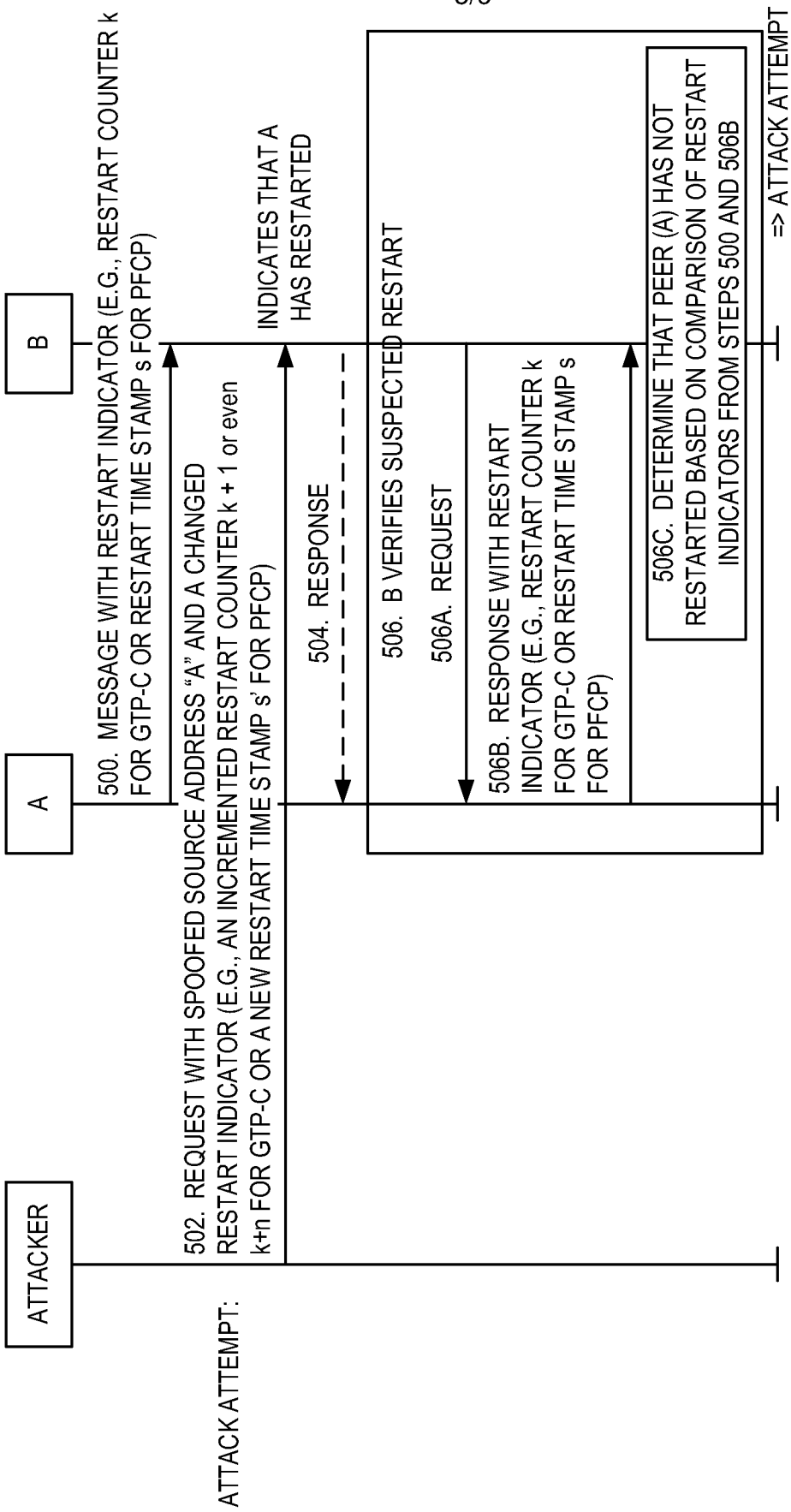
ATTACKER
A
B
ATTACK ATTEMPT:
500. MESSAGE WITH RESTART INDICATOR (E.G., RESTART COUNTER k FOR GTP-C OR RESTART TIME STAMP s FOR PFCP)
502. REQUEST WITH SPOOFED SOURCE ADDRESS "A" AND A CHANGED RESTART INDICATOR (E.G., AN INCREMENTED RESTART COUNTER k + 1 or even k+n FOR GTP-C OR A NEW RESTART TIME STAMP s' FOR PFCP)
INDICATES THAT A HAS RESTARTED
504. RESPONSE
506. B VERIFIES SUSPECTED RESTART
506A. REQUEST
506B. RESPONSE WITH RESTART INDICATOR (E.G., RESTART COUNTER k FOR GTP-C OR RESTART TIME STAMP s FOR PFCP)
506C. DETERMINE THAT PEER (A) HAS NOT RESTARTED BASED ON COMPARISON OF RESTART INDICATORS FROM STEPS 500 AND 506B
=> ATTACK ATTEMPT CAN BE AVOIDED

FIG. 5

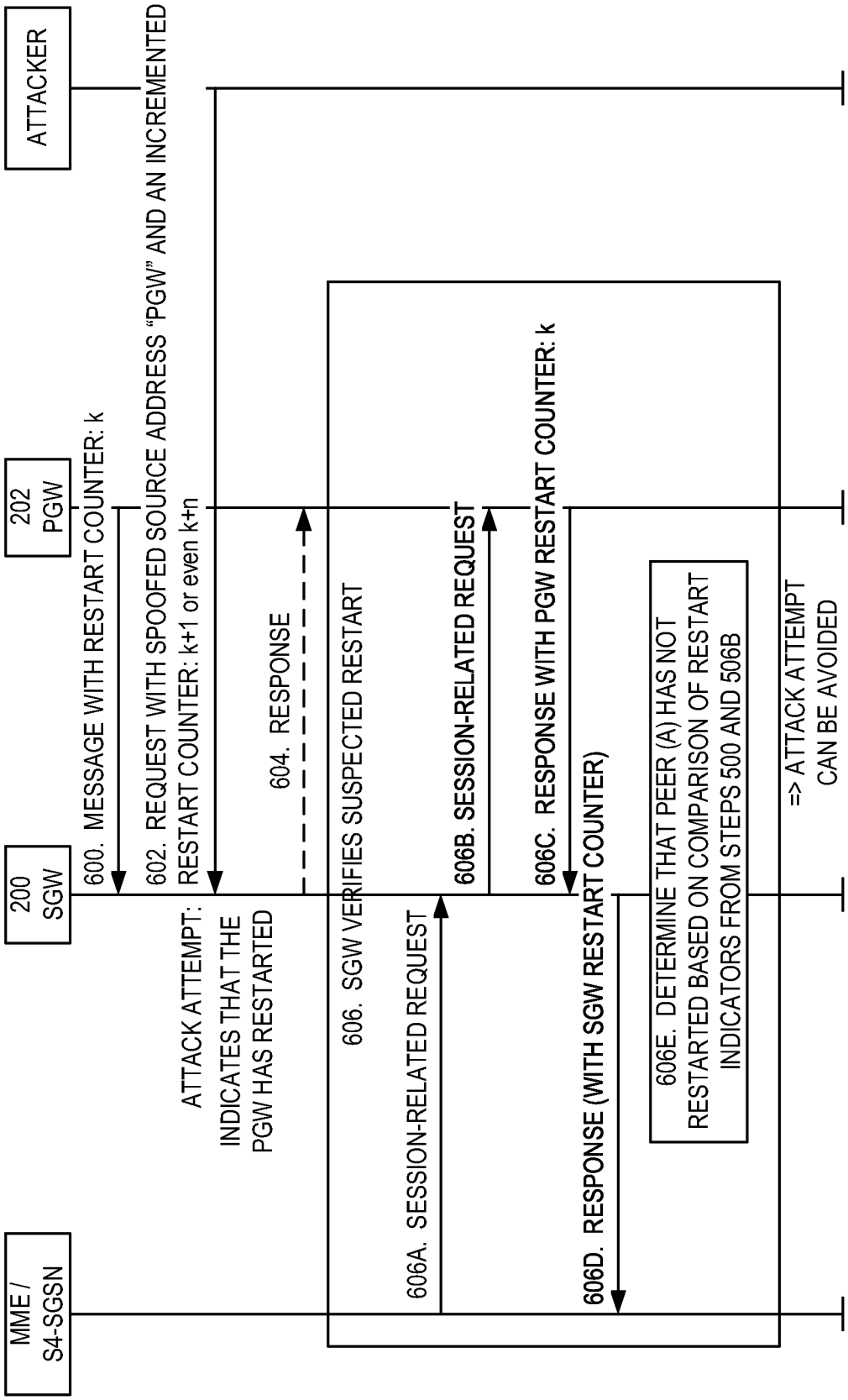
ATTACKER
202 PGW
200 SGW
MME / S4-SGSN
600. MESSAGE WITH RESTART COUNTER: k
602. REQUEST WITH SPOOFED SOURCE ADDRESS "PGW" AND AN INCREMENTED RESTART COUNTER: k+1 or even k+n
ATTACK ATTEMPT: INDICATES THAT THE PGW HAS RESTARTED
604. RESPONSE
606. SGW VERIFIES SUSPECTED RESTART
606A. SESSION-RELATED REQUEST
606B. SESSION-RELATED REQUEST
606C. RESPONSE WITH PGW RESTART COUNTER: k
606D. RESPONSE (WITH SGW RESTART COUNTER)
606E. DETERMINE THAT PEER (A) HAS NOT RESTARTED BASED ON COMPARISON OF RESTART INDICATORS FROM STEPS 500 AND 506B
=> ATTACK ATTEMPT CAN BE AVOIDED

FIG. 6

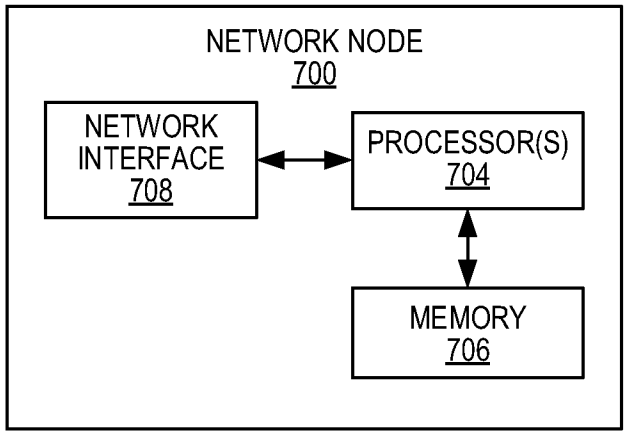
NETWORK NODE
700
NETWORK INTERFACE
708
PROCESSOR(S)
704
MEMORY
706

FIG. 7

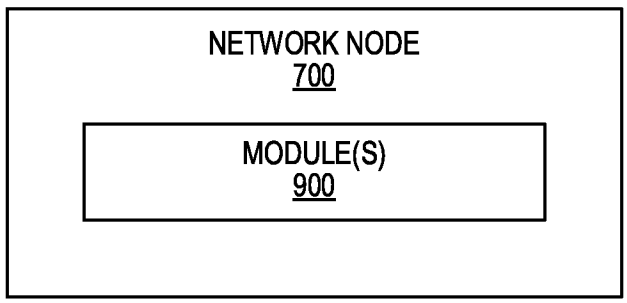
NETWORK NODE
700
MODULE(S)
900

FIG. 9

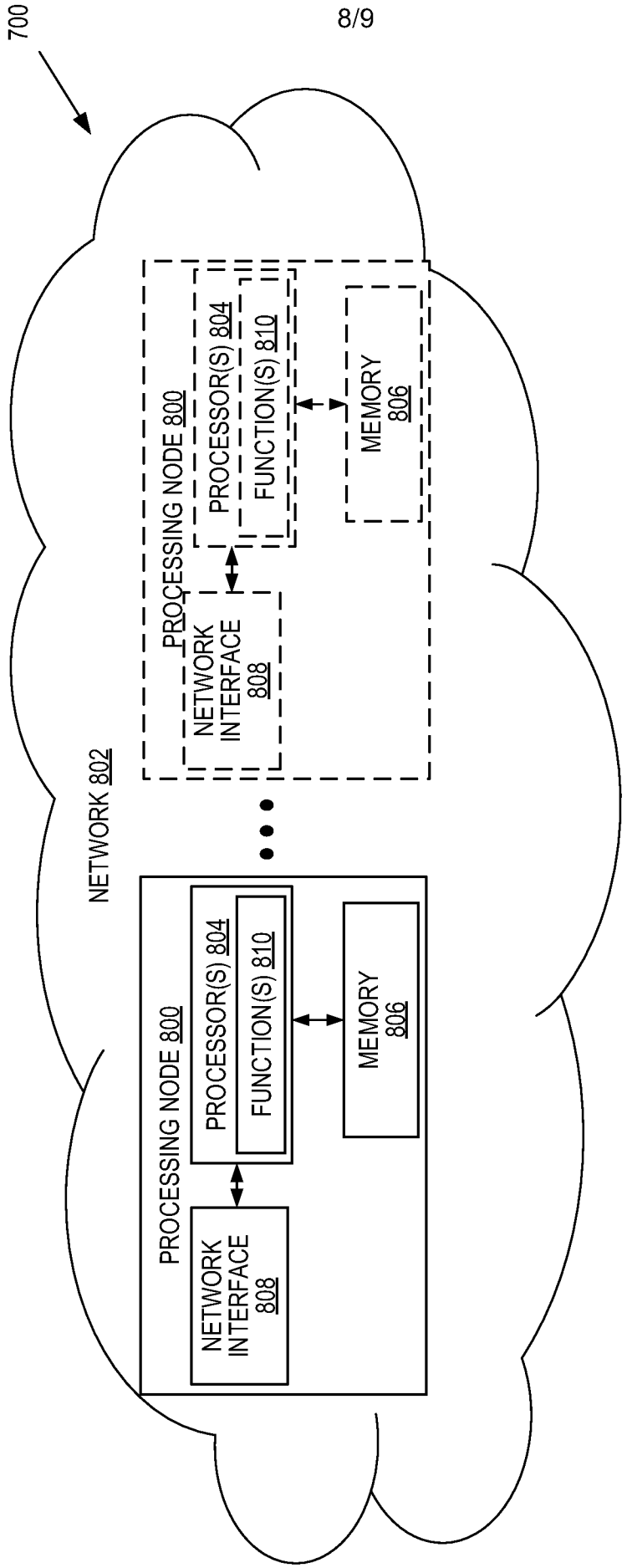
700
NETWORK 802
PROCESSING NODE 800
NETWORK INTERFACE 808
PROCESSOR(S) 804
FUNCTION(S) 810
MEMORY 806
PROCESSING NODE 800
NETWORK INTERFACE 808
PROCESSOR(S) 804
FUNCTION(S) 810
MEMORY 806

FIG. 8

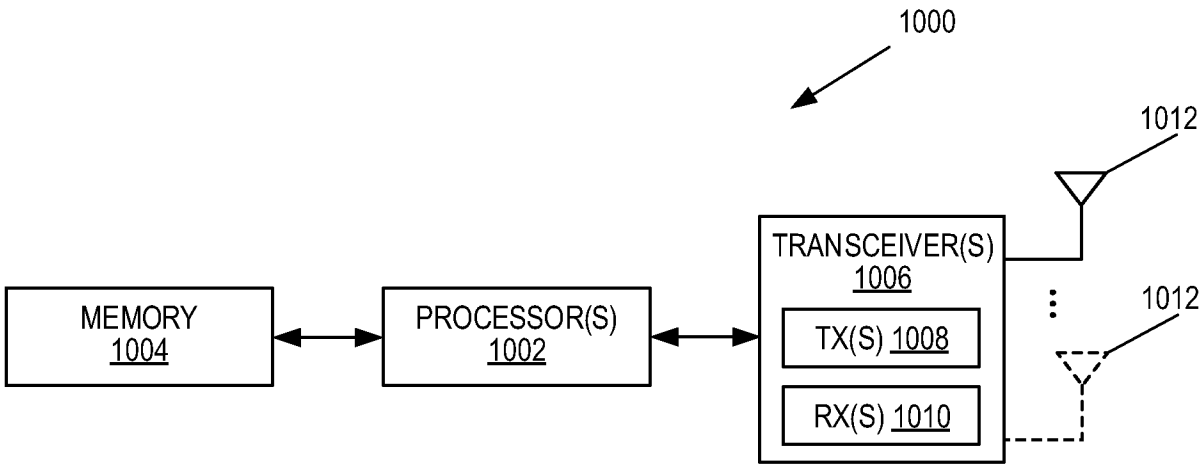
1000
1012
TRANSCEIVER(S)
1006
TX(S) 1008
RX(S) 1010
1012
MEMORY
1004
PROCESSOR(S)
1002

FIG. 10

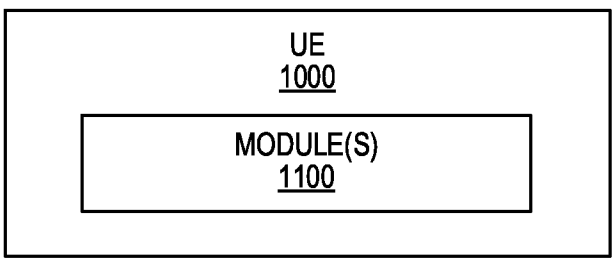
UE
1000
MODULE(S)
1100

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2020/050194

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W

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

SE, DK, FI, NO classes as above

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

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20110258682 A1 (YIN YU), 20 October 2011 (2011-10-20); abstract; [0047]-[0049],[0065]	1-10
	--	
A	WO 2011095256 A1 (ERICSSON TELEFON AB L M ET AL), 11 August 2011 (2011-08-11); abstract; claim 1	1-10
	--	
A	US 20050216954 A1 (RAMAIAH ANANTHA ET AL), 29 September 2005 (2005-09-29); abstract	1-10
	--	
A	US 20160315963 A1 (FIASCHI GIOVANNI ET AL), 27 October 2016 (2016-10-27); abstract	1-10
	--	

☒ 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

"D" document cited by the applicant in the international application

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04-06-2020	04-06-2020

Name and mailing address of the ISA/SE	Authorized officer
Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Eddie Rmaili Telephone No. + 46 8 782 28 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2020/050194

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3GPP Standard; 3GPP TS 23.007, - 20091217 - 3rd Generation Partnership Project (3GPP), Mobile Competence Centre ; 650, route des Lucioles ; F-06921 Sophia-Antipolis Cedex ; France. 2009-12-17. 3rd Generation Partnership Project; Technical Specification Group Core Network; Restoration procedures (Release 8); whole document; abstract --	1-10
P, X	3GPP Draft; CP-193041, - 20191120 - 3rd Generation Partnership Project (3GPP), Mobile Competence Centre ; 650, route des Lucioles ; F-06921 Sophia-Antipolis Cedex ; France. 2019-11-20. GTP Recovery Counter and GSN node behaviour; whole document; abstract -- --------	1-10

International application No.
PCT/SE2020/050194

Continuation of: second sheet

International Patent Classification (IPC)

H04L 9/00 (2006.01)
H04W 12/00 (2009.01)
H04W 12/06 (2009.01)

US	20110258682	A1	20/10/2011	CN	101771564	B	09/10/2013
				WO	2010075685	A1	08/07/2010
WO	2011095256	A1	11/08/2011	NONE			
US	20050216954	A1	29/09/2005	CA	2565409	A1	29/12/2005
				CN	101390064	A	18/03/2009
				EP	1751910	A2	14/02/2007
				US	7472416	B2	30/12/2008
				WO	2005125079	A3	21/12/2006
US	20160315963	A1	27/10/2016	US	10122755	B2	06/11/2018
				WO	2015096905	A1	02/07/2015