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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 December 2022 (22.12.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/263222 A1

(51) International Patent Classification:
H04W 12/12 (2021.01) *H04W 88/16* (2009.01)
H04W 36/14 (2009.01)

(21) International Application Number:
PCT/EP2022/065341

(22) International Filing Date:
07 June 2022 (07.06.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
21180089.1 17 June 2021 (17.06.2021) EP

(71) Applicant: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Inventors: **RÖMER, Stefanus**; Hönscheidstraße 4a, 55773 Hennef (DE). **BIEWALD, Manuel**; Marktplatz 32, 95514 Neustadt am Kulm (DE). **LACHMUND, Sven**; Max-von-Gruber-Str. 2, 80804 München (DE). **BAUMANN, Jürgen**; Heerstr. 43, 53111 Bonn (DE).

(74) Agent: **BRAUN-DULLAEUS PANNEN EMMERLING PATENT- UND RECHTSANWALTSPARTNERSCHAFT MBB**; Platz der Ideen 2, 40476 Düsseldorf (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, IQ, IR, IS, IT, JM, 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, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) Title: TECHNIQUES TO ENABLE A SECURE DATA COMMUNICATION BETWEEN A FIRST NETWORK AND A SECOND NETWORK THAT COMPRISE AT LEAST IN PART A DIFFERENT COMMUNICATION ENVIRONMENT

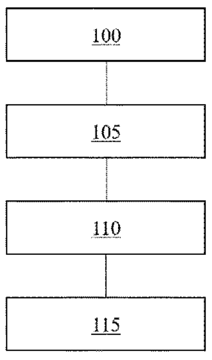


Fig. 2

(57) Abstract: A method and system for to enable a secure data communication between a first network of a first network provider and a second network of a second network provider, wherein the first network comprises at least a first part that is a 5G communication environment, wherein the second network comprises at least a first part that is communication environment preceding the 5G communication environment and wherein an access link to the first part of the second network comprises a GTP-firewall to protect the first part of the second network; wherein the method comprises the following step: - Establishing a handover process from the 5G communication environment of the first network to the non-5G first part of second network;; - Directing a control plane traffic of the data transmission from a SEPP of the first network to a SEPP of the second network; wherein the SEPP of the first network encrypts the data transmission and the SEPP of the second network decrypts the encrypted data transmission; - Directing a user plane traffic of the data transmission to the access link to the non-5G first part of the second network and through the GTP-firewall; - Providing the decrypted control plane traffic to the GTP-firewall, wherein the GTP-firewall performs security measures based on information extracted from the control plane traffic.

WO 2022/263222 A1

Techniques to enable a secure data communication between a first network and a second network that comprise at least in part a different communication environment

The invention relates to techniques to enable a secure data communication between a first network and a second network of second that comprise at least in part a different communication environment.

In particular, the invention relates to the typical use case of a roaming situation in which a user has access to a visited network and connects into his home network. During handover process in the context of roaming situations it can happen that different communication standards of the visited network and the home network are applied so that the visited network and the home network need to agree on a common communication standard in the handover process. It can happen that the user is only allowed to use certain communication standard due to his contract with a network provider. Then the following situation can occur: The user has access to a 5G communication environment in the visited network and roams into his home network that only supports the 4G communication environment. However, such use cases typically lead to technical compatibly problems between the two different communication standards.

In practice so-called GTP firewalls are used to protect 4G core network components in the roaming case.

From 2.5G up to 4G the “un-secure” GTP-protocol is used for both, control- and user-plane to handle data services. To protect a Home Public Land Mobile Network (hPLMN) a GTP-Firewall is placed between hPLMN and a foreign IPX-Network, where behind the IPX-Network typically is a Visited Public Land Mobile Network (vPLMN) lies.

These firewalls do not only check for allowed sockets (allowed source IP, port and destination IP, port), but they are also capable to inspect and validate a content of GTP messages (DPI Deep Packet Inspection). With these information additional security measures like the following are applied:

- Validation of message flow and content verification of IEs (Information Elements);
- Based on TEIDs (Tunnel Endpoint Identifier) only allow GTP-U data transfer if the corresponding GTP-C was successfully established;
- Allowing incoming traffic only for own IMSI and MSISDN prefixes;
- Validation of handovers for existing tunnels from one IP-node to another;
- Releasing idling tunnels after a defined time limit (depending on used RAT-Type);
- Limiting the number of requests per second based on APN to protect internal network elements;

On the other side, in 5G networks there is a strict separation of control plane traffic and user plane traffic. The control plane traffic is authenticated and encrypted by a SEPP (Security Edge Protection Proxy) before it is sent to a roaming network of a roaming partner. As a result of this encryption, a GTP-Firewall that is used for the user plane traffic in 4G cannot read the corresponding control traffic and hence is not able to identify the corresponding GTP tunnels. The leads to the adverse technical effect that the GTP-Firewall looses its capability to apply the above-mentioned security measures. In an “isolated” 5G network, the build-in 5G-security is sufficient to apply the above-mentioned security measures.

In contrary to previous mobile network generations (e.g. 4G), 5G comes with built-in signalling security (Security-by-design to combat fraud & attacks). In particular, 5G introduces secure signalling for roaming over a N32 interface to fix the root cause for attacks and fraud:

- Only legitimate roaming partners can send signalling messages;
- It can be determined if messages were modified on transit;

- Sensitive information in signalling messages is encrypted and not readable on transit;
- Incoming messages are checked for their plausibility.

Fig. 1 shows a generic 5G core network with its build-in signaling security features: The above-mentioned in-built security mechanisms for 5G roaming are sufficient in a pure 5G roaming scenario when a 5G user is registered in a visited 5G public land mobile network (vPLMN) and establishes data connections back to the home public land mobile network (hPLMN). Such a scenario is referred to as “outbound roaming in a visited 5G network”.

However, when seamless handover from 5G to 4G and/or from 4G to 5G in the vPLMN shall be supported, compatibly problems occur due to the different security measures. The GTP-Firewall is not capable to read the encrypted 5G control traffic.

WO 2020/148330 A1 teaches a user plane network entity of a 5G core network that performs: obtaining GPRS Tunneling Protocol User Plane (GTP-U) tunneling information of a new or updated protocol data unit (PDU) session from a control plane network entity of the 5G core network; and adjusting according to the obtained GTP-U tunneling information a GTP-U firewall for selectively allowing to pass through only GTP-U traffic concerning GTP-U tunnels defined by the GTP-U tunneling information. The control plane network entity performs: obtaining from control plane signaling the GTP-U tunneling information and communicating same to the GTP-U firewall. However, WO 2020/148330 A1 does only teach a pure 5G solution without addressing capability problems that occur during a handover process if the hPLMN supports 4G and the vPLMN supports 5G or the other way round. In addition, the method according to WO 2020/148330 A1 creates a great load of data traffic to obtain the necessary GPRS Tunneling Protocol User Plane (GTP-U) tunneling information.

In the view of above, it is an object of the present invention to efficiently provide the GTP-Firewall with the necessary information to protect 2G, 3G and 4G core network components in the roaming case.

This object is solved by the features of the independent claims.

The features of the various aspects of the invention described below or the various examples of implementation may be combined with each other, unless this is explicitly excluded or is technically impossible.

According to a first aspect of the invention, a method to enable a secure data communication between a first network of a first network provider and a second network of a second network provider is taught,

wherein the first network comprises at least a first part that is a 5G communication environment, wherein the second network comprises at least a first part that is communication environment preceding the 5G communication environment and wherein an access link to the first part of the second network comprises a GTP-firewall to protect the first part of the second network; in other words: the first part of the second network runs on a non-5G technique, such a technique can be for example according to 4G mobile communication protocols.

wherein the method comprises the following step:

- Establishing a handover process from the 5G communication environment of the first network to the non-5G first part of second network; during the handover process, the hPLMN and the vPLMN agree on the standard they shall use for further data transmission. If the non-5G first part of second network is 4G, then they will agree on both using 4G for data transmission. However, to facilitate this handover process in a secure way, certain information of the 5G control traffic are necessary in order to run the GTP-firewall properly before data is transmitted to the 4G core network. This is a typical roaming use case that introduces the challenge that each of the network providers wants to secure his own network from not authorized communications coming from a foreign network.
- Directing a control plane traffic of the data transmission from a vSEPP of the first network to a hSEPP of the second network; wherein the vSEPP of the first network encrypts the data

transmission and the hSEPP of the second network decrypts the encrypted data transmission; as already the name indicates, the SEPPs (Security Edge Protection Proxy) provide a security measure by performing the encryption;

- Directing a user plane traffic of the data transmission to the access link to the non-5G first part of the second network and through the GTP-firewall; this is the case, if for some reasons the second network does not provide a 5G environment for the user plane traffic. This can be due to system requirements, system failure or due to contract conditions between the network provider and the user.
- Providing the decrypted control plane traffic to the GTP-firewall, wherein the GTP-firewall performs security measures based on information extracted from the control plane traffic.

This provides the advantage that a seamless handover from 5G to 4G and/or from 4G to 5G in the vPLMN is enabled. One possible use case is if a user communicates with his user equipment, like a smartphone, in a roaming situation. When a seamless handover from 5G to 4G and/or from 4G to 5G in the vPLMN is supported, the additional so-called GTP-FW at the border between the hPLMN and the vPLMN is needed in order to maintain the security level and to protect against attacks and fraud. The GTP-FW needs to be informed about these handover events, e.g. by a Modified bearer signaling message. This is facilitated by providing the decrypted control plane traffic to the GTP-firewall.

In particular, for validation of new or existing tunnel connections for the user data (GTP-U tunnels), the knowledge of at least the source and destination IP and port of the involved GSNs/UPFs and a valid Tunnel Endpoint ID (TEID) for both directions is necessary to apply security rules by the GTP-firewall. Additional information elements IEs like SUPI, PLMN-ID etc. can be available to the GTP-FW to perform further validity checks in handover scenarios. The SUPI can comprise an IMSI and/or a line-ID.

In an embodiment, the GTP-firewall blocks data traffic to the non-5G first part of the second network as a security measure.

This provides the advantage that the GTP-firewall of the second network can efficiently secure the non-5G first part of the second network. The non-5G first part of the second network can be a 4G core network. If the non-5G first part of the second network is a 4G core mobile network, this provides the advantage that the typical use cases of roaming situations are covered.

In an embodiment, the first network is a vPLMN network and the second network is a hPLMN network designed for roaming use cases.

If all the data communication occurs within the network of single network provider, then even the switch from a 5G communication protocol to a 4G communication protocol is not causing capability problems as pointed out in the introduction of this invention because the network provider basically has all the necessary information ready. In such a situation the attack from the outside cannot occur because all the communication is within one single network. However, if the first network is a hPLMN network and the second network is a vPLMN network designed for roaming use cases this advantageously covers the typical use case of roaming scenarios that play an important role if the user wants to communicate from abroad.

In an embodiment, the GTP-firewall is located at the interface between the hPLMN network and the vPLMN network.

This provides the advantage that the GTP-firewall can decide very soon if it blocks the data traffic to the core of the hPLMN network. If the GTP-firewall would logically be located deeper within the hPLMN network this would cause an unnecessary security risk and an unnecessary use of computational resources if the GTP-firewall would decide to block the data traffic anyway.

In an embodiment, the first network comprises a second part that is a communication environment preceding a 5G communication environment and/or wherein the second network comprises a second part that is a 5G communication environment.

This provides the advantage that the switch from 4G to 5G and from 5G to 4G is possible in any direction between the two networks. Another advantage is that the 5G communication infrastructure of the second network can be used to provide the decrypted control plane traffic to the GTP-firewall. For example, the hSEPP of the 5G part of the second network can be used to decrypt the control plane traffic for the GTP-firewall.

In an embodiment, the GTP-FW is implemented within the SEPP of the second network, in particular within the hSEPP of the HPLMN network. This provides the advantage that providing the decrypted control plane traffic to the GTP-firewall does only cause internal traffic within the SEPP of the second network. In addition, this is one possibility to perform the security measures of the GTP-FW logically at the edge of the second network. Further advantages are a reduced complexity for network or SBA integration. Less internal signaling traffic within the SBA. Efficient interworking with the GTP-FW why are in the process communication that allows a very efficient implementation. However, on the downside the hSEPP gets more complex and there is a tight coupling between control plane (CP) and user plane (UP) within the hSEPP that may narrow down landscape of a vendor. SBA means Service Based Architecture (as defined by 3GPP TS 29.571) where service producers offer their services to a service consumer over a so-called service based interface (SBI) based on http/2 – JSON requests. The service producer registers the profile of its service based interfaces with all parameters in a central Network Repository Function (NRF). The service consumer can query the NRF for a specific SBI. This new architecture allows for loosely coupled network functions which can scale independently of each other. The SBA is a key concept of 5G standalone core.

In an embodiment, the SEPP stores the decrypted control plane traffic within an internal database along with an associated time stamp, and wherein the GTP-FW regularly checks new entries of that database or wherein the SEPP notifies the GTP-FW about new entries within the database.

This provides the advantage of an efficient mechanism to trigger the activity of the GTP-FW and an efficient method for the GTP-FW to find the relevant entries.

In an embodiment, a copy of the N4 traffic is transmitted to the GTP-FW. This provides the advantage of a loosely coupling between the CP and the UP that enhances the flexibility with respect to the design of the network for the network operator. However, as downside copying and analyzing of complete N4 traffic consumes a lot of resources. In addition, a N4 is not a REST API but connection-orientated based on GTP-C. So, a new N4 connection needs to be configured to the GTP-FW.

In an embodiment, the GTP-FW is being provided with information elements that are a subset of the decrypted control plane traffic.

This provides the advantage of providing only information elements to the GTP-FW that are actually needed to perform its security measures. As stated above, copying and analyzing of complete N4 traffic consumes a lot of resources. This is circumvented by selecting only certain information elements that are necessary to perform the security measures and making them available to the GTP-FW.

In an embodiment, the GTP-FW gets the information elements that are subset of the control plane traffic from SMFs that are related to traffic management from the first part of the first network to the first part of the second network. SMF means Session Management Function as defined by 3GPP TS29.508.

Basically, this is the preferred solution because it also provides loosely coupling between the CP and the UP. This also provides the advantage of high flexibility and scalability because new SMFs and UPF (UPF: User Plane Function as defined by TS29.281) can easily be added. The additional internal SBA signaling traffic to provide the GTP-FW with the information elements is only recused in roaming cases. The amount of the additional SBA traffic is not increased that much because the information elements are only a subset of the control plane traffic.

In an embodiment, the GTP-FW performs the following steps:

- Registering with a service profile in a NRF;
- Asking the NRF for all SMFs that serve roaming traffic;

- Subscribing to a notification service of all SMFs that serve roaming traffic, wherein the SMFs send selected information elements to the GTP-FW.

This provides the advantage of selecting the appropriate information elements from the decrypted control plane traffic. This also provides an efficient measure to trigger the activity of the GTP-FW.

In an embodiment, the GTP-FW gets the information elements that are subset of the control plane traffic from a NEF (Network Exposure Function).

This provides the advantage of a complete decoupling from SBA. A further advantage is topology hiding of internal SBA. As a downside, this alternative provides less efficient interworking with the GTP-FW in terms if message delay and controlling the session depends on the offered NEF functionality.

In an embodiment, the hPLMN network and/or the vPLMN are cellular networks.

This provides the advantage that the method can be used in the very frequent use cases if users access the communication network by their smartphones or other user equipment in roaming situations.

According to a second aspect of the invention, a communication system to enable a secure data communication between a first network of a first network provider and a second network of a second network provider is provided, the communication system comprises

- the first network that comprises at least a first part that is a 5G communication environment,
- the second network that comprises at least a first part that is communication environment preceding the 5G communication environment;
- an access link to the first part of the second network with a GTP-firewall to protect the first part of the second network;

wherein the communication system is configured to perform the steps according to the method described above.

The inventive communication system basically provides the same advantages as already described within the context of the method.

In the following, preferred implementation examples of the present invention are explained with reference to the accompanying figure:

Fig. 1: shows a generic 5G core network with its build-in signaling security features.

Fig. 2: shows a flow diagram of a method according to the invention.

Fig. 3: shows a first embodiment of the method according to Fig. 2 within a communication system.

Fig. 4: shows a second embodiment of the method according to Fig. 2 within a communication system.

Fig. 5: shows a third embodiment of the method according to Fig. 2.

Fig. 6: shows a fourth embodiment of the method according to Fig. 2.

Fig. 7: shows a fifths embodiment of the method according to Fig. 2.

In the following, numerous features of the present invention are explained in detail by means of preferred embodiments. The present disclosure is not limited to the specifically named combinations of features. Rather, the features mentioned here can be combined arbitrarily into inventive embodiments, unless this is expressly excluded below.

In roaming scenarios when a seamless session handover from 5G network of a vPLMN to a 4G network of a hPLMN shall be established, special control plane information - such as for example the TEID - shall be available for the GTP-firewall that is used for 4G traffic in order to verify the correctness of any new or existing GTP-U tunnel on the N9 interface. Handover from 5G to 4G always means that the technology is changed in both hPLMN and vPLMN.

The same applies to the reverse case, 4G to 5G. Practically always triggered by the vPLMN.

Fig. 2 shows a flow diagram according to the invention with the following steps:

Step 100: Establishing a data transmission according to 5G protocols from the 5G communication environment 150 of the first network 155 to the 4G first part 186 of the second network 165;

Step 105: Directing control plane traffic of the data transmission from a SEPP 170 of the first network 155 to a hSEPP 175 of the second network 165; wherein the vSEPP 170 of the first network 155 encrypts the data transmission and the hSEPP 175 of the second network 165 decrypts the encrypted data transmission;

Step 110: Directing user plane traffic of the data transmission via the access link 180 to the 4G first part 186 of the second network 165 and through a GTP-firewall 185;

Step 115: Providing the decrypted control plane traffic to the GTP-firewall 185, wherein the GTP-firewall 185 performs security measures based on information extracted from the control plane traffic.

The second network 165 typically comprises a 5G part, too. The 5G part of the second network 165 comprises a control plane part 168 and a user plane part 160. The technical infrastructure of the 5G control plane part 168 can be used to facilitate the invention according to the inventive method.

Fig. 3 shows a first embodiment of the method according to Fig. 2 within a communication system 120.

In this embodiment, the GTP-FW 185 is fully integrated within the hSEPP 175 function. The hSEPP 175 handles all control traffic between the vPLMN 155 and the hPLMN 165 and therefore has access to the information elements such as TEID, SUPI, PLMN-ID for any new roaming connection. The GTP-FW 185 can receive these information elements via an internal inter process interface from the hSEPP 175 to perform a security assessment.

For example, the required information can be stored in a shared data memory - e.g. a file or an internal database. In this procedure, the hSEPP 175 writes each change with a time stamp to the shared data store and the GTP-FW 185 periodically searches for new entries. Alternatively, the GTP-FW 185 can be informed via an internal notification that there is a new entry. In all embodiments according to the invention, the GTP-FW 185 is logically placed before the 4G Core 186 of the second network, i.e. the first part of the second network 165.

Fig. 4 shows a second embodiment of the method according to Fig. 2 within the communication system 120. Fig. 4 shows an integration of the GTP-FW 185 within a SBA in order to subscribe to relevant control plane events within a SMF 190.

In Fig. 4, the GTP-FW 185 registers with a service profile at the NRF 195. The service profile contains entries, such as: NF type, NF instance ID, NF service name, Serving PMNL-ID, S-NSSAI, DNN and/or FQDN. NRF: Network Repository Function as described by 3GPP TS29.510: Central "information service for all Network Functions within the SBA. By registering in the NRF, the respective network function makes itself known within the SBA as a producer and available to consumers. At the same time, the NF in question can ask specifically for other NFs and then use their services. In concrete terms, this means that only after the GTP-FW has registered in the NRF can it ask for SMFs that are active within the roaming slice. It is also possible to use subscription updates to get further information elements.

After successful registration at the NRF 195, the GTP-FW 185 asks the NRF 195 for all SMFs 190 that belong to the same network slice (S-NSSAI) and DNN that provides roaming traffic or roaming connections, e.g. depending on parameters such as DNN, S-NSSAI, NF type.

In the next step, GTP-FW 185 subscribes to all these SMFs 190 for an event notification service to receive the necessary information elements such as TEID, SUPI, PLMN-ID for any new roaming connection, e.g. based on a handover.

The GTP-FW 185 will also subscribe to all these SMFs for any termination event for active roaming connection. This termination event notification shall contain the necessary information elements such as TEID, SUPI, PLMN-ID in order to identify the corresponding GTP-U connection and to terminate this connection within the GTP-FW 185.

Hence, according to the embodiment of Fig. 4, the GTP-FW 185 is also provided with a selection of information, i.e. a subset of the decrypted control traffic, to perform the security measures. As Fig. 4 shows, this information is directed to the GTP-FW 185 after it has been decrypted by the hSEPP 175. The same is true within the context according to all embodiments. hSEPP 175 always decrypts the control plane traffic.

The advantage of the solution according to Fig. 4 is that the required control plane information is pre-selected by the SMFs 190 and only these information elements are sent by notification from the SMFs 190 to the GTP-FW 185. Hereby the amount of additional signaling traffic is minimized and a more efficient implementation of the GTP-FW 185 can be achieved. Alternatively, an additional Service Control Proxy (SCP) can be used as an intermediator between the relevant SMFs and the GTP-FWs in order to reduce the amount of additional signaling traffic.

Fig. 5 shows a third embodiment of the method according to Fig. 2 within the communication system 120. Fig. 5 shows an interrogation via a NEF 200.

In this embodiment, the GTP-FW 185 interrogates with the NEF 200 via a first link 205 to get the necessary information elements such as TEID, SUPI, PLMN-ID for any new roaming connection and any termination event notification for existing roaming connections. The NEF 200 then interrogates the NRF 195 for all SMFs 190 that belong to the same network slice (S-NSSAI) and DNN which serves roaming traffic/connections, e.g. depending on parameters such as DNN, S-NSSAI, NF type. The NEF 200 will then subscribe to all SMFs 190 within the roaming slice for a notification service to get informed about the necessary information elements such as TEID, SUPI, PLMN-ID for any new roaming connection. The NEF 200 will also subscribe to all these SMFs 190 for any termination event for active roaming connection. This termination event notification shall contain the necessary information elements such as TEID, SUPI, PLMN-ID in order to identify the corresponding GTP-U connection and to terminate this connection within the GTP-FW 185.

Fig. 6 shows a fourth embodiment of the method according to Fig. 2 within the communication system 120. Fig. 6 reading out an N4 interface.

In this embodiment, the GTP-FW 185 receives a copy of the complete N4 traffic (N4*) from all SMFs 190 within the roaming network slice via a second link 210 that has access to the N4 traffic. This N4* traffic is analyzed by the GTP-FW in order to get the necessary information elements such as TEID, SUPI, PLMN-ID for any new roaming connection. As a downside, this version does not provide any filtering functionality and thus leads to a huge amount of signaling traffic.

Fig. 7 shows a fifths embodiment of the method according to Fig. 2.

In this embodiment, the GTP-FW 185 has a direct N4 interface 215 to all SMFs 190 that facilitate the roaming traffic. In this case a new functionality of the SMF 190 is required that either sends a complete copy of the entire N4 traffic to the GTP-FW 185 or which only sends the N4 protocol elements to the GTP-FW 185 in the roaming case. The complete N4 traffic is copied and send to the GTP-FW 185. In the case that only a subset of the N4 traffic is sent to the GTP-FW 185, this solution is still inefficient compared to solutions of Fig. 4 and 5 because all protocol elements need be analyzed in order to select the necessary information elements for the GTP-FW 185. In other words, the bulk of the N4 traffic is useless for the GTP-FW 185 and only a small selected portion is needed. One advantage of having all parts of the protocol available at the GTP-FW is that new security requirements that require other IEs have them available immediately and don't require the interface, whichever one, to be adapted first.

Claims

1. A method to enable a secure data communication between a first network of a first network provider and a second network of a second network provider,

   wherein the first network (155) comprises at least a first part (150) that is a 5G communication environment, wherein the second network (165) comprises at least a first part (186) that is communication environment preceding the 5G communication environment and wherein an access link (180) to the first part of the second network comprises a GTP-firewall (185) to protect the first part (186) of the second network;

   wherein the method comprises the following step:

   - Establishing a handover process from the 5G communication environment (150) of the first network to the non-5G first part (186) of second network (165), in particular to a 4G communication environment (186) of the second network (165);
   - Directing a control plane traffic of the data transmission from a SEPP (170) of the first network (155) to a SEPP (175) of the second network (165); wherein the SEPP (170) of the first network encrypts the data transmission and the SEPP (175) of the second network decrypts the encrypted data transmission;
   - Directing a user plane traffic of the data transmission to the access link (180) to the non-5G first part of the second network (165) and through the GTP-firewall (175);
   - Providing the decrypted control plane traffic to the GTP-firewall (175), wherein the GTP-firewall (175) performs security measures based on information extracted from the control plane traffic.

2. The method of claim 1, wherein the GTP-firewall blocks data traffic to the non-5G first part of the second network as a security measure.

3. The method of any of the claims, wherein the first part of a communication environment preceding the 5G communication environment is a 2G, 3G and/or a 4G environment.

4. The method of any of the claims, wherein the first network is a HPLMN network and the second network is a VPLMN network designed for roaming use cases.

5. The method of claim 4, wherein the GTP-firewall is located at the interface between the HPLMN network and the VPLMN network.

6. The method of any of the claims, wherein the first network comprises a second part that is a communication environment preceding a 5G communication environment and/or wherein the second network comprises a second part that is a 5G communication environment.

7. The method of any of the claims, wherein the GTP-FW is implemented within the SEPP of the second network, in particular within the hSEPP of the HPLMN network.

8. The method of claim 7, wherein the SEPP stores the decrypted control plane traffic within an internal database along with an associated time stamp, and wherein the GTP-FW regularly checks new entries of that database or wherein the SEPP notifies the GTP-FW about new entries within the database.

9. The method of any of the claims 1 to 6, wherein a copy of the N4 traffic is transmitted to the GTP-FW.

10. The method of any of the claims 1 to 6, wherein the GTP-FW is being provided with information elements that are a subset of the control plane traffic.

11. The method of claim 10, wherein the GTP-FW gets the information elements that are subset of the control plane traffic from SMFs that are related to traffic management from the first part of the first network to the first part of the second network.

12. The method of claim 11, wherein the GTP-FW performs the following steps:

    - Registering with a service profile in a NRF;
    - Asking the NRF for all SMFs that serve roaming traffic;
    - Subscribing to a notification service of all SMFs that serve roaming traffic, wherein the SMFs send selected information elements to the GTP-FW.

13. The method of claim 10, wherein the GTP-FW gets the information elements that are subset of the control plane traffic from a NEF.

14. The method of any of the claims, wherein the HPLMN network and/or the VPLMN are cellular networks.

15. Communication system to enable a secure data communication between a first network of a first network provider and a second network of a second network provider,

wherein the first network comprises at least a first part that is a 5G communication environment, wherein the second network comprises at least a first part that is communication environment preceding the 5G communication environment and an access link to the first part of the second network with a GTP-firewall to protect the first part of the second network;

wherein the communication system is configured to perform the steps of the method of any of the claims 1-14.

Figures

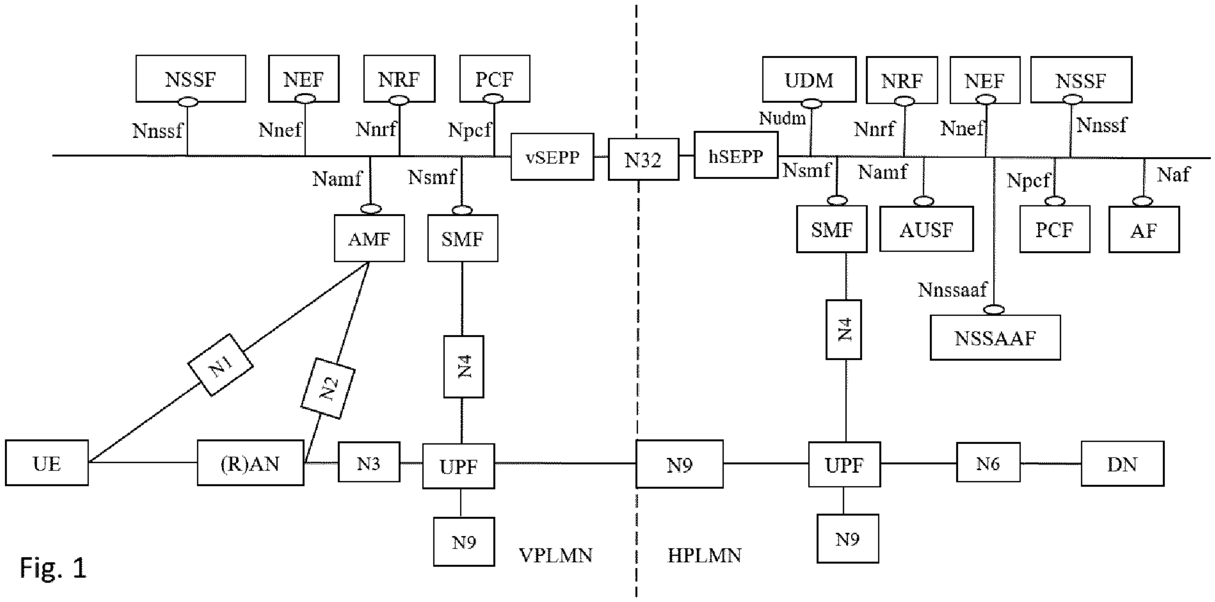


Fig. 1

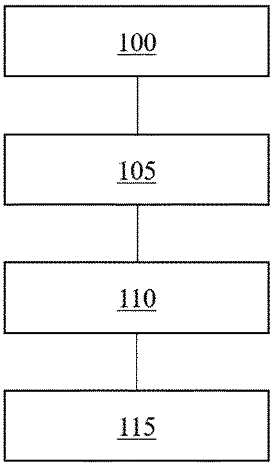


Fig. 2

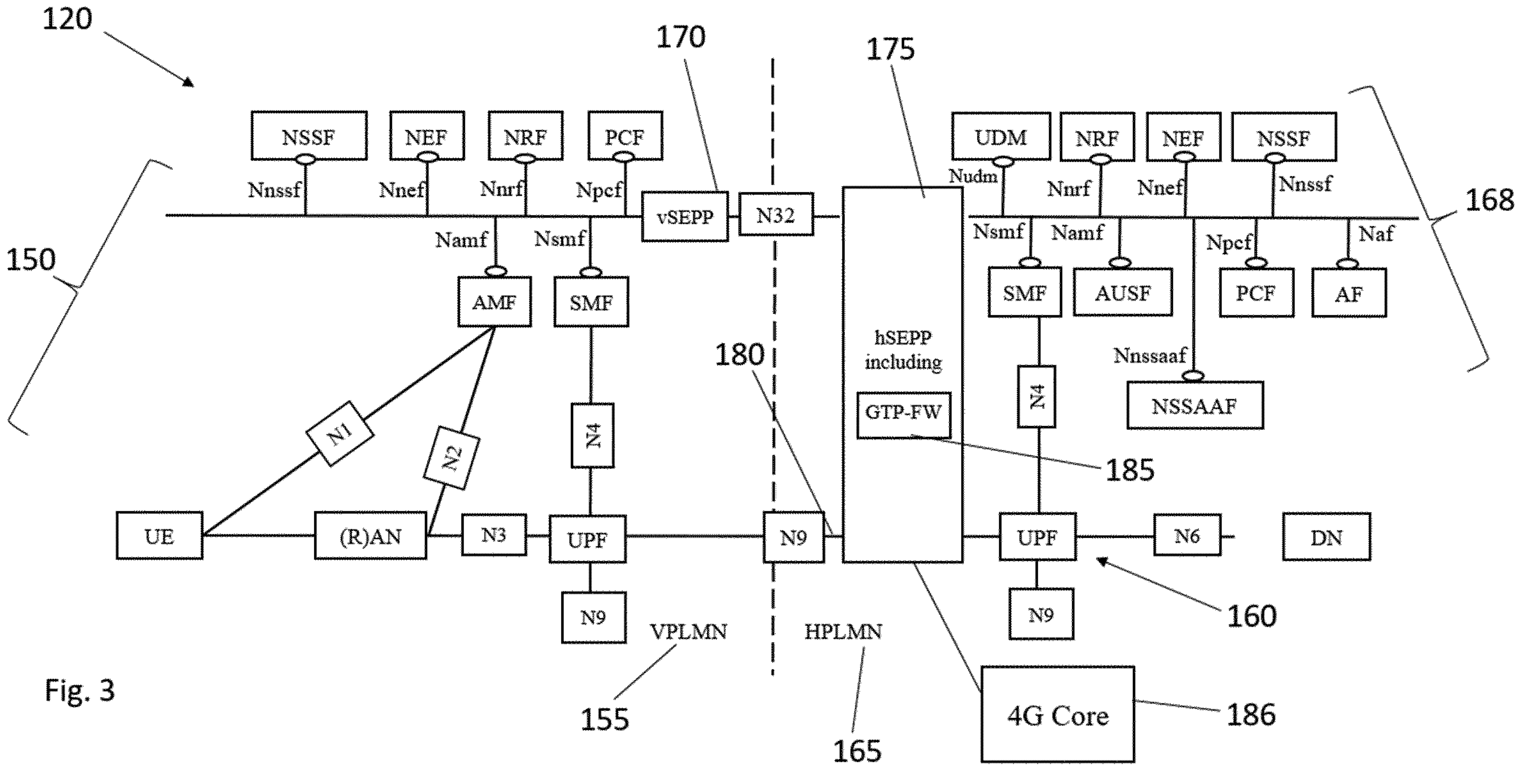

120
170
175
150
168
NSSF
NEF
NRF
PCF
Nnssf
Nnef
Nnrf
Npcf
vSEPP
N32
Namf
Nsmf
AMF
SMF
UDM
NRF
NEF
NSSF
Nudm
Nnrf
Nnef
Nnssf
Nsmf
Namf
Npcf
Naf
SMF
AUSF
PCF
AF
hSEPP
including
GTP-FW
Nnssaaf
NSSAAF
180
N1
N2
N4
N4
185
UE
(R)AN
N3
UPF
N9
UPF
N6
DN
N9
N9
160
VPLMN
HPLMN
4G Core
186
155
165

Fig. 3

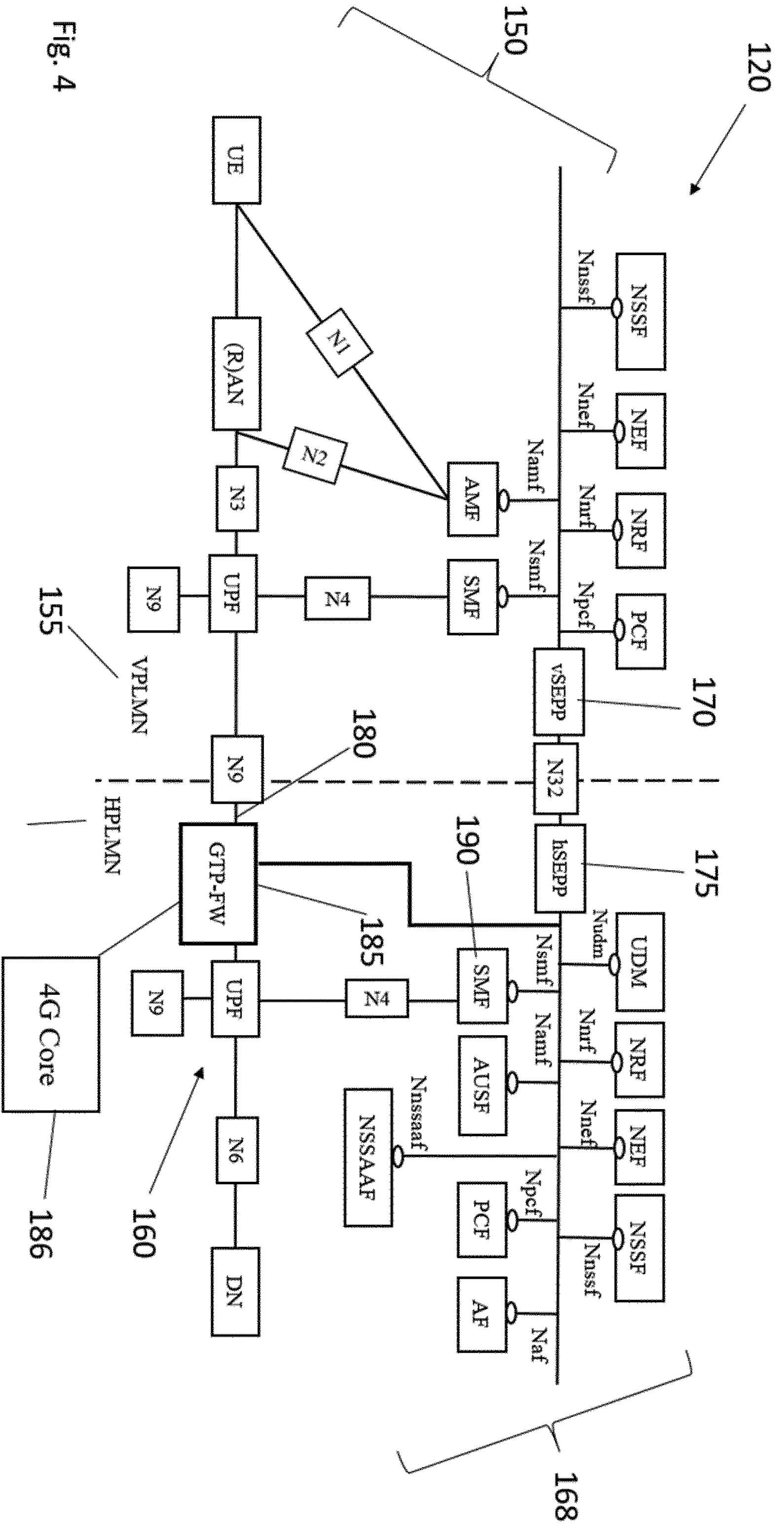
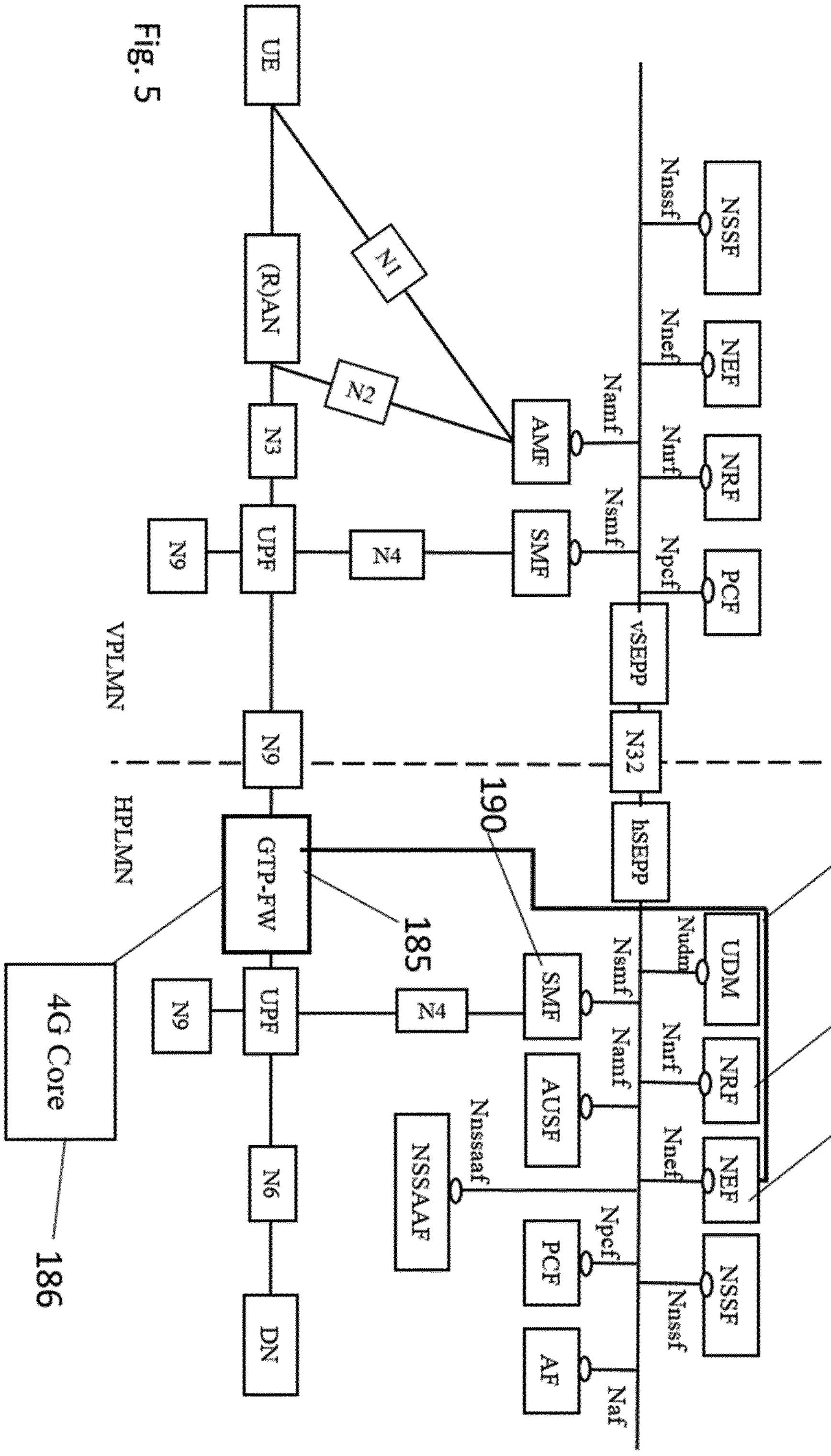


Fig. 4

120
150
UE
(R)AN
N1
N2
N3
AMF
SMF
UPF
N4
N9
NSSF
NEF
NRF
PCF
Nnssf
Nnef
Namf
Nnrf
Nsmf
Npcf
vSEPP
170
155
VPLMN
N9
180
N32
HPLMN
165
hSEPP
175
190
GTP-FW
185
4G Core
186
UDM
Nudm
Nsmf
SMF
N4
UPF
N9
Namf
AUSF
Nnrf
NRF
Nnef
NEF
Nnssaaf
NSSAAF
Npcf
PCF
Nnssf
NSSF
AF
Naf
N6
DN
160
168

Fig. 5


UE
(R)AN
N1
N2
N3
AMF
UPF
N4
SMF
N9
Namf
Nsmf
NSSF
NEF
NRF
PCF
Nnssf
Nnef
Nnrf
Npcf
vSEPP
N32
hSEPP
VPLMN
HPLMN
N9
GTP-FW
185
190
205
195
200
UDM
NRF
NEF
NSSF
Nudm
Nnrf
Nnef
Nnssf
SMF
AUSF
NSSAAF
PCF
AF
Nsmf
Namf
Nnssaaf
Npcf
Naf
UPF
N4
N9
N6
DN
4G Core
186

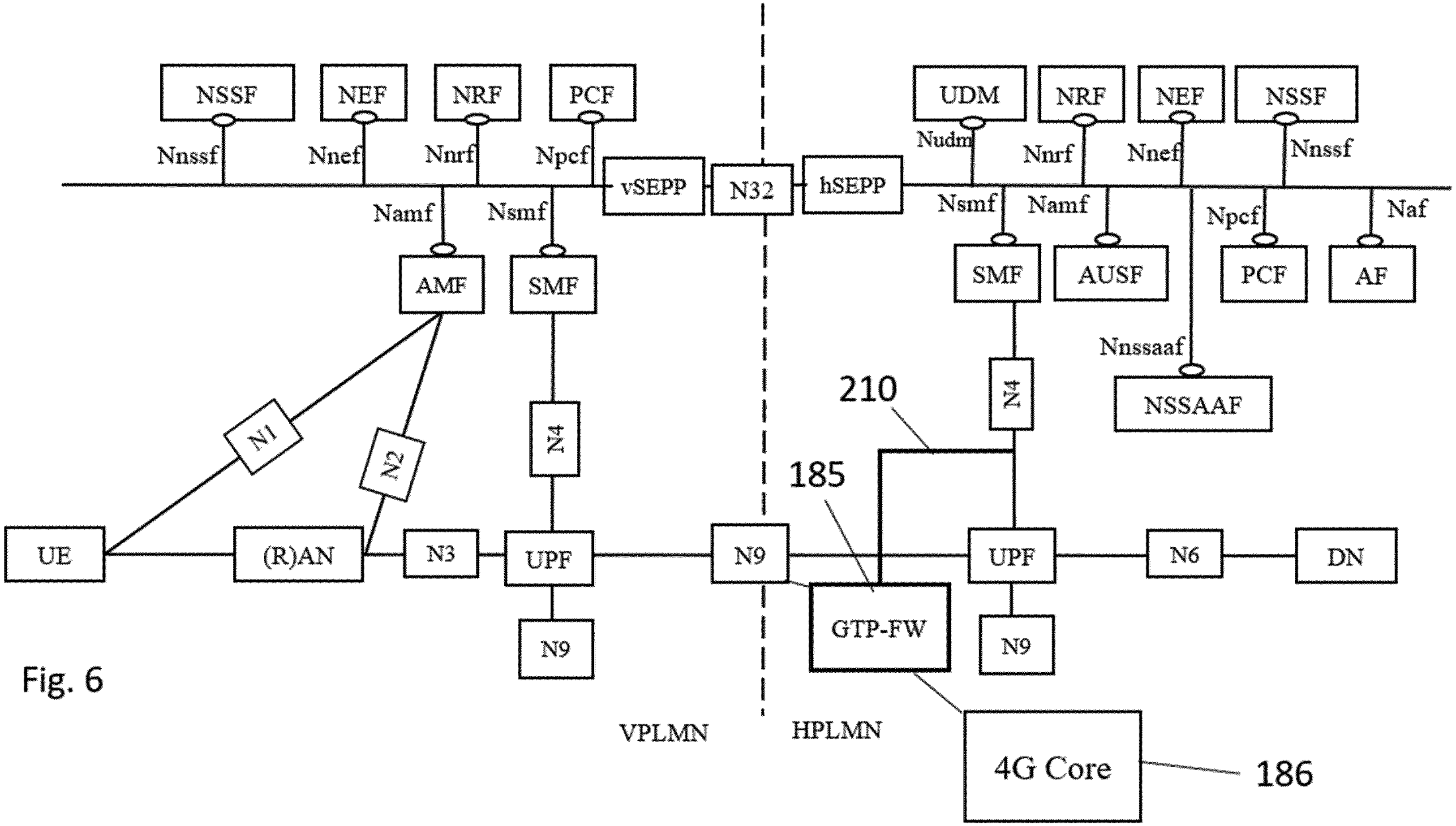

NSSF
NEF
NRF
PCF
Nnssf
Nnef
Nnrf
Npcf
Namf
Nsmf
vSEPP
N32
hSEPP
UDM
NRF
NEF
NSSF
Nudm
Nnrf
Nnef
Nnssf
Nsmf
Namf
Npcf
Naf
AMF
SMF
SMF
AUSF
PCF
AF
Nnssaaf
NSSAAF
N1
N2
N4
N4
210
185
UE
(R)AN
N3
UPF
N9
UPF
N6
DN
N9
GTP-FW
N9
VPLMN
HPLMN
4G Core
186

Fig. 6

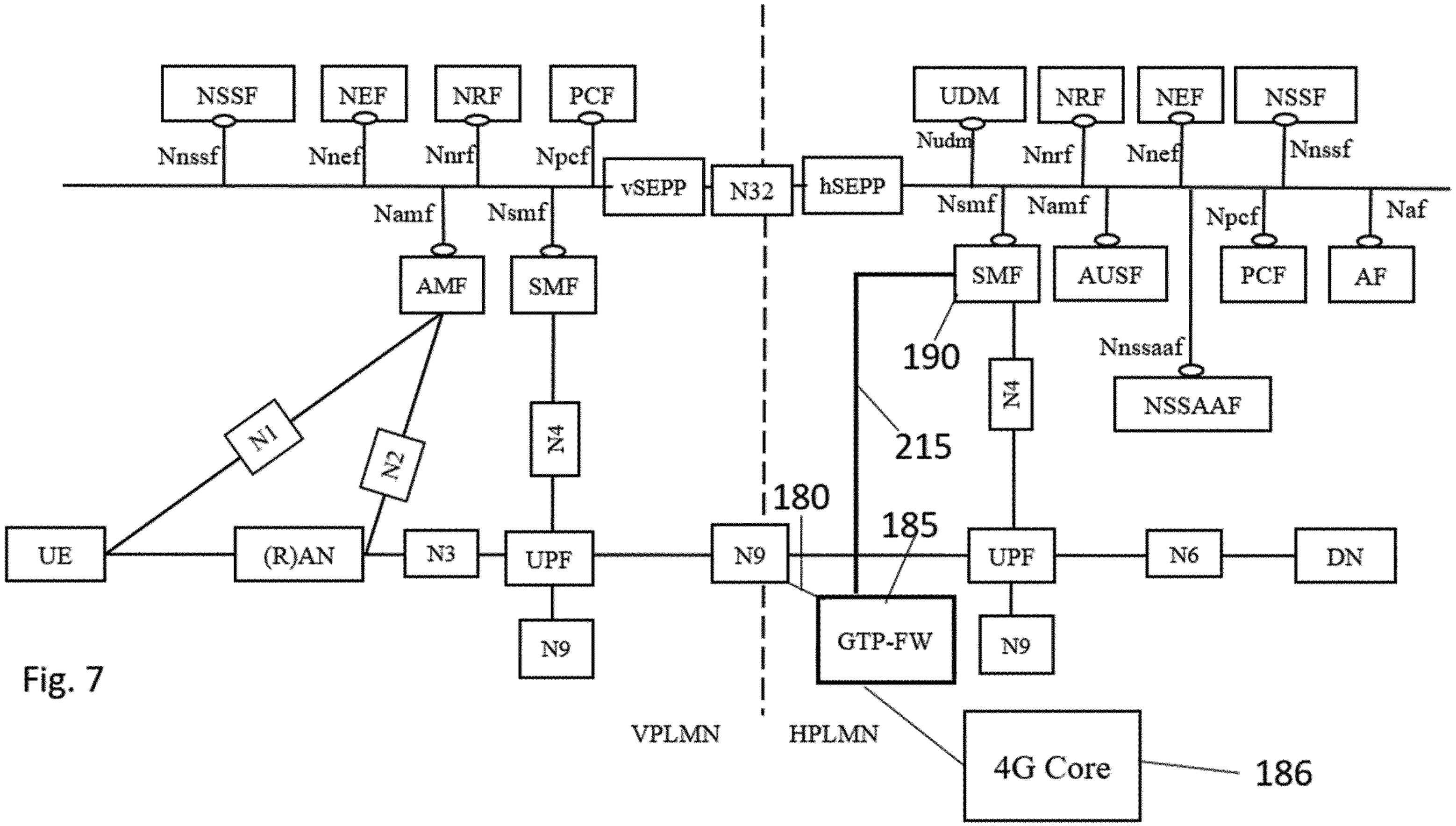

NSSF
NEF
NRF
PCF
Nnssf
Nnef
Nnrf
Npcf
Namf
Nsmf
AMF
SMF
vSEPP
N32
hSEPP
UDM
NRF
NEF
NSSF
Nudm
Nnrf
Nnef
Nnssf
Nsmf
Namf
Npcf
Naf
SMF
AUSF
PCF
AF
Nnssaaf
NSSAAF
190
215
N1
N2
N4
N4
180
185
UE
(R)AN
N3
UPF
N9
UPF
N6
DN
N9
GTP-FW
N9
VPLMN
HPLMN
4G Core
186

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/065341

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/12
ADD. H04W36/14 H04W88/16

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W 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)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2020/148330 A1 (NOKIA SOLUTIONS & NETWORKS OY [FI]) 23 July 2020 (2020-07-23) cited in the application paragraphs [0003], [0007], [0100], [0115] -----	1-15
A	GSM ASSOCIATION, GSM ASSOCIATION, GSMA FLOOR2 THE WALBROOK BUILDING 25 WALLBROOK LONDON, UK, 10 June 2021 (2021-06-10), XP040721009, paragraphs [7.6.1], [7.6.3], [7.6.3.2] ----- -/--	1-15

☒ 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 16 September 2022	Date of mailing of the international search report 28/09/2022
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Rüschmann, Frank

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GSMA: "Diameter IPX Network End-to-End Security Solution", 3GPP DRAFT; S3-191845 DESS31_05 LS TO 3GPP SA3 TO REVIEW DIAMETER SOLUTION - FINAL8, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTI , vol. SA WG3, no. Sapporo(Japan); 20190624 - 20190628 21 June 2019 (2019-06-21), XP051752794, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg%5Fsa/WG3%5FSecurity/TSGS3%5F95Bis%5FSapporo/Docs/S3%2D191845%2Ezip [retrieved on 2019-06-21] paragraphs [D.2.1], [D.3.3], [D3.3.3] -----	1-15
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects; Study on security aspects of the 5G Service Based Architecture (SBA) (Release 16)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 33.855, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V16.1.0 25 September 2020 (2020-09-25), pages 1-103, XP051961171, Retrieved from the Internet: URL:ftp://ftp.3gpp.org/Specs/archive/33_series/33.855/33855-g10.zip 33855-g10.doc [retrieved on 2020-09-25] paragraph [4.1.17.1] ----- -/--	1-15

1

International application No
PCT/EP2022/065341

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"3 Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 16)", 3GPP STANDARD; TECHNICAL SPECIFICATION; 3GPP TS 33.501, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG3, no. V16.6.0 6 April 2021 (2021-04-06), pages 1-254, XP052000594, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/33_series/33.501/33501-g60.zip 33501-g60_clean.doc [retrieved on 2021-04-06] paragraphs [5.9.2.3], [08.3], [09.5], [0013] -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2022/065341

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2020148330 A1	23-07-2020	EP 3912321 A1	24-11-2021
		US 2022124501 A1	21-04-2022
		WO 2020148330 A1	23-07-2020