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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2024 (12.12.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/251405 A1

(51) International Patent Classification:
H04W 76/12 (2018.01) *H04L 12/46* (2006.01)

(21) International Application Number:
PCT/EP2024/057598

(22) International Filing Date:
21 March 2024 (21.03.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20240100075 05 February 2024 (05.02.2024) GR

(71) Applicant: LENOVO (SINGAPORE) PTE. LTD. [SG/SG]; 151, Lorong Chuan #02-01, New Tech Park, Singapore 556741 (SG).

(72) Inventor: SALKINTZIS, Apostolis; 3 Rethimnou St Glika Nera, 15354 Athens (GR).

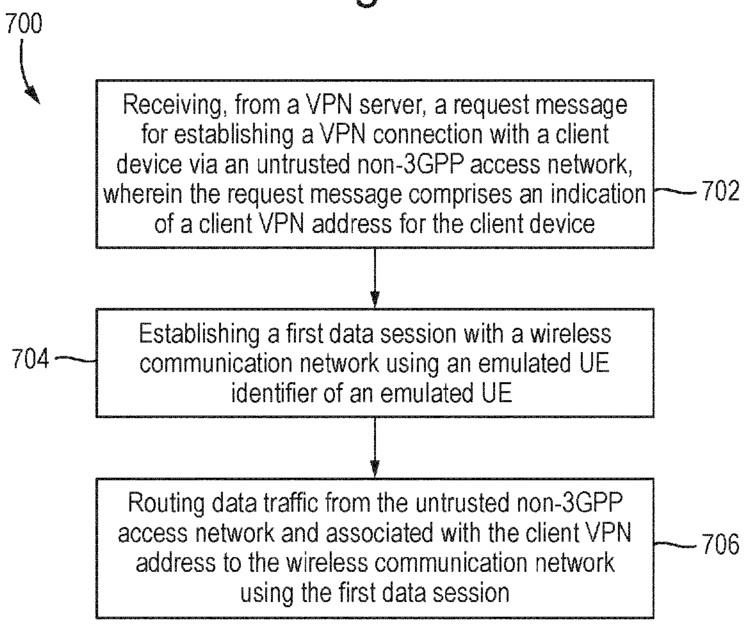
(74) Agent: OPENSHAW & CO.; 8 Castle Street, Farnham Surrey GU9 7HR (GB).

(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, CV, 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, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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,

(54) Title: NETWORK FUNCTION IN A WIRELESS COMMUNICATION NETWORK

Fig. 7



(57) Abstract: Various aspects of the present disclosure relate to a network function for wireless communication, comprising: at least one memory; and at least one processor coupled with the at least one memory and configured to cause the network function to: receive, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

WO 2024/251405 A1

[Continued on next page]

DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
— *upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)*

NETWORK FUNCTION IN A WIRELESS COMMUNICATION NETWORK

TECHNICAL FIELD

[0001] The subject matter disclosed herein relates generally to the field of network functions. In particular, this document defines a network function for wireless communication, a processor for wireless communication and a method performed by a network function.

BACKGROUND

[0002] A wireless communications system may include one or multiple network communication devices, such as base stations, which may support wireless communications for one or multiple user communication devices, which may be otherwise known as user equipment (UE), or other suitable terminology. The wireless communications system may support wireless communications with one or multiple user communication devices by utilizing resources of the wireless communication system (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers, or the like). Additionally, the wireless communications system may support wireless communications across various radio access technologies including third generation (3G) radio access technology, fourth generation (4G) radio access technology, fifth generation (5G) radio access technology, among other suitable radio access technologies beyond 5G (e.g., sixth generation (6G)).

SUMMARY

[0003] An article “a” before an element is unrestricted and understood to refer to “at least one” of those elements or “one or more” of those elements. The terms “a,” “at least one,” “one or more,” and “at least one of one or more” may be interchangeable. As used herein, including in the claims, “or” as used in a list of items (e.g., a list of items prefaced by a phrase such as “at least one of” or “one or more of” or “one or both of”) indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase “based on” shall not be construed as a reference to a closed set of conditions. For example, an example step that is described as “based on condition A” may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase “based on” shall be construed in the same manner as the phrase “based at least in part on. Further, as used herein, including in the claims, a “set” may include one or more elements.

[0004] There is provided a network function for wireless communication, comprising: at least one memory; and at least one processor coupled with the at least one memory and configured to cause the network function to: receive, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0005] The is further provided a processor for wireless communication, comprising: at least one controller coupled with at least one memory and configured to cause the processor to: receive, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0006] There is further provided a method performed by a network function, the method comprising: receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Figure 1 illustrates an example of a wireless communications system in accordance with aspects of the present disclosure.

[0008] Figure 2 is a network diagram illustrating devices in a wireless communication network in accordance with aspects of the present disclosure.

[0009] Figure 3 is a signalling diagram illustrating a method performed by devices in a wireless communication network in accordance with aspects of the present disclosure.

[0010] Figure 4 illustrates an example of a user equipment (UE) 400 in accordance with aspects of the present disclosure.

[0011] Figure 5 illustrates an example of a processor 500 in accordance with aspects of the present disclosure.

[0012] Figure 6 illustrates an example of a network entity (NE) 600 in accordance with aspects of the present disclosure.

[0013] Figure 7 illustrates a flowchart of a method performed by a NE in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0014] User devices (also referred to as "User Equipment") may connect to a fifth Generation (5G) mobile network, not only via third Generation Partnership Project (3GPP) access networks (such as Next-Generation Radio Access Network NG-RAN), but also via trusted and untrusted non-3GPP access networks. devices using non-3GPP access to connect to a 5G mobile network include:

- Devices that can support the 5G Non Access Stratum (NAS) protocol over non-3GPP access. Such devices may connect to a 5G core network via a Non-3GPP Interworking Function (N3IWF), when they are connected to an untrusted non-

3GPP access network, or via a Trusted Non-3GPP Gateway Function (TNGF), when they are connected to a trusted non-3GPP access network.

- Devices that cannot support the 5G NAS protocol over non-3GPP access. According to the current 3GPP specifications, such devices may connect to a 5G core network only via a trusted Wireless Local Area Network (WLAN) access network. For this purpose, a Trusted WLAN Interworking Function (TWIF) is specified in 3GPP TS 23.501 V18.4.0, title “System architecture for the 5G System (5GS); Stage 2” and the devices are referred to as "Non 5G Capable over WLAN" (N5CW) devices. However, the current 3GPP specifications do not define how devices that cannot support the 5G NAS protocol over non-3GPP access connect to a 5G core network via an untrusted non-3GPP access network. Such devices may be referred to as client devices.

[0015] The lack of a standardized mechanism to enable client devices that cannot support the 5G NAS protocol over non-3GPP access to connect to a 5G core network via an untrusted non-3GPP access tends to limit the range of scenarios where 5G services can be utilized. This is because, in most practical cases, client devices that are incapable of supporting the 5G NAS protocol over non-3GPP access (e.g., laptops, Internet of Things (IoT) devices, and other equipment) may be connected to untrusted non-3GPP access networks, such as public hotspots in airports, malls, coffee shops, etc.

[0016] Aspects of the present disclosure are described in the context of a wireless communications system.

[0017] Figure 1 illustrates an example of a wireless communications system 100 in accordance with aspects of the present disclosure. The wireless communications system 100 may include one or more NE 102, one or more UE 104, and a core network (CN) 106. The wireless communications system 100 may support various radio access technologies. In some implementations, the wireless communications system 100 may be a 4G network, such as an LTE network or an LTE-Advanced (LTE-A) network. In some other implementations, the wireless communications system 100 may be a NR network, such as a 5G network, a 5G-Advanced (5G-A) network, or a 5G ultrawideband (5G-UWB) network. In other implementations, the wireless communications system 100 may be a combination of a 4G network and a 5G network, or other suitable radio access technology including Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20. The wireless communications system 100 may support radio access technologies beyond 5G, for example, 6G. Additionally, the wireless communications system 100 may support technologies, such as time division multiple access (TDMA), frequency division multiple access (FDMA), or code division multiple access (CDMA), etc.

[0018] The one or more NE 102 may be dispersed throughout a geographic region to form the wireless communications system 100. One or more of the NE 102 described herein may be or include or may be referred to as a network node, a base station, a network element, a network function, a network entity, a radio access network (RAN), a NodeB, an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. An NE 102 and a UE 104 may communicate via a communication link, which may be a wireless or wired connection. For example, an NE 102 and a UE 104 may perform wireless communication (e.g., receive signalling, transmit signalling) over a Uu interface.

[0019] An NE 102 may provide a geographic coverage area for which the NE 102 may support services for one or more UEs 104 within the geographic coverage area. For example, an NE 102 and a UE 104 may support wireless communication of signals related to services (e.g., voice, video, packet data, messaging, broadcast, etc.) according to one or multiple radio access technologies. In some implementations, an NE 102 may be moveable, for example, a satellite associated with a non-terrestrial network (NTN). In some implementations, different geographic coverage areas associated with the same or different radio access technologies may overlap, but the different geographic coverage areas may be associated with different NE 102.

[0020] The one or more UE 104 may be dispersed throughout a geographic region of the wireless communications system 100. A UE 104 may include or may be referred to as a remote unit, a mobile device, a wireless device, a remote device, a subscriber device, a transmitter device, a receiver device, or some other suitable terminology. In some implementations, the UE 104 may be referred to as a unit, a station, a terminal, or a client, among other examples. Additionally, or alternatively, the UE 104 may be referred to as an

Internet-of-Things (IoT) device, an Internet-of-Everything (IoE) device, or machine-type communication (MTC) device, among other examples.

[0021] A UE 104 may be able to support wireless communication directly with other UEs 104 over a communication link. For example, a UE 104 may support wireless communication directly with another UE 104 over a device-to-device (D2D) communication link. In some implementations, such as vehicle-to-vehicle (V2V) deployments, vehicle-to-everything (V2X) deployments, or cellular-V2X deployments, the communication link may be referred to as a sidelink. For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0022] An NE 102 may support communications with the CN 106, or with another NE 102, or both. For example, an NE 102 may interface with other NE 102 or the CN 106 through one or more backhaul links (e.g., S1, N2, N2, or network interface). In some implementations, the NE 102 may communicate with each other directly. In some other implementations, the NE 102 may communicate with each other or indirectly (e.g., via the CN 106. In some implementations, one or more NE 102 may include subcomponents, such as an access network entity, which may be an example of an access node controller (ANC). An ANC may communicate with the one or more UEs 104 through one or more other access network transmission entities, which may be referred to as a radio heads, smart radio heads, or transmission-reception points (TRPs).

[0023] The CN 106 may support user authentication, access authorization, tracking, connectivity, and other access, routing, or mobility functions. The CN 106 may be an evolved packet core (EPC), or a 5G core (5GC), which may include a control plane entity that manages access and mobility (e.g., a mobility management entity (MME), an access and mobility management functions (AMF)) and a user plane entity that routes packets or interconnects to external networks (e.g., a serving gateway (S-GW), a Packet Data Network (PDN) gateway (P-GW), or a user plane function (UPF)). In some implementations, the control plane entity may manage non-access stratum (NAS) functions, such as mobility, authentication, and bearer management (e.g., data bearers, signal bearers, etc.) for the one or more UEs 104 served by the one or more NE 102 associated with the CN 106.

[0024] The CN 106 may communicate with a packet data network over one or more backhaul links (e.g., via an S1, N2, N2, or another network interface). The packet data network may include an application server. In some implementations, one or more UEs 104 may communicate with the application server. A UE 104 may establish a session (e.g., a protocol data unit (PDU) session, or the like) with the CN 106 via an NE 102. The CN 106 may route traffic (e.g., control information, data, and the like) between the UE 104 and the application server using the established session (e.g., the established PDU session). The PDU session may be an example of a logical connection between the UE 104 and the CN 106 (e.g., one or more network functions of the CN 106).

[0025] In the wireless communications system 100, the NEs 102 and the UEs 104 may use resources of the wireless communications system 100 (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers)) to perform various operations (e.g., wireless communications). In some implementations, the NEs 102 and the UEs 104 may support different resource structures. For example, the NEs 102 and the UEs 104 may support different frame structures. In some implementations, such as in 4G, the NEs 102 and the UEs 104 may support a single frame structure. In some other implementations, such as in 5G and among other suitable radio access technologies, the NEs 102 and the UEs 104 may support various frame structures (i.e., multiple frame structures). The NEs 102 and the UEs 104 may support various frame structures based on one or more numerologies.

[0026] One or more numerologies may be supported in the wireless communications system 100, and a numerology may include a subcarrier spacing and a cyclic prefix. A first numerology (e.g., μ=0) may be associated with a first subcarrier spacing (e.g., 15 kHz) and a normal cyclic prefix. In some implementations, the first numerology (e.g., μ=0) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., μ=1) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., μ=2) may be associated with a third subcarrier spacing (e.g., 60 kHz) and a normal cyclic prefix or an extended cyclic prefix. A fourth numerology (e.g., μ=3) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., μ=4) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix.

[0027] A time interval of a resource (e.g., a communication resource) may be organized according to frames (also referred to as radio frames). Each frame may have a duration, for example, a 10 millisecond (ms) duration. In some implementations, each frame may include multiple subframes. For example, each frame may include 10 subframes, and each subframe may have a duration, for example, a 1 ms duration. In some implementations, each frame may have the same duration. In some implementations, each subframe of a frame may have the same duration.

[0028] Additionally or alternatively, a time interval of a resource (e.g., a communication resource) may be organized according to slots. For example, a subframe may include a number (e.g., quantity) of slots. The number of slots in each subframe may also depend on the one or more numerologies supported in the wireless communications system 100. For instance, the first, second, third, fourth, and fifth numerologies (i.e., μ=0, μ=1, μ=2, μ=3, μ=4) associated with respective subcarrier spacings of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz may utilize a single slot per subframe, two slots per subframe, four slots per subframe, eight slots per subframe, and 16 slots per subframe, respectively. Each slot may include a number (e.g., quantity) of symbols (e.g., OFDM symbols). In some implementations, the number (e.g., quantity) of slots for a subframe may depend on a numerology. For a normal cyclic prefix, a slot may include 14 symbols. For an extended cyclic prefix (e.g., applicable for 60 kHz subcarrier spacing), a slot may include 12 symbols. The relationship between the number of symbols per slot, the number of slots per subframe, and the number of slots per frame for a normal cyclic prefix and an extended cyclic prefix may depend on a numerology. It should be understood that reference to a first numerology (e.g., μ=0) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[0029] In the wireless communications system 100, an electromagnetic (EM) spectrum may be split, based on frequency or wavelength, into various classes, frequency bands, frequency channels, etc. By way of example, the wireless communications system 100 may support one or multiple operating frequency bands, such as frequency range designations

FR1 (410 MHz – 7.125 GHz), FR2 (24.25 GHz – 52.6 GHz), FR3 (7.125 GHz – 24.25 GHz), FR4 (52.6 GHz – 114.25 GHz), FR4a or FR4-1 (52.6 GHz – 71 GHz), and FR5 (114.25 GHz – 300 GHz). In some implementations, the NEs 102 and the UEs 104 may perform wireless communications over one or more of the operating frequency bands. In some implementations, FR1 may be used by the NEs 102 and the UEs 104, among other equipment or devices for cellular communications traffic (e.g., control information, data). In some implementations, FR2 may be used by the NEs 102 and the UEs 104, among other equipment or devices for short-range, high data rate capabilities.

[0030] FR1 may be associated with one or multiple numerologies (e.g., at least three numerologies). For example, FR1 may be associated with a first numerology (e.g., μ=0), which includes 15 kHz subcarrier spacing; a second numerology (e.g., μ=1), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., μ=2), which includes 60 kHz subcarrier spacing. FR2 may be associated with one or multiple numerologies (e.g., at least 2 numerologies). For example, FR2 may be associated with a third numerology (e.g., μ=2), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., μ=3), which includes 120 kHz subcarrier spacing.

[0031] In the realm of wireless communication, there exists a category of access networks utilizing technologies that are not specified by the 3rd Generation Partnership Project (3GPP), commonly referred to as non-3GPP access networks. These networks may encompass Wireless Local Area Networks (WLANs) or fixed broadband access networks. A non-3GPP access network may be either "trusted" or "untrusted".

[0032] A non-3GPP access network may be deemed "untrusted" if it falls outside the mobile operator's domain of control. Common examples of such untrusted non-3GPP access networks may include the WLAN hotspots found in public spaces like airports, malls, and coffee shops. These hotspots are widely available and provide connectivity convenience but do not offer the security and service quality assurances that a 5G network would.

[0033] A non-3GPP access network may be deemed "trusted" if it is deployed and managed either directly by the mobile operator or by a partner organization that the mobile operator trusts. This trust may be established based on the security, reliability, and control that the mobile operator has over the network, ensuring that the services provided meet the operator's standards for network integrity and user data protection.

[0034] A N3IWF function defined in 3GPP specifications may enable devices that support the 5G NAS protocol over non-3GPP access to connect to a 5G core network.

[0035] A TWIF function defined in 3GPP specifications may be used over “trusted” non-3GPP access and is for connection to trusted non-3GPP access points (TNAPs). In addition, each user device connected to the TWIF will typically support both Universal Subscriber Identity Module (USIM) and Extensible Authentication Protocol-Authentication and Key Agreement’ (EAP-AKA) authentication.

[0036] Examples described herein may relate to enabling client devices that are not capable of supporting the 5G NAS protocol over non-3GPP access networks to connect to a 5G core network via untrusted non-3GPP access networks.

[0037] The client devices are not capable of supporting the 5G NAS protocol over non-3GPP access networks may be referred to as “Non-5G Capable over Non-3GPP access” (N5CN3) devices.

[0038] Examples described herein may relate to a network function. In some examples, the network function may be a non-3GPP Interworking Function-X (N3IWF-X). Examples described herein may relate to a network function which allows client devices to establish a secure and reliable connection to a 5G network through commonly available untrusted non-3GPP access points. In some examples, such a network function may be referred to as a N3IWF-X. In some examples, the N3IWF-X acts as an intermediary, emulating the behaviour of a 5G-capable User Equipment (UE) on behalf of the client device, by exposing the common N2/N3 interfaces towards the 5G core network and by facilitating Registration and a Protocol Data Unit (PDU) session establishment on behalf of the client devices. In some examples, the client device may be an N5CN3 device.

[0039] By implementing N3IWF-X, a wide array of client devices, including laptops and Internet of Things (IoT) devices, gain the capability to access 5G-specific services such as IP Multimedia Subsystem (IMS) and other operator-exclusive offerings, which were previously inaccessible through untrusted networks. This advancement significantly broadens the applicability and reach of 5G services, extending them to scenarios and environments where only untrusted non-3GPP access is available.

[0040] The network function described herein, which may be embodied in an N3IWF-X, tends to provide a significant enhancement over a conventional Trusted WLAN Interworking Function (TWIF). In some examples, the described network function tends to not restrict the connectivity to operator-managed or trusted networks. Indeed, the network function described herein has the potential to open a new avenue for 5G network utilization across a vast and untapped landscape of untrusted network environments.

[0041] Examples described herein may relate to a network function, which may be a N3IWF-X, and which facilitates the connection of one or more client devices to a wireless communication network. Examples described herein may relate to a new network function, N3IWF-X, which facilitates the connection of Non-5G Capable over Non-3GPP access (N5CN3) devices to a 5G core network (5GC) via untrusted non-3GPP access networks.

[0042] Figure 2 is a network diagram 200 illustrating devices in a wireless communication network in accordance with aspects of the present disclosure.

[0043] The network diagram 200 comprises the following devices: a first client device 210, a second client device 212, the first client device 210 and second client device 212 have each established a Virtual Private Network (VPN) connection to a VPN server 232 via an untrusted non-3GPP access network 220, labelled VPN Tunnel 1 and a VPN Tunnel 2 respectively. The VPN Server 232 is connected to a N3IWF-X 234. The N3IWF-X 234 is connected to a 5G Core (5GC) 240 via an N2/N3 connection. The 5GC 240 is connected to 5G Services 242. The 5G Services may include IP Multimedia Subsystem (IMS). The untrusted non-3GPP access network may be a WLAN. The first client device 210 may be a Non-5G Capable over Non-3GPP (N5CN3) device. The second client device 212 may be a N5CN3 device.

[0044] In some examples, the N3IWF-X 234 is collocated with the VPN Server 232. In some examples the N3IWF-X 234 is collocated with an Access Node (not shown). In some examples the N3IWF-X 234 is collocated with the VPN Server 232 and is collocated with the Access Node (not shown). In some examples the N3IWF-X 234 is a N3IWF 234. In some examples the N3IWF-X 234 is an N3IWF-X App 234.

[0045] In some examples, the N3IWF-X 234 comprises three collocated functionalities (VPN Server 232, N3IWF-X app 234, Access Node (not shown)); as indicated by the dashed box in Figure 2. The VPN Server 232, N3IWF-X app 234, Access Node (not shown) may not be collocated.

[0046] In some examples, each time a client device 210, 212 connects to the VPN server 232, an emulated UE instance is created. This emulated UE may automatically register to 5GC and establish a PDU Session. All data traffic relating to the first client device 210 and second client device 212 may then be routed via the established PDU Session. Multiple client devices 210, 212 may be supported simultaneously, each one may be associated with a different emulated UE instance and a different PDU Session.

[0047] Figure 3 is a signalling diagram illustrating a method 300 performed by devices in a wireless communication network in accordance with aspects of the present disclosure.

[0048] The method 300 is performed by the following devices: a client device 310, an untrusted non-3GPP access network 320, a VPN server 332, an N3IWF-X 334, an Access Node 336 and a 5G Core (5GC) 340.

[0049] In some examples, the N3IWF-X 334 is collocated with the VPN Server 332. In some examples the N3IWF-X 334 is collocated with an Access Node 336. In some examples, the N3IWF-X 334 is collocated with the VPN Server 332 and is collocated with the Access Node 336; as indicated by the dashed box in Figure 3. In some examples the N3IWF-X 334 is a N3IWF. In some examples the N3IWF-X 334 is an N3IWF-X App 334.

[0050] In some examples, the N3IWF-X 334 comprises three collocated functionalities (VPN Server 332, N3IWF-X app 334, Access Node 336); as indicated by the dashed box in Figure 3. In some examples, the VPN Server 332, N3IWF-X app 334, Access Node 336 may not be collocated.

[0051] The method starts at step 371, the client device 310 may be a N5CN3 device 310. In some examples, the N5CN3 device 310 connects to the untrusted non-3GPP access network 320 and obtains Internet Protocol (IP) connectivity. The N5CN3 device 310 may receives IP configuration data including an IP address.

[0052] In step 372, the N5CN3 device 310 may discover the IP address of the N3IWF-X 334. The N3IWF-X 334 may provide 5G connectivity to a specific Public Land Mobile Network (PLMN). The PLMN may provide the 5G Services. In some examples, the N5CN3 device 310 may be configured with the identity of the PLMN. The identify of the PLMN may comprise a Mobile Country Code (MCC). The identify of the PLMN may comprise a Mobile Network Code (MNC).

[0053] In some examples, discovering the IP address of the N3IWF-X 334, the N5CN3 device 310 may use a Domain Name System (DNS). In some examples, discovering the IP address of the N3IWF-X 334 may comprise the N5CN3 device 310 transmitting a DNS query.

[0054] In some examples, the N5CN3 device 310 may transmit a DNS query to resolve a domain name. In some examples, the domain name may be a N3IWF-X domain name. In some examples, an N3IWF-X domain name may be "n3iwfx.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"; where the MCC, MNC is the identity of the specific PLMN. The N3IWF-X domain name may be different from a conventional domain name used by a conventional N3IWF. For example, a conventional domain name may be "n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org". The N3IWF-X domain name may indicate that the N5CN3 device 310 want to discover the address information of an N3IWF-X 334, not a conventional N3IWF.

[0055] Alternatively, if the N5CN3 device 310 support 3GPP access (e.g., New Radio (NR) access) and is registered to the same PLMN through 3GPP access, the N5CN3 device 310 may attempt to discover an N3IWF-X 334 near to its present location area. An N3IWF-X 334 deployed near to the location are of the N5CN3 device 310 may provide a higher quality VPN connection compared to other N3IWF-X devices. For example, a higher quality VPN connection may comprise reduced latency or packet error rate compared to other N3IWF-X devices. In this case, the N5CN3 device 310 may transmit a DNS query to resolve the domain name: "tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.n3iwf-x.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" where the TAC-low-byte and the

TAC-high-byte indicate the Tracking Area Code (TAC) of the area which the device is register in via 3GPP access.

[0056] In step 373a, the N5CN3 device 310 initiates a VPN connection to the discovered N3IWF-X function 334. The VPN technology used can be any appropriate technology, including e.g., Internet Key Exchange (IKE)v2, OpenVPN, Transport Layer Security (TLS), Secure Sockets Layer (SSL), etc. The VPN connection is terminated to a VPN server 332 function, which may be located inside the N3IWF-X 334, as indicated by the dashed box in Figure 3, or can be standalone and outside the N3IWF-X 334.

[0057] In step 373b, during the VPN connection establishment, an authentication procedure is triggered wherein the VPN server 332 and the N5CN3 device 310 are mutually authenticated. This authentication may be based on certificates which are exchanged between the VPN server 332 and the N5CN3 device 310, on common keys which are preconfigured on VPN server 332 and the N5CN3 device 310, or any other appropriate credentials.

[0058] In step 374, after the authentication is successfully executed, but before the VPN connection is fully established, the VPN server 332 assigns a VPN address to the N5CN3 device 310 and sends a connection request to the N3IWF-X 334. The connection request may comprise a request message. The request message may comprise a client identifier (id) for the N5CN3 device 310. The request message may comprise or further comprise a VPN address (client VPN address) for the N5CN3 device 310. When the VPN server 332 is collocated with the N3IWF-X 334, the connection request may be sent to an application running inside the N3IWF-X 334 that implements the main N3IWF-X logic (e.g., a N3IWF-X App). When the VPN server 332 is not collocated outside the N3IWF-X 334, the connection request may be sent to the address of N3IWF-X 334, which may be preconfigured in the VPN server 332.

[0059] In step 375, the N3IWF-X 334 (or the N3IWF-X app) instantiates a new emulated User Equipment (UE) (not shown). This may involve emulating the operation of a UE device. The N3IWF-X 234 may be pre-configured with a list of emulated UEs, each one associated with a different VPN Client Id. When the N3IWF-X 334 receives the connection request, it may select to instantiate an emulated UE (out of the list of pre-configured emulated UEs) based on the received Client Id. Note that each emulated UE may be associated with configuration data that specifies the subscription data of the emulated UE, such as its permanent subscription identity (SUPI), credentials, default values for DNN, slices, etc.

[0060] In steps 376a to 376c, after the emulated UE is instantiated, it may initiate a standard 5G registration procedure with the 5GC (as shown in step 376b), followed by a Protocol Data Unit (PDU) Session Establishment procedure (as shown in step 376c). Both procedures may be executed between the emulated UE and an Access & Mobility Management Function (AMF) in 5GC 340 via an access node 336 (such as a next generation Node B (gNB)), which supports the standard N2/N3 interfaces. This access node 336 may be collocated with the N3IWF-X 334 or it may be non-collocated. In some examples, the access node 336 may be an emulated gNB implemented inside the N3IWF-X 334.

[0061] From the 5GC 340 point of view, the N3IWF-X 334 may be seen as initiating a 5G registration procedure and a PDU Session Establishment procedure on behalf of the N5CN3 device 310. This behaviour may be similar to the behaviour of TWIF as discussed in 3GPP TS 23.502 V18.4.0.

[0062] After the N3IWF-X 334 (or the N3IWF-X app 334) instantiates the emulated UE, it may monitor the operation of this emulated UE and determine when the 5G registration and the PDU Session Establishment procedures are completed. If they are successfully completed in a pre-configured period, the N3IWF-X 334 may proceed to step 377. Otherwise, the N3IWF-X 334 may send a Connection Rejected response to the VPN server 332, which then rejects the VPN connection with the N5CN3 device 310.

[0063] In step 377, once the N3IWF-X 334 determines that the PDU session is successfully established, the N3IWF-X 334 may configure its IP layer so that it routes all data traffic from the "Client VPN address" of the N5CN3 device 310 via the established PDU session. This kind of routing ensures that all uplink traffic received from the N5CN3 device 310 is sent through the established PDU Session and all downlink traffic received from the PDU Session is sent to the N5CN3 device 310.

[0064] Note that the N3IWF-X 334 may simultaneously support many N5CN3 devices 310, each one associated with a different emulated UE and with a different PDU Session.

[0065] In step 378a, after the N3IWF-X 334 successfully configures its IP layer, it may send a Connection Accepted message to VPN server 332.

[0066] In step 378b, the VPN Server 332 may complete the VPN connection with the N5CN3 device 310. This finalizes the VPN connection establishment and the association of the VPN connection with a PDU Session towards the 5G core network 340.

[0067] In step 379, after the N5CN3 device 310 successfully establishes the VPN connection, it starts sending (and receiving) IP packets via this VPN connection. The IP packets sent over the VPN connection are forwarded to the N3IWF-X (or N3IWF-X app) 334, which transmits them via the PDU session associated with the N5CN3 device 310 or, equivalently, with the VPN connection of the N5CN3 device 310.

[0068] The method 300 tends to allow for the seamless integration of N5CN3 devices 310 into the 5G ecosystem, providing them with the full suite of services offered by the 5GC 340, despite the devices' inherent limitations in supporting the 5G Non Access Stratum (NAS) protocol over non-3GPP access networks. The N3IWF-X function 334, therefore, enables the use of untrusted non-3GPP access networks 320 as a viable and secure medium for 5G service delivery, vastly expanding the coverage and accessibility of 5G networks.

[0069] Some examples described herein describe a N3IWF-X function which serves to substantially improve the interoperability of 5G networks with a broader range of user equipment, particularly in environments where trusted non-3GPP access is not available.

[0070] Figure 4 illustrates an example of a UE 400 in accordance with aspects of the present disclosure. The UE 400 may include a processor 402, a memory 404, a controller 406, and a transceiver 408. The processor 402, the memory 404, the controller 406, or the transceiver 408, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[0071] The processor 402, the memory 404, the controller 406, or the transceiver 408, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[0072] The processor 402 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 402 may be configured to operate the memory 404. In some other implementations, the memory 404 may be integrated into the processor 402. The processor 402 may be configured to execute computer-readable instructions stored in the memory 404 to cause the UE 400 to perform various functions of the present disclosure.

[0073] The memory 404 may include volatile or non-volatile memory. The memory 404 may store computer-readable, computer-executable code including instructions when executed by the processor 402 cause the UE 400 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such the memory 404 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[0074] In some implementations, the processor 402 and the memory 404 coupled with the processor 402 may be configured to cause the UE 400 to perform one or more of the functions described herein (e.g., executing, by the processor 402, instructions stored in the memory 404). For example, the processor 402 may support wireless communication at the UE 400 in accordance with examples as disclosed herein.

[0075] The controller 406 may manage input and output signals for the UE 400. The controller 406 may also manage peripherals not integrated into the UE 400. In some implementations, the controller 406 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 406 may be implemented as part of the processor 402.

[0076] In some implementations, the UE 400 may include at least one transceiver 408. In some other implementations, the UE 400 may have more than one transceiver 408. The transceiver 408 may represent a wireless transceiver. The transceiver 408 may include one or more receiver chains 410, one or more transmitter chains 412, or a combination thereof.

[0077] A receiver chain 410 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 410 may include one or more antennas for receive the signal over the air or wireless medium. The receiver chain 410 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 410 may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 410 may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[0078] A transmitter chain 412 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 412 may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmitter chain 412 may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmitter chain 412 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[0079] Figure 5 illustrates an example of a processor 500 in accordance with aspects of the present disclosure. The processor 500 may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 500 may include a controller 502 configured to perform various operations in accordance with examples as described herein. The processor 500 may optionally include at least one memory 504, which may be, for example, an L1/L2/L3 cache. Additionally, or alternatively, the processor 500 may optionally include one or more arithmetic-logic units (ALUs) 506. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0080] The processor 500 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor 500) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM (SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[0081] The controller 502 may be configured to manage and coordinate various operations (e.g., signalling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 500 to cause the processor 500 to support various operations in accordance with examples as described herein. For example, the controller 502 may operate as a control unit of the processor 500, generating control signals that manage the operation of various components of the processor 500. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0082] The controller 502 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 504 and determine subsequent instruction(s) to be executed to cause the processor 500 to support various operations in accordance with examples as described herein. The controller 502 may be configured to track memory address of instructions associated with the memory 504. The controller 502 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 502 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 500 to cause the processor 500 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 502 may be configured to manage flow of data within the processor 500. The controller 502 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 500.

[0083] The memory 504 may include one or more caches (e.g., memory local to or included in the processor 500 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementations, the memory 504 may reside within or on a processor chipset (e.g., local to the processor 500). In some other implementations, the memory 504 may reside external to the processor chipset (e.g., remote to the processor 500).

[0084] The memory 504 may store computer-readable, computer-executable code including instructions that, when executed by the processor 500, cause the processor 500 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 502 and/or the processor 500 may be configured to execute computer-readable instructions stored in the memory 504 to cause the processor 500 to perform various functions. For example, the processor 500 and/or the controller 502 may be coupled with or to the memory 504, the processor 500, the controller 502, and the memory 504 may be configured to perform various functions described herein. In some examples, the processor 500 may include multiple processors and the memory 504 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[0085] The one or more ALUs 506 may be configured to support various operations in accordance with examples as described herein. In some implementations, the one or more ALUs 506 may reside within or on a processor chipset (e.g., the processor 500). In some other implementations, the one or more ALUs 506 may reside external to the processor chipset (e.g., the processor 500). One or more ALUs 506 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 506 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 506 be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 506 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 506 to handle conditional operations, comparisons, and bitwise operations.

[0086] The processor 500 may support wireless communication in accordance with examples as disclosed herein. The processor 500 may be configured to or operable to support a means for receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0087] Figure 6 illustrates an example of a NE 600 in accordance with aspects of the present disclosure. The NE 600 may include a processor 602, a memory 604, a controller 606, and a transceiver 608. The processor 602, the memory 604, the controller 606, or the transceiver 608, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[0088] The processor 602, the memory 604, the controller 606, or the transceiver 608, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[0089] The processor 602 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 602 may be configured to operate the memory 604. In some other implementations, the memory 604 may be integrated into the processor 602. The processor 602 may be configured to execute computer-readable instructions stored in the memory 604 to cause the NE 600 to perform various functions of the present disclosure.

[0090] The memory 604 may include volatile or non-volatile memory. The memory 604 may store computer-readable, computer-executable code including instructions when executed by the processor 602 cause the NE 600 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such the memory 604 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[0091] In some implementations, the processor 602 and the memory 604 coupled with the processor 602 may be configured to cause the NE 600 to perform one or more of the functions described herein (e.g., executing, by the processor 602, instructions stored in the memory 604). For example, the processor 602 may support wireless communication at the NE 600 in accordance with examples as disclosed herein. The NE 600 may be configured to support a means for receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0092] The controller 606 may manage input and output signals for the NE 600. The controller 606 may also manage peripherals not integrated into the NE 600. In some implementations, the controller 606 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 606 may be implemented as part of the processor 602.

[0093] In some implementations, the NE 600 may include at least one transceiver 608. In some other implementations, the NE 600 may have more than one transceiver 608. The transceiver 608 may represent a wireless transceiver. The transceiver 608 may include one or more receiver chains 610, one or more transmitter chains 612, or a combination thereof.

[0094] A receiver chain 610 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 610 may include one or more antennas for receive the signal over the air or wireless medium. The receiver chain 610 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 610 may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 610 may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[0095] A transmitter chain 612 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 612 may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmitter chain 612 may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmitter chain 612 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[0096] Figure 7 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a Network Entity (NE) as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0097] At 702, the method may include receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device. The operations of 702 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 702 may be performed by a NE as described with reference to Figure 6.

[0098] At 704, the method may include establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE. The operations of 704 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 704 may be performed by a NE as described with reference to Figure 6.

[0099] At 706, the method may include routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session. The operations of 706 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 706 may be performed a NE as described with reference to Figure 6.

[0100] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0101] There is provided herein a network function for wireless communication, comprising: at least one memory; and at least one processor coupled with the at least one memory and configured to cause the network function to: receive, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0102] Such a network function enables connection between the client device and the wireless communication network via an untrusted non-third generation partnership project, non-3GPP, access network. Such a connection is enabled for a client device that cannot support the 5G NAS protocol over the non-3GPP access network.

[0103] The network function may be a Non-3GPP Interworking Function, N3IWF. The network function may be a 5G-Untrusted Interworking Function, 5G-UIF. The network function may be a Non-3GPP Access Bridge, N3AB. The network function may be a Universal 5G Access Gateway, U5G-AG. The network function may be an N3IWF-X. The network function may comprise an N3IWF-X application. The N3IWF-X application may be an N3IWF-X App. The network function may be collocated with the virtual private network, VPN, server. The network function may be collocated with an access node. The access node may be for accessing the wireless communication network. The network function may be an N3IWF-X App. The network function may be collocated with a VPN server, an N3IWF-X App, and an access node. The access node may be a next generation Node B, gNB. The access node may support the N2 and the N3 interfaces according to 3GPP standards.

[0104] The wireless communication network may be a public land mobile network, PLMN. The VPN connection may comprise one or more of Internet Key Exchange (IKE)v2, OpenVPN, Transport Layer Security (TLS) or Secure Sockets Layer (SSL). The untrusted non-3GPP access network may be a Wireless Local Area Network, WLAN. The untrusted non-3GPP access network may be a fixed broadband access network.

[0105] The client device may be a, Non-5G Capable over Non-3GPP access, N5CN3 device. The client device may connect to the untrusted non-3GPP access network. The client device may receive IP configuration data from the untrusted non-3GPP access network. The IP configuration data may include an IP address. The client device may not comprise a USIM. The client device may not be capable of communicating with the 5G network directly. The client device may not be configured to use a NAS protocol. The client device may not be configured to use a 5G NAS protocol.

[0106] The first data session may be a Protocol Data Unit, PDU, Session. Establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE may comprise establishing a PDU session with a wireless communication network using an emulated UE identifier of an emulated UE. The first data session may be established via an access node. The access node may be a Next Generation Node B, gNB.

[0107] The wireless communication network may be a fifth generation, 5G, network. The wireless communication network may comprise a 5G Core (5GC). The wireless communication network may comprise an Access & Mobility Management Function, AMF.

[0108] Data traffic associated with the client VPN address may be routed from the untrusted non-3GPP access network to the wireless communication network using the first data session established using the emulated UE identifier. Data traffic associated with the client VPN address may be routed to the untrusted non-3GPP access network from the wireless communication network using the first data session established using the emulated UE identifier. Data traffic associated with the client VPN address may be routed from the untrusted non-3GPP access network to the wireless communication network using the first data session established using the emulated UE identifier over the VPN connection. Data traffic associated with the client VPN address may be routed to the untrusted non-3GPP access network from the wireless communication network using the first data session established using the emulated UE identifier over the VPN connection. The data traffic may be routed over the VPN connection. The at least one processor coupled with the at least one memory may be further configured to cause the network function to: select the emulated UE from a list of pre-configured emulated UEs.

[0109] The at least one processor coupled with the at least one memory may be further configured to cause the network function to instantiate an emulated UE for each client device. The instantiating may be based on the client VPN address.
The request message may further comprise a second indication of a client identifier for the client device. The at least one processor coupled with the at least one memory may be further configured to cause the network function to: select the emulated UE based on the client identifier for the client device.

[0110] The at least one processor coupled with the at least one memory may be further configured to cause the network function to: send, to the VPN server, an accept message for accepting the VPN connection with the client device via the untrusted non-3GPP access network. The accept message may be sent in response to the first data session for the emulated UE being successfully established.

[0111] The at least one processor coupled with the at least one memory may be further configured to cause the network function to send, to the VPN server, a reject message to reject the VPN connection with the client device via the untrusted non-3GPP access network.

[0112] A domain name of the network function may indicate a capability to support one or more client devices to access to the wireless communication network via the untrusted non-3GPP access network.

[0113] The client device may require support from the network function to access the wireless communication network via the untrusted non-3GPP access network. The client device may require support from the network function to access the wireless communication network via the untrusted non-3GPP access network because the client device does not support 5G Non-Access Stratum (NAS) protocol. The client device may be incapable of directly accessing the wireless communication network over the untrusted non-3GPP access network because the client device does not support 5G Non-Access Stratum (NAS) protocol.

[0114] The client device may discover the IP address of the network function. The client device may discover the IP address of the network function by transmitting a Domain Name System (DNS) query message to a DNS server. The DNS query message may request resolution of the domain name of the network function. The domain name may further indicate the wireless communication network.

[0115] The at least one processor coupled with the at least one memory may be further configured to cause the network function to: register the emulated UE with the wireless communication network and to establish the first data session with the wireless communication network using the emulated UE identifier of the emulated UE.

[0116] The first data session may be used for data communication between the emulated UE and the wireless communication network.

[0117] The at least one processor coupled with the at least one memory may be further configured to cause the network function to: send, to the VPN server, a reject message for rejecting the VPN connection with the client device via the untrusted non-3GPP access network. The at least one processor coupled with the at least one memory may be further configured to cause the network function to: send, to the VPN server, a reject message for rejecting the VPN connection with the client device via the untrusted non-3GPP access network in response to a failure to establish the first data session with the wireless communication network using the emulated UE identifier of the emulated UE.

[0118] Registering the emulated UE with the wireless communication network may be performed after the emulated UE is instantiated. The registration may comprise a standard 5G registration procedure with the 5GC, followed by a Protocol Data Unit (PDU) Session Establishment procedure.

[0119] The network function may be collocated with the VPN server. The network function may be collocated with the VPN server in the same network entity. The network function may comprise the VPN server. The network function may be collocated with an access node. The network function may be collocated with the access node in the same network entity. The network function may comprise the access node. The network function may be collocated with the VPN server and the access node in the same network entity. The network function may comprise the VPN server and the access node.

[0120] The wireless communication network may be a 5G network. The client device may not be configured with the 5G NAS protocol. The client device may be such that the client device cannot support the 5G NAS protocol over untrusted non-3GPP access.

[0121] The is further provided a processor for wireless communication, comprising: at least one controller coupled with at least one memory and configured to cause the processor to: receive, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0122] Such a processor enables connection between the client device and the wireless communication network via an untrusted non-third generation partnership project, non-3GPP, access network. Such a connection is enabled for a client device that cannot support the 5G NAS protocol over the non-3GPP access network.

[0123] There is further provided a method performed by a network function, the method comprising: receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device; establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

[0124] Such a method enables connection between the client device and the wireless communication network via an untrusted non-third generation partnership project, non-3GPP, access network. Such a connection is enabled for a client device that cannot support the 5G NAS protocol over the non-3GPP access network.

[0125] The method may further comprise selecting the emulated UE from a list of pre-configured emulated UEs. The method may further comprise instantiating an emulated UE for each client device. The instantiating may be based on the client VPN address. The request message may further comprise a second indication of a client identifier for the client device. The method may further comprise selecting the emulated UE based on the client identifier for the client device.

[0126] The method may further comprise sending, to the VPN server, an accept message for accepting the VPN connection with the client device via the untrusted non-

3GPP access network. The accept message may be sent in response to the first data session for the emulated UE being successfully established.

[0127] The method may comprise sending, to the VPN server, a reject message to reject the VPN connection with the client device via the untrusted non-3GPP access network.

[0128] A domain name of the network function may indicate a capability to support one or more client devices to access to the wireless communication network via the untrusted non-3GPP access network.

[0129] The client device may require support from the network function to access the wireless communication network via the untrusted non-3GPP access network. The client device may require support from the network function to access the wireless communication network via the untrusted non-3GPP access network because the client device does not support 5G Non-Access Stratum (NAS) protocol. The client device may be incapable of directly accessing the wireless communication network over the untrusted non-3GPP access network because the client device does not support 5G Non-Access Stratum (NAS) protocol.

[0130] The client device may discover the IP address of the network function. The client device may discover the IP address of the network function by transmitting a Domain Name System (DNS) query message to a DNS server. The DNS query message may request resolution of the domain name of the network function. The domain name may further indicate the wireless communication network.

[0131] The method may further comprise registering the emulated UE with the wireless communication network. Registering the emulated UE with the wireless communication network may be performed after the emulated UE is instantiated. The method may further comprise registering the emulated UE with the wireless communication network and establishing the first data session with the wireless communication network using the emulated UE identifier of the emulated UE. The first data session may be used for data communication between the emulated UE and the wireless communication network. The registration may comprise a standard 5G registration procedure with the 5GC, followed by a Protocol Data Unit (PDU) Session Establishment procedure.

[0132] The method may further comprise sending, to the VPN server, a reject message for rejecting the VPN connection with the client device via the untrusted non-3GPP access network. The method may further comprise sending, to the VPN server, a reject message for rejecting the VPN connection with the client device via the untrusted non-3GPP access network in response to a failure to establish the first data session with the wireless communication network using the emulated UE identifier of the emulated UE.

[0133] The network function may be collocated with the VPN server. The network function may be collocated with the VPN server in the same network entity. The network function may be collocated with an access node. The network function may be collocated with the access node in the same network entity. The network function may be collocated with the VPN server and the access node in the same network entity.

[0134] The wireless communication network may be a 5G network. The client device may not be configured with the 5G NAS protocol. The client device may be such that the client device cannot support the 5G NAS protocol over untrusted non-3GPP access.

[0135] Some examples described herein may relate to a N3IWF-X network function enabling Non-5G Capable over Non-3GPP access (N5CN3) devices to seamlessly integrate into the 5G ecosystem via untrusted non-3GPP access networks.

[0136] There are described herein Discovery and Connectivity processes between a N5CN3 device and a N3IWF-X. Such processes may commence with an N5CN3 device connecting to an untrusted non-3GPP network and obtaining an IP address. The N5CN3 device may then discover the N3IWF-X using a unique domain naming convention that differentiates from standard/conventional N3IWF discovery, indicating a specific desire to connect to an N3IWF-X function tailored for N5CN3 devices.

[0137] Dedicated Emulated UE Instantiation: Upon receiving a VPN connection request, the N3IWF-X function instantiates a new emulated UE, uniquely associated with the N5CN3 device's VPN client ID. This instantiation is a critical novelty that enables each N5CN3 device to be represented within the 5G network by a distinct emulated UE.

[0138] There are further described herein Monitoring 5G Registration and PDU Session Establishment processes between a N5CN3 device and a N3IWF-X. The N3IWF-X may monitor the 5G registration and PDU session establishment procedures initiated by the emulated UE. If both procedures are successfully completed, the N3IWF-X may signal that the VPN connection with the N5CN3 device may be accepted. Otherwise, the N3IWF-X may signal that the VPN connection with the N5CN3 device may be rejected.

[0139] There are further described herein Associating VPN connection with PDU Session processes between a N5CN3 device and a N3IWF-X. The N3IWF-X may configure IP routing to ensure that the N5CN3 device's traffic is funnelled through the emulated UE's PDU session. This traffic routing may be indistinguishable from a 5G-capable device from the 5GC's perspective.

[0140] Some examples described herein may relate to Simultaneous Multi-Device Support by the N3IWF-X. The N3IWF-X may be capable to support multiple N5CN3 devices concurrently, each one associated with a separate emulated UE and distinct PDU session, thus providing scalable 5G access.

[0141] Some examples described herein may relate to Traffic Forwarding by the N3IWF-X. The N5CN3 device may transmit IP packets through the established VPN connection, which are appropriately routed through the associated PDU session by the N3IWF-X, enabling access to 5G services.

[0142] There is further provided a method for providing 5G network access to devices incapable of supporting 5G Non-Access Stratum (NAS) protocol over non-3GPP access networks, the method comprising: connecting the device to an untrusted non-3GPP access network and obtaining an IP address for the device; discovering an address of a network function (N3IWF-X) using a Domain Name System (DNS) query, where the network function is configured to facilitate access to a Public Land Mobile Network (PLMN); initiating a Virtual Private Network (VPN) connection between the device and the network function; optionally authenticating the device with the network function; instantiating, by the network function, an emulated User Equipment (UE) process associated with the device based on a VPN client identification; Performing a 5G registration and Protocol Data Unit (PDU) Session Establishment procedure between the emulated UE and a 5G core network; configuring IP routing within the network function to route traffic from the device's VPN address through the established PDU session; and completing the VPN connection to provide the device with access to the 5G services.

[0143] The network function (N3IWF-X) may be configured to support multiple devices simultaneously, each device associated with a distinct emulated UE and separate PDU session.

[0144] The VPN server function may be integrated within the network function (N3IWF-X).

[0145] There is further provided a network function apparatus (N3IWF-X) configured to facilitate connection of devices incapable of supporting 5G NAS protocol over non-3GPP access networks to a 5G core network, the apparatus comprising: a processor; a memory coupled to the processor, the memory storing instructions that, when executed by the processor, cause the apparatus to perform operations comprising: receiving a connection request from a device over a VPN; instantiating an emulated UE process for each device based on a client VPN address; performing a 5G registration procedure and establishing a PDU session for the emulated UE with a 5G core network; configuring IP routing to route the device's traffic through the established PDU session; completing the VPN connection to enable the device to access 5G network services.

[0146] The emulated UE may be configured to emulate 5G NAS signaling on behalf of the device to establish the PDU session with the 5G core network.

[0147] The apparatus may be further configured to route IP packets received from the device to a destination in the 5G core network through the established PDU session.

[0148] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0149] The description herein is provided to enable a person having ordinary skill in the art to make or use the disclosure. Various modifications to the disclosure will be apparent to a person having ordinary skill in the art, and the generic principles defined herein may be applied to other variations without departing from the scope of the disclosure. Thus, the disclosure is not limited to the examples and designs described herein but is to be accorded the broadest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A network function for wireless communication, comprising:

at least one memory; and

at least one processor coupled with the at least one memory and configured to cause the network function to:

receive, from a virtual private network, VPN, server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device;

establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and

route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

2. The network function according to claim 1, wherein the at least one processor coupled with the at least one memory is further configured to cause the network function to:

select the emulated UE from a list of pre-configured emulated UEs.

3. The network function according to claim 1 or 2, wherein the request message further comprises a second indication of a client identifier for the client device.

4. The network function according to claim 3, wherein the at least one processor coupled with the at least one memory is further configured to cause the network function to:

select the emulated UE based on the client identifier for the client device.

5. The network function according to any one of claims 1 to 4, wherein the at least one processor coupled with the at least one memory is further configured to cause the network function to:

send, to the VPN server, an accept message for accepting the VPN connection with the client device via the untrusted non-3GPP access network.

6. The network function according to any one of claims 1 to 5, wherein a domain name of the network function indicates a capability to support one or more client devices to access the wireless communication network via the untrusted non-3GPP access network.

7. The network function according to claim 6, wherein the domain name further indicates the wireless communication network.

8. The network function according to any one of claims 1 to 7, wherein the at least one processor coupled with the at least one memory is further configured to cause the network function to:

register the emulated UE with the wireless communication network; and

establish the first data session with the wireless communication network using the emulated UE identifier of the emulated UE.

9. The network function according to any one of claims 1 to 8, wherein the at least one processor coupled with the at least one memory is further configured to cause the network function to:

send, to the VPN server, a reject message for rejecting the VPN connection with the client device via the untrusted non-3GPP access network in response to a failure to establish the first data session with the wireless communication network using the emulated UE identifier of the emulated UE.

10. The network function according to any one of claims 1 to 9, wherein the network function is collocated with the VPN server.

11. The network function according to any one of claims 1 to 10, wherein the network function is collocated with an access node.

12. The network function of any one of claims 1 to 11, wherein the wireless communication network is a fifth generation, 5G, network.

13. The network function of claim 12, wherein the client device cannot support a 5G non-access stratum, NAS, protocol over the untrusted non-3GPP access.

14. A processor for wireless communication, comprising:

at least one controller coupled with at least one memory and configured to cause the processor to:

receive, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device;

establish a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and

route data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

15. A method performed by a network function, the method comprising:

receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device;

establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE; and

routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session.

16. The method according to claim 15, further comprising selecting the emulated UE from a list of pre-configured emulated UEs.

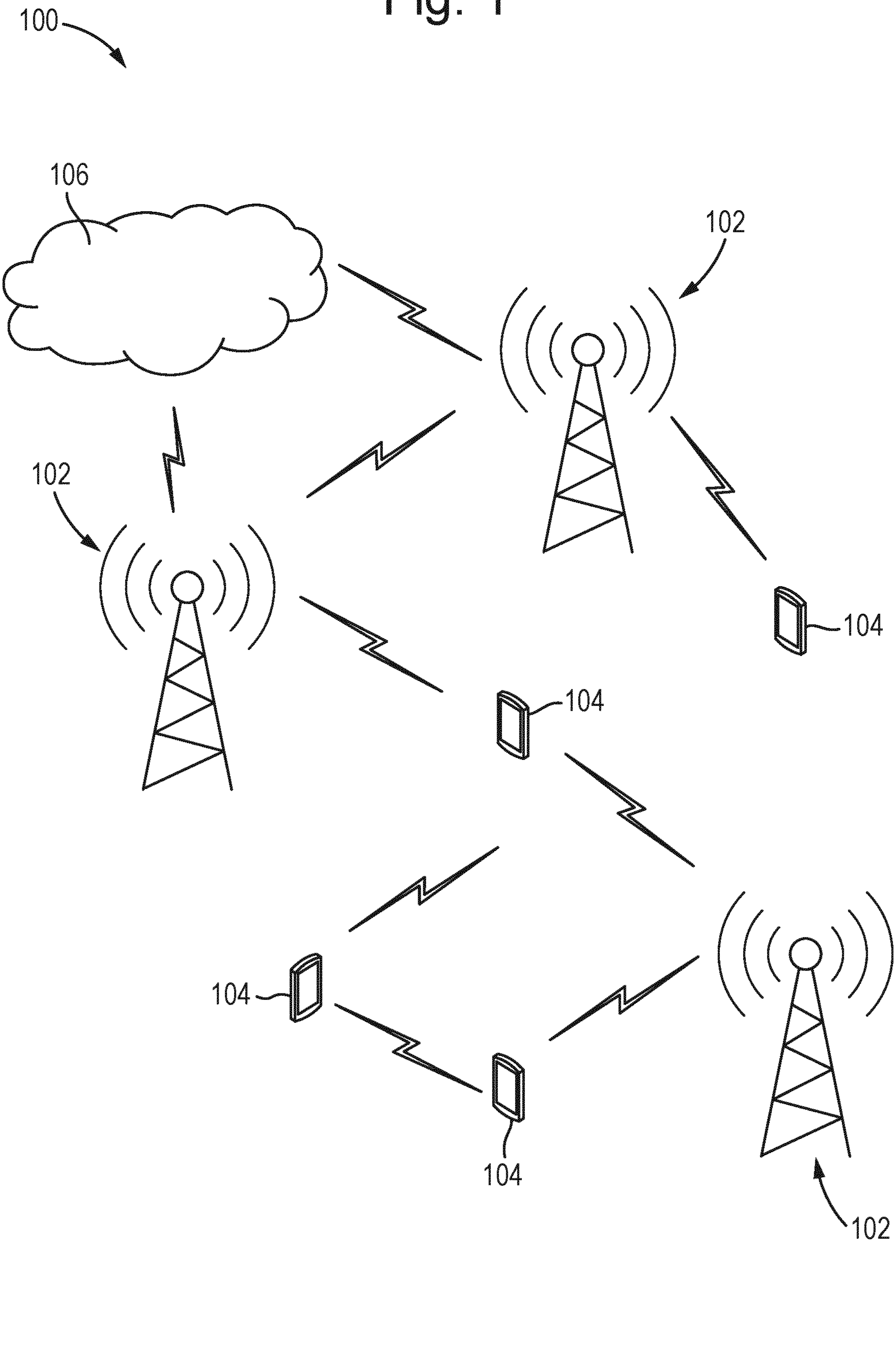
17. The method according to claim 15 or 16, wherein the request message further comprises a second indication of a client identifier for the client device.

18. The method according to claim 17, further comprising selecting the emulated UE based on the client identifier for the client device.

19. The method according to any one of claims 15 to 18, further comprising sending, to the VPN server, an accept message for accepting the VPN connection with the client device via the untrusted non-3GPP access network.

20. The method according to any one of claims 15 to 19, wherein a domain name of the network function indicates a capability to support one or more client devices to access to the wireless communication network via the untrusted non-3GPP access network.

Fig. 1



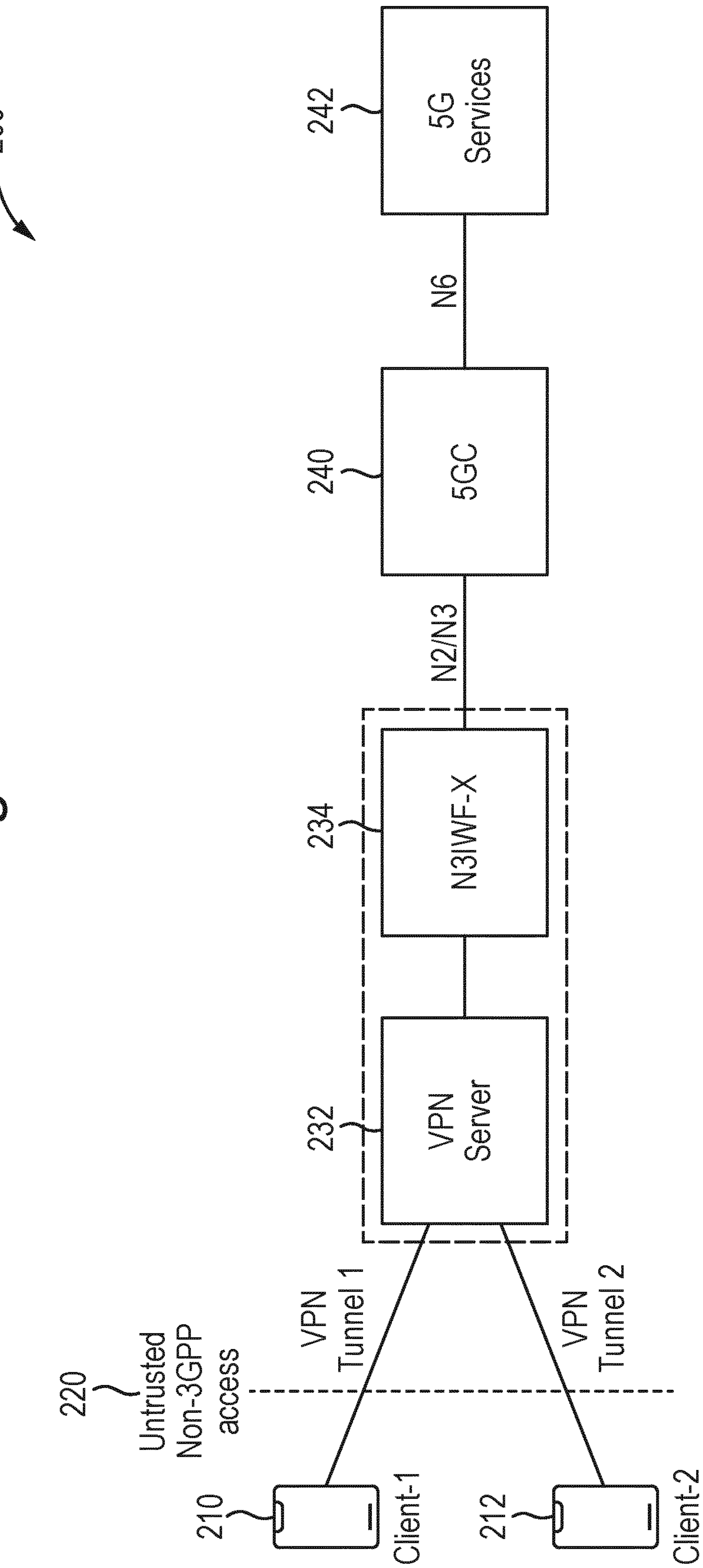

200
242
5G Services
N6
240
5GC
N2/N3
234
N3IWF-X
232
VPN Server
VPN Tunnel 1
VPN Tunnel 2
220
Untrusted Non-3GPP access
210
Client-1
212
Client-2

Fig. 2

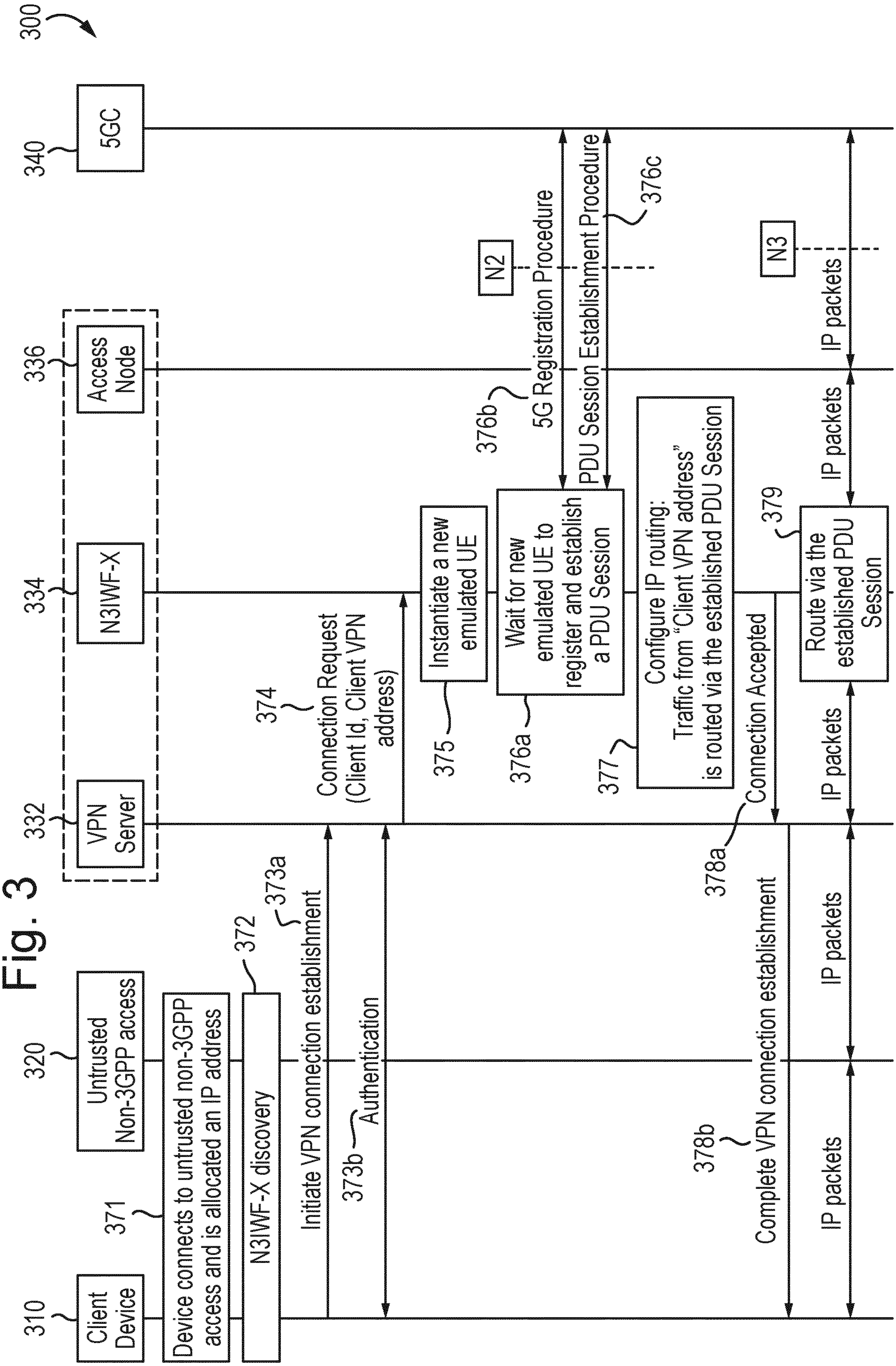

300
Client Device
310
Untrusted Non-3GPP access
320
VPN Server
332
N3IWF-X
334
Access Node
336
5GC
340
Device connects to untrusted non-3GPP access and is allocated an IP address
371
N3IWF-X discovery
372
Initiate VPN connection establishment
373a
Authentication
373b
Connection Request (Client Id, Client VPN address)
374
Instantiate a new emulated UE
375
Wait for new emulated UE to register and establish a PDU Session
376a
5G Registration Procedure
376b
PDU Session Establishment Procedure
376c
N2
Configure IP routing: Traffic from "Client VPN address" is routed via the established PDU Session
377
Connection Accepted
378a
Complete VPN connection establishment
378b
Route via the established PDU Session
379
IP packets
N3

Fig. 3

Fig. 4

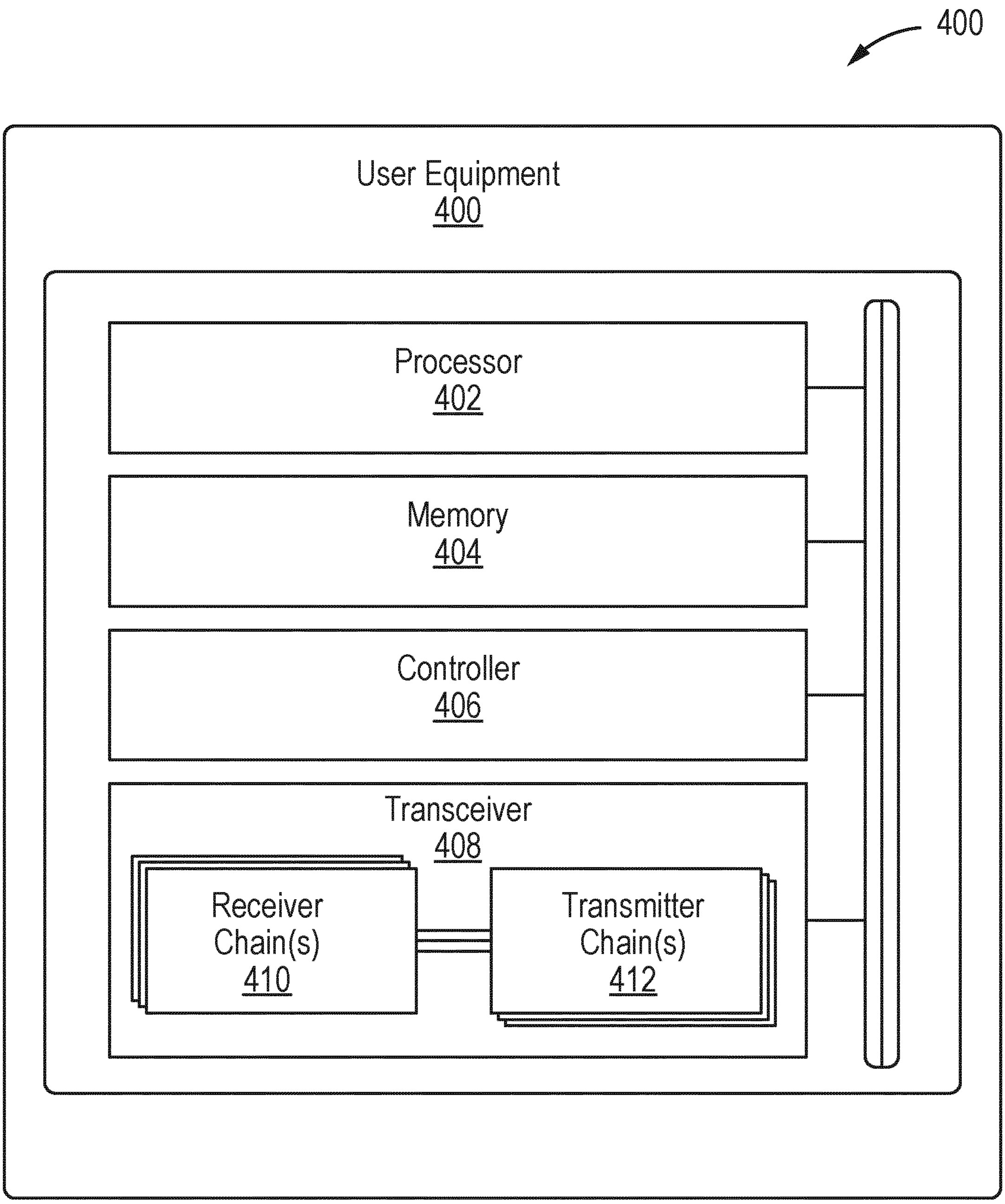

400
User Equipment
400
Processor
402
Memory
404
Controller
406
Transceiver
408
Receiver
Chain(s)
410
Transmitter
Chain(s)
412

Fig. 5

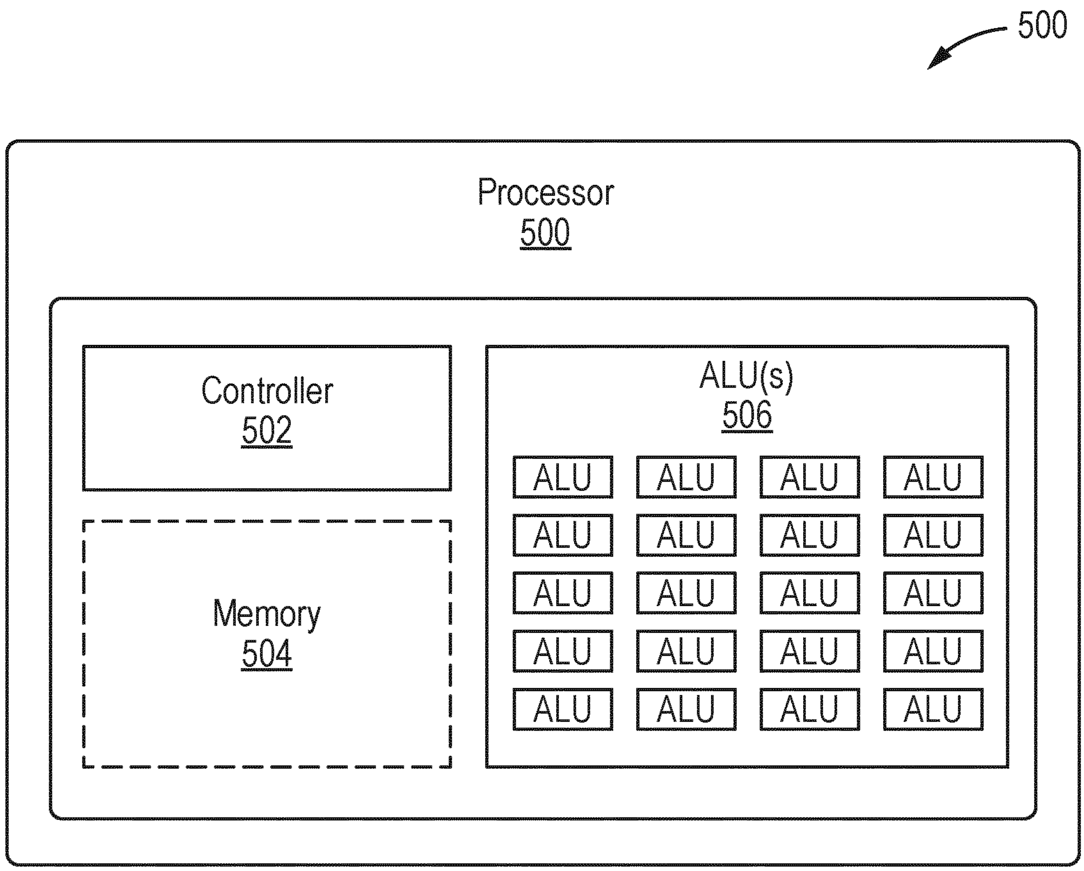


Fig. 6

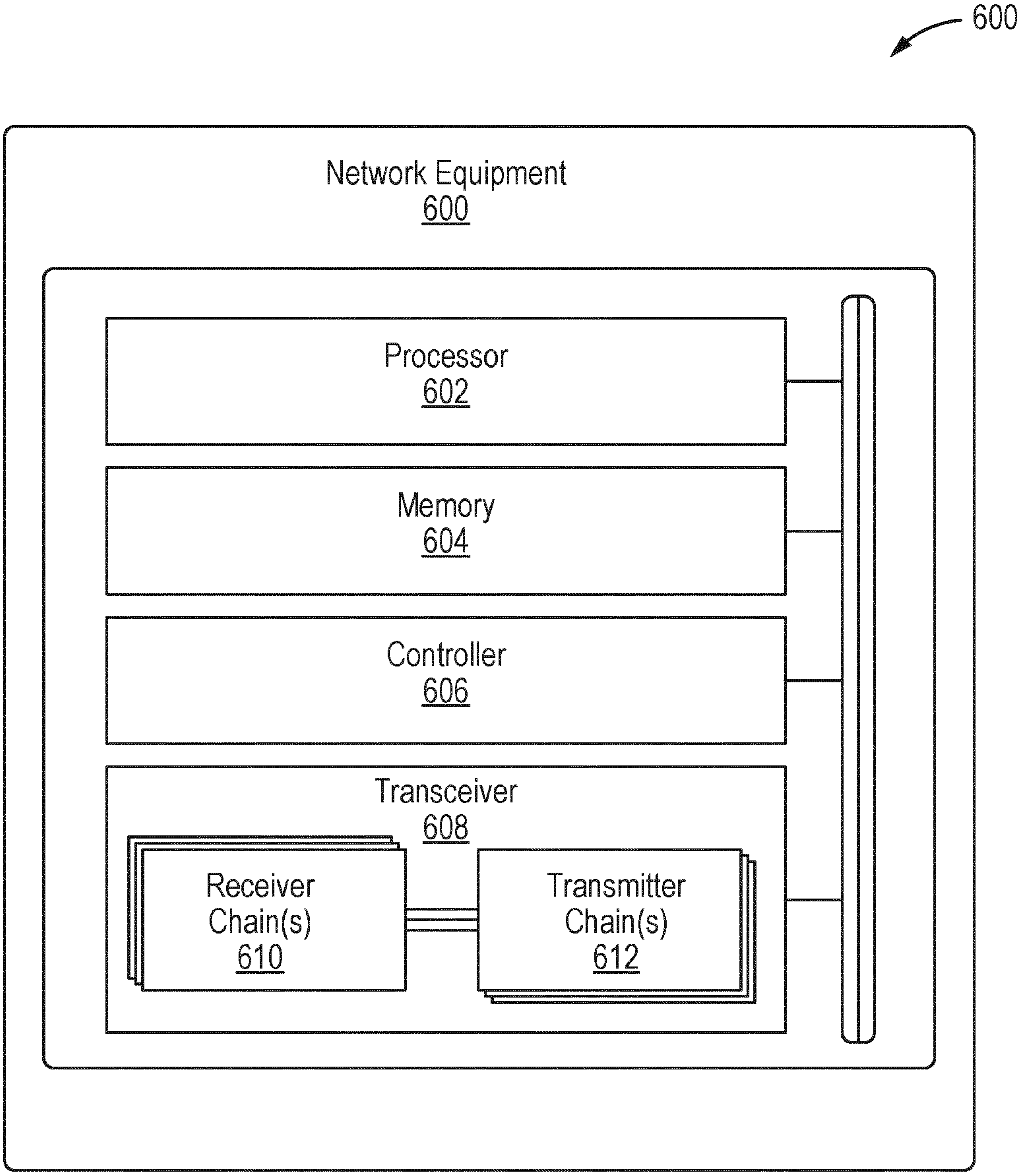
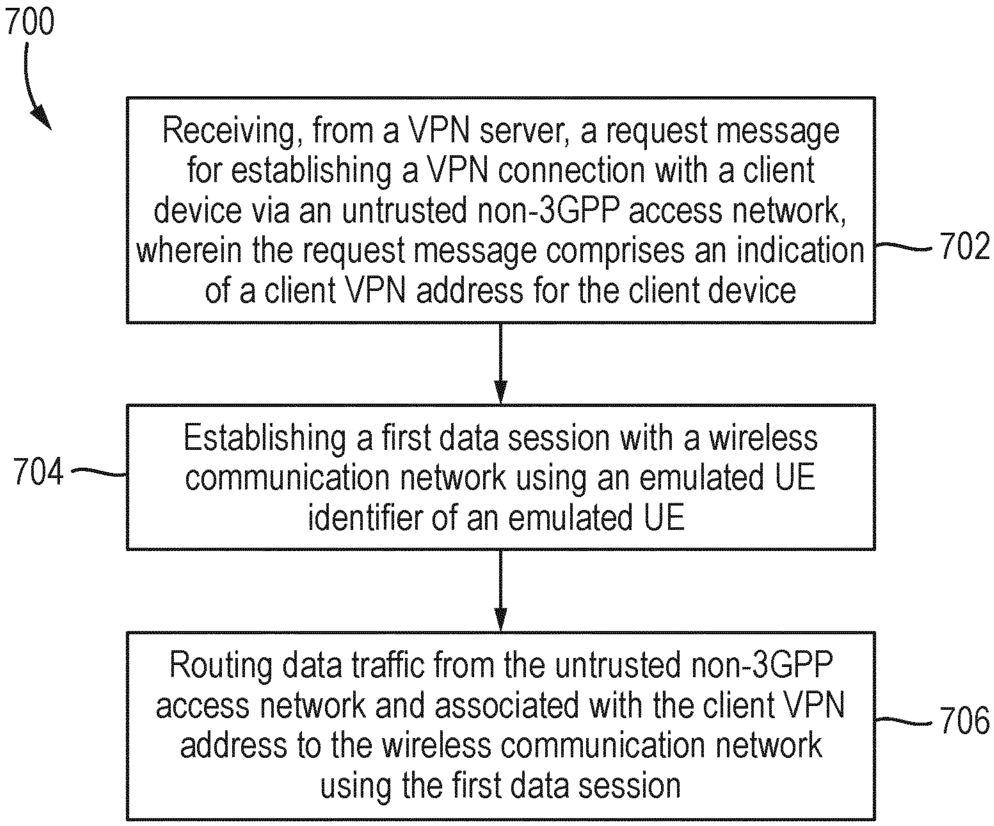

600
Network Equipment
600
Processor
602
Memory
604
Controller
606
Transceiver
608
Receiver
Chain(s)
610
Transmitter
Chain(s)
612

Fig. 7


700
Receiving, from a VPN server, a request message for establishing a VPN connection with a client device via an untrusted non-3GPP access network, wherein the request message comprises an indication of a client VPN address for the client device
702
Establishing a first data session with a wireless communication network using an emulated UE identifier of an emulated UE
704
Routing data traffic from the untrusted non-3GPP access network and associated with the client VPN address to the wireless communication network using the first data session
706

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2024/057598

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W76/12
ADD. H04L12/46

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	ROSETI CESARE: "Integration of a non-3GPP satellite interface in a 5G multiple access configuration", 2021 4TH INTERNATIONAL SYMPOSIUM ON ADVANCED ELECTRICAL AND COMMUNICATION TECHNOLOGIES (ISAECT), IEEE, 6 December 2021 (2021-12-06), pages 1-6, XP034001164, DOI: 10.1109/ISAECT53699.2021.9668502 [retrieved on 2022-01-03] pages 1,2,3 -----	1-20

-/--

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

[x] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 October 2024	12/11/2024

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Espuela, Vicente

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2021/306849 A1 (LIU JENNIFER [US]) 30 September 2021 (2021-09-30) paragraphs [0006] - [0008] paragraphs [0050] - [0055] paragraphs [0058] - [0064] paragraphs [0072] - [0079] figures 2-4 -----	1-20
A	MARIO TEIXEIRA LEMES ET AL: "A Tutorial on Trusted and Untrusted non-3GPP Accesses in 5G Systems -- First Steps Towards a Unified Communications Infrastructure", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 18 September 2021 (2021-09-18), XP091366311, DOI: 10.1109/ACCESS.2022.3219829 pages 2-9 pages 12-14 -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2024/057598

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021306849 A1	30-09-2021	AU 2019319095 A1	18-02-2021
		AU 2022252749 A1	03-11-2022
		AU 2024200276 A1	01-02-2024
		BR 112021002402 A2	04-05-2021
		CA 3106505 A1	13-02-2020
		CA 3234868 A1	13-02-2020
		CL 2021000335 A1	27-08-2021
		CL 2021000337 A1	27-08-2021
		CN 112586047 A	30-03-2021
		CN 118433706 A	02-08-2024
		CO 2021002942 A2	30-04-2021
		EP 3834519 A1	16-06-2021
		EP 4408086 A1	31-07-2024
		JP 7320598 B2	03-08-2023
		JP 2021533680 A	02-12-2021
		JP 2023123430 A	05-09-2023
		JP 2024095698 A	10-07-2024
		KR 20210024654 A	05-03-2021
		KR 20210025678 A	09-03-2021
		KR 20230128142 A	01-09-2023
		PH 12021550155 A1	13-09-2021
		SA 521421213 B1	09-05-2024
		SG 11202100720P A	25-02-2021
		US 2021306849 A1	30-09-2021
		WO 2020030851 A1	13-02-2020