



(51) International Patent Classification:

H04W 4/50 (2018.01) *H04W 12/069* (2021.01)
H04L 67/141 (2022.01) *H04W 28/02* (2009.01)
H04W 28/24 (2009.01) *H04L 9/40* (2022.01)
H04W 12/033 (2021.01)

(21) International Application Number:

PCT/US2024/036804

(22) International Filing Date:

03 July 2024 (03.07.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/525,591 07 July 2023 (07.07.2023) US

(71) Applicant: **INTERDIGITAL PATENT HOLDINGS, INC.** [US/US]; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809 (US).

(72) Inventors: **DE FOY, Xavier**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA). **FERDI, Samir**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA). **GUDUMASU, Srinivas**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA). **STARSINIC, Michael**; 1001 E. Hector Street, Conshohocken, PA 19428 (US). **METHENNI, Achref**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA). **ROY, Michel**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA). **DI GIROLAMO, Rocco**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA). **SARATHCHANDRA, Magurawalage, Chathura**; Madhusanka, 64 Great Eastern Street, London EC2A 3QR (GB). **DI LALLO, Kevin**; 1000 Sherbrooke Street, Montreal, QC H3A 3G4 (CA).

(74) Agent: **ROCCIA, Vincent, J.** et al.; Condo Roccia Koptiw LLP, 1800 JFK Blvd., Suite 1700, Philadelphia, PA 19103 (US).

(54) Title: SYSTEMS, METHODS, AND APPARATUS FOR NEF-BASED PDC CREATION

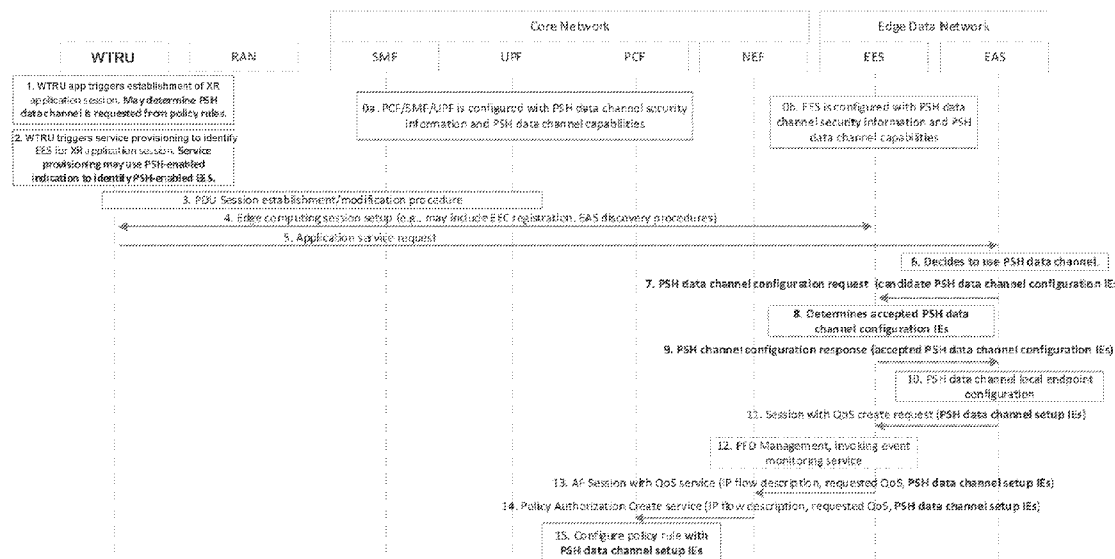


FIG. 5A

(57) Abstract: Systems, methods, devices, and instrumentalities are described herein related to NEF-based PDC creation and operation (e.g., by an enabler server, such as an edge enabler server (EES)). A device (e.g., an enabler server) may include a processor configured to perform one or more actions. The device may receive a session request message from a second network node, receive a session request message from a second network node. The session request message may indicate a request for a session. The session request message may include a protocol data unit set handling (PSH) data channel (PDC) setup information element (IE) and an indication of a Quality of Service (QoS) associated with the session. The device may determine a PDC should be established based on the request for the session, the PDC setup IE, and the indication of the QoS.

(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, 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))*

SYSTEMS, METHODS, AND APPARATUS FOR NEF-BASED PDC CREATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 63/525,591, filed July 7, 2023, the contents of which is incorporated by reference herein.

BACKGROUND

[0002] Mobile communications using wireless communication continue to evolve. A fifth generation may be referred to as 5G. A previous (legacy) generation of mobile communication may be, for example, fourth generation (4G) long-term evolution (LTE).

SUMMARY

[0003] Systems, methods, devices, and instrumentalities are described herein related to NEF-based PDC creation and operation (e.g., by an enabler server, such as an edge enabler server (EES)).

[0004] A device (e.g., an enabler server) may include a processor configured to perform one or more actions. The device may receive a session request message from a second network node. The session request message may indicate a request for a session and may include a protocol data unit set handling (PSH) data channel (PDC) setup information element (IE) and an indication of a Quality of Service (QoS) associated with the session. The device may determine that a PDC should be established based on the request for the session, the PDC setup IE, and the indication of the QoS. The device may send a service request message to a third network node when it is determined that the PDC should be established. The service request message may include the indication of the QoS and PDC setup IE. The device may receive a service response message from the third network node. The second message may indicate the PDC has been established based on the PDC setup IE. The device may send a session response message to the second network node. The session response message may indicate that the PDC is associated with the requested session and that the PDC has been established based on the PDC setup IE.

[0005] The PDU setup IE may indicate at least one of a PDU protocol, an internet protocol (IP) address for a PDC endpoint, a port for a PDC endpoint, a security parameter, an authentication method, an authentication parameter, an identity associated with a security certificate or key, or a protocol parameter,

or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection parameter. The PDU establishment request message may indicate a request to create a session with a Quality of Service (QoS). The service message may be associated with at least one of an application function, a network function (NF), a policy creation function (PCF), or a policy authorization. The PDC setup IE may be a first PDC setup IE. At least the service response message or the session response message may include a second PDC setup IE.

[0006] The device may receive a setup request message from the second network node. The request message may include one or more candidate PDC setup IEs. The device may determine the PDC setup IE from the one or more candidate PDC setup IEs. The device may send a setup response message to the second network node. The setup response message may include at least the PDC setup IE.

[0007] A method performed by a first network node may include receiving a session request message from a second network node. The session request message may indicate a request for a session and include a protocol data unit set handling data channel (PDC) setup information element (IE) and an indication of a Quality of Service (QoS) associated with the session. The method may include determining a PDC should be established based on the request for the session, the PDC setup IE, and the indication of the QoS. The method may include sending a service request message to a third network node when it is determined that the PDC should be established. The service request message may include the indication of the QoS and PDC setup IE. The method may include receiving a service response message from the third network node. The second message indicates the PDC has been established based on the PDC setup IE. The method may include sending a session response message to the second network node. The session response message may indicate that the PDC is associated with the requested session and that that the PDC has been established based on the PDC setup IE.

[0008] The PDU setup IE may indicate at least one of a PDU protocol, an internet protocol (IP) address for a PDC endpoint, a port for a PDC endpoint, a security parameter, an authentication method, an authentication parameter, an identity associated with a security certificate or key, a protocol parameter, or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection parameter.

[0009] The PDU establishment request message may indicate a request to create a session with a Quality of Service (QoS). The service message may be associated with at least one of an application function, a network function (NF), a policy creation function (PCF), or a policy authorization. The PDC setup IE may be a first PDC setup IE. At least the service response message or the session response message may include a second PDC setup IE.

[0010] The method may include receiving a setup request message from the second network node. The request message may include one or more candidate PDC setup IEs. The method may include determining

the PDC setup IE from the one or more candidate PDC setup IEs. The method may include sending a setup response message to the second network node. The setup response message may include at least the PDC setup IE.

[0011] A first network node may provide an enabler application server. The first network node may include a processor configured to perform one or more actions. The first network node may include determining one or more candidate protocol data unit set handling (PSH) data channel (PDC) setup information elements (IEs) associated with a service flow or an application. The first network node may include sending a setup request message to the second network node. The setup request message may include the one or more candidate PDC setup IEs. The first network node may include receiving a setup response message from the second network node. The setup response message may include a PDC setup IE from the one or more candidate PDC setup IEs. The first network node may include sending a session request message to a second network node. The session request message may indicate a request for a session and may include the PDC setup IE and an indication of a Quality of Service (QoS) associated with the session. The first network node may include receiving a session response message from the second network node. The session response message indicates that the PDC may be associated with the requested session and that the PDC may have been established based on the PDC setup IE.

[0012] The PDU setup IE may indicate at least one of a PDU protocol, an internet protocol (IP) address for a PDC endpoint, a port for a PDC endpoint, a security parameter, an authentication method, an authentication parameter, an identity associated with a security certificate or key, a protocol parameter, or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection parameter.

[0013] The PDU establishment request message may indicate a request to create a session with a Quality of Service (QoS). The PDC setup IE may be a first PDC setup IE. The session response message may include a second PDC setup IE.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1A is a system diagram illustrating an example communications system in which one or more disclosed embodiments may be implemented.

[0015] FIG. 1B is a system diagram illustrating an example wireless transmit/receive unit (WTRU) that may be used within the communications system illustrated in FIG. 1A according to an embodiment.

[0016] FIG. 1C is a system diagram illustrating an example radio access network (RAN) and an example core network (CN) that may be used within the communications system illustrated in FIG. 1A according to an embodiment.

[0017] FIG. 1D is a system diagram illustrating a further example RAN and a further example CN that may be used within the communications system illustrated in FIG. 1A according to an embodiment.

[0018] FIG. 2 depicts example processes for protocol data unit (PDU) set (PS) identification of downlink encrypted traffic.

[0019] FIG. 3 depicts an example of configuring, establishing, and operating PDCs.

[0020] FIGS. 4A-4B depict an example of PDC operation on the data plane.

[0021] FIGS. 5A-5B depict an example method for establishing and operating a PDC.

[0022] FIGS. 6A-6B depict an example method for WTRU-initiated PDC establishment and operation.

[0023] FIG. 7 depicts an example method for WTRU-initiated PSH tunnel security establishment.

[0024] FIG. 8 depicts an example method for AF-initiated PSH tunnel security establishment.

[0025] FIG. 9 depicts an example method for PSH tunnel security establishment using an EAP-based authentication method between WTRU, SMF, and AF.

DETAILED DESCRIPTION

[0026] FIG. 1A is a diagram illustrating an example communications system 100 in which one or more disclosed embodiments may be implemented. The communications system 100 may be a multiple access system that provides content, such as voice, data, video, messaging, broadcast, etc., to multiple wireless users. The communications system 100 may enable multiple wireless users to access such content through the sharing of system resources, including wireless bandwidth. For example, the communications systems 100 may employ one or more channel access methods, such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), orthogonal FDMA (OFDMA), single-carrier FDMA (SC-FDMA), zero-tail unique-word DFT-Spread OFDM (ZT UW DTS-s OFDM), unique word OFDM (UW-OFDM), resource block-filtered OFDM, filter bank multicarrier (FBMC), and the like.

[0027] As shown in FIG. 1A, the communications system 100 may include wireless transmit/receive units (WTRUs) 102a, 102b, 102c, 102d, a RAN 104/113, a CN 106/115, a public switched telephone network (PSTN) 108, the Internet 110, and other networks 112, though it will be appreciated that the disclosed embodiments contemplate any number of WTRUs, base stations, networks, and/or network elements. Each of the WTRUs 102a, 102b, 102c, 102d may be any type of device configured to operate and/or communicate in a wireless environment. By way of example, the WTRUs 102a, 102b, 102c, 102d, any of which may be referred to as a "station" and/or a "STA", may be configured to transmit and/or receive

wireless signals and may include a user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a subscription-based unit, a pager, a cellular telephone, a personal digital assistant (PDA), a smartphone, a laptop, a netbook, a personal computer, a wireless sensor, a hotspot or Mi-Fi device, an Internet of Things (IoT) device, a watch or other wearable, a head-mounted display (HMD), a vehicle, a drone, a medical device and applications (e.g., remote surgery), an industrial device and applications (e.g., a robot and/or other wireless devices operating in an industrial and/or an automated processing chain contexts), a consumer electronics device, a device operating on commercial and/or industrial wireless networks, and the like. Any of the WTRUs 102a, 102b, 102c and 102d may be interchangeably referred to as a UE.

[0028] The communications systems 100 may also include a base station 114a and/or a base station 114b. Each of the base stations 114a, 114b may be any type of device configured to wirelessly interface with at least one of the WTRUs 102a, 102b, 102c, 102d to facilitate access to one or more communication networks, such as the CN 106/115, the Internet 110, and/or the other networks 112. By way of example, the base stations 114a, 114b may be a base transceiver station (BTS), a Node-B, an eNode B, a Home Node B, a Home eNode B, a gNB, a NR NodeB, a site controller, an access point (AP), a wireless router, and the like. While the base stations 114a, 114b are each depicted as a single element, it will be appreciated that the base stations 114a, 114b may include any number of interconnected base stations and/or network elements.

[0029] The base station 114a may be part of the RAN 104/113, which may also include other base stations and/or network elements (not shown), such as a base station controller (BSC), a radio network controller (RNC), relay nodes, etc. The base station 114a and/or the base station 114b may be configured to transmit and/or receive wireless signals on one or more carrier frequencies, which may be referred to as a cell (not shown). These frequencies may be in licensed spectrum, unlicensed spectrum, or a combination of licensed and unlicensed spectrum. A cell may provide coverage for a wireless service to a specific geographical area that may be relatively fixed or that may change over time. The cell may further be divided into cell sectors. For example, the cell associated with the base station 114a may be divided into three sectors. Thus, in one embodiment, the base station 114a may include three transceivers (e.g., one for each sector of the cell). In an embodiment, the base station 114a may employ multiple-input multiple output (MIMO) technology and may utilize multiple transceivers for each sector of the cell. For example, beamforming may be used to transmit and/or receive signals in desired spatial directions.

[0030] The base stations 114a, 114b may communicate with one or more of the WTRUs 102a, 102b, 102c, 102d over an air interface 116, which may be any suitable wireless communication link (e.g., radio frequency (RF), microwave, centimeter wave, micrometer wave, infrared (IR), ultraviolet (UV), visible light, etc.). The air interface 116 may be established using any suitable radio access technology (RAT).

[0031] More specifically, as noted above, the communications system 100 may be a multiple access system and may employ one or more channel access schemes, such as CDMA, TDMA, FDMA, OFDMA, SC-FDMA, and the like. For example, the base station 114a in the RAN 104/113 and the WTRUs 102a, 102b, 102c may implement a radio technology such as Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access (UTRA), which may establish the air interface 115/116/117 using wideband CDMA (WCDMA). WCDMA may include communication protocols such as High-Speed Packet Access (HSPA) and/or Evolved HSPA (HSPA+). HSPA may include High-Speed Downlink (DL) Packet Access (HSDPA) and/or High-Speed UL Packet Access (HSUPA).

[0032] In an embodiment, the base station 114a and the WTRUs 102a, 102b, 102c may implement a radio technology such as Evolved UMTS Terrestrial Radio Access (E-UTRA), which may establish the air interface 116 using Long Term Evolution (LTE) and/or LTE-Advanced (LTE-A) and/or LTE-Advanced Pro (LTE-A Pro).

[0033] In an embodiment, the base station 114a and the WTRUs 102a, 102b, 102c may implement a radio technology such as NR Radio Access, which may establish the air interface 116 using New Radio (NR).

[0034] In an embodiment, the base station 114a and the WTRUs 102a, 102b, 102c may implement multiple radio access technologies. For example, the base station 114a and the WTRUs 102a, 102b, 102c may implement LTE radio access and NR radio access together, for instance using dual connectivity (DC) principles. Thus, the air interface utilized by WTRUs 102a, 102b, 102c may be characterized by multiple types of radio access technologies and/or transmissions sent to/from multiple types of base stations (e.g., an eNB and a gNB).

[0035] In other embodiments, the base station 114a and the WTRUs 102a, 102b, 102c may implement radio technologies such as IEEE 802.11 (i.e., Wireless Fidelity (WiFi)), IEEE 802.16 (i.e., Worldwide Interoperability for Microwave Access (WiMAX)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, Interim Standard 2000 (IS-2000), Interim Standard 95 (IS-95), Interim Standard 856 (IS-856), Global System for Mobile communications (GSM), Enhanced Data rates for GSM Evolution (EDGE), GSM EDGE (GERAN), and the like.

[0036] The base station 114b in FIG. 1A may be a wireless router, Home Node B, Home eNode B, or access point, for example, and may utilize any suitable RAT for facilitating wireless connectivity in a localized area, such as a place of business, a home, a vehicle, a campus, an industrial facility, an air corridor (e.g., for use by drones), a roadway, and the like. In one embodiment, the base station 114b and the WTRUs 102c, 102d may implement a radio technology such as IEEE 802.11 to establish a wireless local area network (WLAN). In an embodiment, the base station 114b and the WTRUs 102c, 102d may

implement a radio technology such as IEEE 802.15 to establish a wireless personal area network (WPAN). In yet another embodiment, the base station 114b and the WTRUs 102c, 102d may utilize a cellular-based RAT (e.g., WCDMA, CDMA2000, GSM, LTE, LTE-A, LTE-A Pro, NR etc.) to establish a picocell or femtocell. As shown in FIG. 1A, the base station 114b may have a direct connection to the Internet 110. Thus, the base station 114b may not be required to access the Internet 110 via the CN 106/115.

[0037] The RAN 104/113 may be in communication with the CN 106/115, which may be any type of network configured to provide voice, data, applications, and/or voice over internet protocol (VoIP) services to one or more of the WTRUs 102a, 102b, 102c, 102d. The data may have varying quality of service (QoS) requirements, such as differing throughput requirements, latency requirements, error tolerance requirements, reliability requirements, data throughput requirements, mobility requirements, and the like. The CN 106/115 may provide call control, billing services, mobile location-based services, pre-paid calling, Internet connectivity, video distribution, etc., and/or perform high-level security functions, such as user authentication. Although not shown in FIG. 1A, it will be appreciated that the RAN 104/113 and/or the CN 106/115 may be in direct or indirect communication with other RANs that employ the same RAT as the RAN 104/113 or a different RAT. For example, in addition to being connected to the RAN 104/113, which may be utilizing a NR radio technology, the CN 106/115 may also be in communication with another RAN (not shown) employing a GSM, UMTS, CDMA 2000, WIMAX, E-UTRA, or WiFi radio technology.

[0038] The CN 106/115 may also serve as a gateway for the WTRUs 102a, 102b, 102c, 102d to access the PSTN 108, the Internet 110, and/or the other networks 112. The PSTN 108 may include circuit-switched telephone networks that provide plain old telephone service (POTS). The Internet 110 may include a global system of interconnected computer networks and devices that use common communication protocols, such as the transmission control protocol (TCP), user datagram protocol (UDP) and/or the internet protocol (IP) in the TCP/IP internet protocol suite. The networks 112 may include wired and/or wireless communications networks owned and/or operated by other service providers. For example, the networks 112 may include another CN connected to one or more RANs, which may employ the same RAT as the RAN 104/113 or a different RAT.

[0039] Some or all of the WTRUs 102a, 102b, 102c, 102d in the communications system 100 may include multi-mode capabilities (e.g., the WTRUs 102a, 102b, 102c, 102d may include multiple transceivers for communicating with different wireless networks over different wireless links). For example, the WTRU 102c shown in FIG. 1A may be configured to communicate with the base station 114a, which may employ a cellular-based radio technology, and with the base station 114b, which may employ an IEEE 802 radio technology.

[0040] FIG. 1B is a system diagram illustrating an example WTRU 102. As shown in FIG. 1B, the WTRU 102 may include a processor 118, a transceiver 120, a transmit/receive element 122, a speaker/microphone 124, a keypad 126, a display/touchpad 128, non-removable memory 130, removable memory 132, a power source 134, a global positioning system (GPS) chipset 136, and/or other peripherals 138, among others. It will be appreciated that the WTRU 102 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment.

[0041] The processor 118 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the like. The processor 118 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the WTRU 102 to operate in a wireless environment. The processor 118 may be coupled to the transceiver 120, which may be coupled to the transmit/receive element 122. While FIG. 1B depicts the processor 118 and the transceiver 120 as separate components, it will be appreciated that the processor 118 and the transceiver 120 may be integrated together in an electronic package or chip.

[0042] The transmit/receive element 122 may be configured to transmit signals to, or receive signals from, a base station (e.g., the base station 114a) over the air interface 116. For example, in one embodiment, the transmit/receive element 122 may be an antenna configured to transmit and/or receive RF signals. In an embodiment, the transmit/receive element 122 may be an emitter/detector configured to transmit and/or receive IR, UV, or visible light signals, for example. In yet another embodiment, the transmit/receive element 122 may be configured to transmit and/or receive both RF and light signals. It will be appreciated that the transmit/receive element 122 may be configured to transmit and/or receive any combination of wireless signals.

[0043] Although the transmit/receive element 122 is depicted in FIG. 1B as a single element, the WTRU 102 may include any number of transmit/receive elements 122. More specifically, the WTRU 102 may employ MIMO technology. Thus, in one embodiment, the WTRU 102 may include two or more transmit/receive elements 122 (e.g., multiple antennas) for transmitting and receiving wireless signals over the air interface 116.

[0044] The transceiver 120 may be configured to modulate the signals that are to be transmitted by the transmit/receive element 122 and to demodulate the signals that are received by the transmit/receive element 122. As noted above, the WTRU 102 may have multi-mode capabilities. Thus, the transceiver 120

may include multiple transceivers for enabling the WTRU 102 to communicate via multiple RATs, such as NR and IEEE 802.11, for example.

[0045] The processor 118 of the WTRU 102 may be coupled to, and may receive user input data from, the speaker/microphone 124, the keypad 126, and/or the display/touchpad 128 (e.g., a liquid crystal display (LCD) display unit or organic light-emitting diode (OLED) display unit). The processor 118 may also output user data to the speaker/microphone 124, the keypad 126, and/or the display/touchpad 128. In addition, the processor 118 may access information from, and store data in, any type of suitable memory, such as the non-removable memory 130 and/or the removable memory 132. The non-removable memory 130 may include random-access memory (RAM), read-only memory (ROM), a hard disk, or any other type of memory storage device. The removable memory 132 may include a subscriber identity module (SIM) card, a memory stick, a secure digital (SD) memory card, and the like. In other embodiments, the processor 118 may access information from, and store data in, memory that is not physically located on the WTRU 102, such as on a server or a home computer (not shown).

[0046] The processor 118 may receive power from the power source 134, and may be configured to distribute and/or control the power to the other components in the WTRU 102. The power source 134 may be any suitable device for powering the WTRU 102. For example, the power source 134 may include one or more dry cell batteries (e.g., nickel-cadmium (NiCd), nickel-zinc (NiZn), nickel metal hydride (NiMH), lithium-ion (Li-ion), etc.), solar cells, fuel cells, and the like.

[0047] The processor 118 may also be coupled to the GPS chipset 136, which may be configured to provide location information (e.g., longitude and latitude) regarding the current location of the WTRU 102. In addition to, or in lieu of, the information from the GPS chipset 136, the WTRU 102 may receive location information over the air interface 116 from a base station (e.g., base stations 114a, 114b) and/or determine its location based on the timing of the signals being received from two or more nearby base stations. It will be appreciated that the WTRU 102 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

[0048] The processor 118 may further be coupled to other peripherals 138, which may include one or more software and/or hardware modules that provide additional features, functionality and/or wired or wireless connectivity. For example, the peripherals 138 may include an accelerometer, an e-compass, a satellite transceiver, a digital camera (for photographs and/or video), a universal serial bus (USB) port, a vibration device, a television transceiver, a hands free headset, a Bluetooth® module, a frequency modulated (FM) radio unit, a digital music player, a media player, a video game player module, an Internet browser, a Virtual Reality and/or Augmented Reality (VR/AR) device, an activity tracker, and the like. The peripherals 138 may include one or more sensors, the sensors may be one or more of a gyroscope, an

accelerometer, a hall effect sensor, a magnetometer, an orientation sensor, a proximity sensor, a temperature sensor, a time sensor; a geolocation sensor; an altimeter, a light sensor, a touch sensor, a magnetometer, a barometer, a gesture sensor, a biometric sensor, and/or a humidity sensor.

[0049] The WTRU 102 may include a full duplex radio for which transmission and reception of some or all of the signals (e.g., associated with particular subframes for both the UL (e.g., for transmission) and downlink (e.g., for reception) may be concurrent and/or simultaneous. The full duplex radio may include an interference management unit to reduce and or substantially eliminate self-interference via either hardware (e.g., a choke) or signal processing via a processor (e.g., a separate processor (not shown) or via processor 118). In an embodiment, the WTRU 102 may include a half-duplex radio for which transmission and reception of some or all of the signals (e.g., associated with particular subframes for either the UL (e.g., for transmission) or the downlink (e.g., for reception)).

[0050] FIG. 1C is a system diagram illustrating the RAN 104 and the CN 106 according to an embodiment. As noted above, the RAN 104 may employ an E-UTRA radio technology to communicate with the WTRUs 102a, 102b, 102c over the air interface 116. The RAN 104 may also be in communication with the CN 106.

[0051] The RAN 104 may include eNode-Bs 160a, 160b, 160c, though it will be appreciated that the RAN 104 may include any number of eNode-Bs while remaining consistent with an embodiment. The eNode-Bs 160a, 160b, 160c may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 116. In one embodiment, the eNode-Bs 160a, 160b, 160c may implement MIMO technology. Thus, the eNode-B 160a, for example, may use multiple antennas to transmit wireless signals to, and/or receive wireless signals from, the WTRU 102a.

[0052] Each of the eNode-Bs 160a, 160b, 160c may be associated with a particular cell (not shown) and may be configured to handle radio resource management decisions, handover decisions, scheduling of users in the UL and/or DL, and the like. As shown in FIG. 1C, the eNode-Bs 160a, 160b, 160c may communicate with one another over an X2 interface.

[0053] The CN 106 shown in FIG. 1C may include a mobility management entity (MME) 162, a serving gateway (SGW) 164, and a packet data network (PDN) gateway (or PGW) 166. While each of the foregoing elements are depicted as part of the CN 106, it will be appreciated that any of these elements may be owned and/or operated by an entity other than the CN operator.

[0054] The MME 162 may be connected to each of the eNode-Bs 160a, 160b, 160c in the RAN 104 via an S1 interface and may serve as a control node. For example, the MME 162 may be responsible for authenticating users of the WTRUs 102a, 102b, 102c, bearer activation/deactivation, selecting a particular serving gateway during an initial attach of the WTRUs 102a, 102b, 102c, and the like. The MME 162 may

provide a control plane function for switching between the RAN 104 and other RANs (not shown) that employ other radio technologies, such as GSM and/or WCDMA.

[0055] The SGW 164 may be connected to each of the eNode Bs 160a, 160b, 160c in the RAN 104 via the S1 interface. The SGW 164 may generally route and forward user data packets to/from the WTRUs 102a, 102b, 102c. The SGW 164 may perform other functions, such as anchoring user planes during inter-eNode B handovers, triggering paging when DL data is available for the WTRUs 102a, 102b, 102c, managing and storing contexts of the WTRUs 102a, 102b, 102c, and the like.

[0056] The SGW 164 may be connected to the PGW 166, which may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between the WTRUs 102a, 102b, 102c and IP-enabled devices.

[0057] The CN 106 may facilitate communications with other networks. For example, the CN 106 may provide the WTRUs 102a, 102b, 102c with access to circuit-switched networks, such as the PSTN 108, to facilitate communications between the WTRUs 102a, 102b, 102c and traditional land-line communications devices. For example, the CN 106 may include, or may communicate with, an IP gateway (e.g., an IP multimedia subsystem (IMS) server) that serves as an interface between the CN 106 and the PSTN 108. In addition, the CN 106 may provide the WTRUs 102a, 102b, 102c with access to the other networks 112, which may include other wired and/or wireless networks that are owned and/or operated by other service providers.

[0058] Although the WTRU is described in FIGS. 1A-1D as a wireless terminal, it is contemplated that in certain representative embodiments that such a terminal may use (e.g., temporarily or permanently) wired communication interfaces with the communication network.

[0059] In representative embodiments, the other network 112 may be a WLAN.

[0060] A WLAN in Infrastructure Basic Service Set (BSS) mode may have an Access Point (AP) for the BSS and one or more stations (STAs) associated with the AP. The AP may have an access or an interface to a Distribution System (DS) or another type of wired/wireless network that carries traffic in to and/or out of the BSS. Traffic to STAs that originates from outside the BSS may arrive through the AP and may be delivered to the STAs. Traffic originating from STAs to destinations outside the BSS may be sent to the AP to be delivered to respective destinations. Traffic between STAs within the BSS may be sent through the AP, for example, where the source STA may send traffic to the AP and the AP may deliver the traffic to the destination STA. The traffic between STAs within a BSS may be considered and/or referred to as peer-to-peer traffic. The peer-to-peer traffic may be sent between (e.g., directly between) the source and destination STAs with a direct link setup (DLS). In certain representative embodiments, the DLS may use an 802.11e DLS or an 802.11z tunneled DLS (TDLS). A WLAN using an Independent BSS (IBSS) mode

may not have an AP, and the STAs (e.g., all of the STAs) within or using the IBSS may communicate directly with each other. The IBSS mode of communication may sometimes be referred to herein as an “ad-hoc” mode of communication.

[0061] When using the 802.11ac infrastructure mode of operation or a similar mode of operations, the AP may transmit a beacon on a fixed channel, such as a primary channel. The primary channel may be a fixed width (e.g., 20 MHz wide bandwidth) or a dynamically set width via signaling. The primary channel may be the operating channel of the BSS and may be used by the STAs to establish a connection with the AP. In certain representative embodiments, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) may be implemented, for example in 802.11 systems. For CSMA/CA, the STAs (e.g., every STA), including the AP, may sense the primary channel. If the primary channel is sensed/detected and/or determined to be busy by a particular STA, the particular STA may back off. One STA (e.g., only one station) may transmit at any given time in a given BSS.

[0062] High Throughput (HT) STAs may use a 40 MHz wide channel for communication, for example, via a combination of the primary 20 MHz channel with an adjacent or nonadjacent 20 MHz channel to form a 40 MHz wide channel.

[0063] Very High Throughput (VHT) STAs may support 20MHz, 40 MHz, 80 MHz, and/or 160 MHz wide channels. The 40 MHz, and/or 80 MHz, channels may be formed by combining contiguous 20 MHz channels. A 160 MHz channel may be formed by combining 8 contiguous 20 MHz channels, or by combining two non-contiguous 80 MHz channels, which may be referred to as an 80+80 configuration. For the 80+80 configuration, the data, after channel encoding, may be passed through a segment parser that may divide the data into two streams. Inverse Fast Fourier Transform (IFFT) processing, and time domain processing, may be done on each stream separately. The streams may be mapped on to the two 80 MHz channels, and the data may be transmitted by a transmitting STA. At the receiver of the receiving STA, the above described operation for the 80+80 configuration may be reversed, and the combined data may be sent to the Medium Access Control (MAC).

[0064] Sub 1 GHz modes of operation are supported by 802.11af and 802.11ah. The channel operating bandwidths, and carriers, are reduced in 802.11af and 802.11ah relative to those used in 802.11n, and 802.11ac. 802.11af supports 5 MHz, 10 MHz and 20 MHz bandwidths in the TV White Space (TVWS) spectrum, and 802.11ah supports 1 MHz, 2 MHz, 4 MHz, 8 MHz, and 16 MHz bandwidths using non-TVWS spectrum. According to a representative embodiment, 802.11ah may support Meter Type Control/Machine-Type Communications, such as MTC devices in a macro coverage area. MTC devices may have certain capabilities, for example, limited capabilities including support for (e.g., only support for)

certain and/or limited bandwidths. The MTC devices may include a battery with a battery life above a threshold (e.g., to maintain a very long battery life).

[0065] WLAN systems, which may support multiple channels, and channel bandwidths, such as 802.11n, 802.11ac, 802.11af, and 802.11ah, include a channel which may be designated as the primary channel. The primary channel may have a bandwidth equal to the largest common operating bandwidth supported by all STAs in the BSS. The bandwidth of the primary channel may be set and/or limited by a STA, from among all STAs in operating in a BSS, which supports the smallest bandwidth operating mode. In the example of 802.11ah, the primary channel may be 1 MHz wide for STAs (e.g., MTC type devices) that support (e.g., only support) a 1 MHz mode, even if the AP, and other STAs in the BSS support 2 MHz, 4 MHz, 8 MHz, 16 MHz, and/or other channel bandwidth operating modes. Carrier sensing and/or Network Allocation Vector (NAV) settings may depend on the status of the primary channel. If the primary channel is busy, for example, due to a STA (which supports only a 1 MHz operating mode), transmitting to the AP, the entire available frequency bands may be considered busy even though a majority of the frequency bands remains idle and may be available.

[0066] In the United States, the available frequency bands, which may be used by 802.11ah, are from 902 MHz to 928 MHz. In Korea, the available frequency bands are from 917.5 MHz to 923.5 MHz. In Japan, the available frequency bands are from 916.5 MHz to 927.5 MHz. The total bandwidth available for 802.11ah is 6 MHz to 26 MHz depending on the country code.

[0067] FIG. 1D is a system diagram illustrating the RAN 113 and the CN 115 according to an embodiment. As noted above, the RAN 113 may employ an NR radio technology to communicate with the WTRUs 102a, 102b, 102c over the air interface 116. The RAN 113 may also be in communication with the CN 115.

[0068] The RAN 113 may include gNBs 180a, 180b, 180c, though it will be appreciated that the RAN 113 may include any number of gNBs while remaining consistent with an embodiment. The gNBs 180a, 180b, 180c may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 116. In one embodiment, the gNBs 180a, 180b, 180c may implement MIMO technology. For example, gNBs 180a, 180b may utilize beamforming to transmit signals to and/or receive signals from the gNBs 180a, 180b, 180c. Thus, the gNB 180a, for example, may use multiple antennas to transmit wireless signals to, and/or receive wireless signals from, the WTRU 102a. In an embodiment, the gNBs 180a, 180b, 180c may implement carrier aggregation technology. For example, the gNB 180a may transmit multiple component carriers to the WTRU 102a (not shown). A subset of these component carriers may be on unlicensed spectrum while the remaining component carriers may be on licensed spectrum. In an embodiment, the gNBs 180a, 180b, 180c may implement Coordinated Multi-Point (CoMP) technology.

For example, WTRU 102a may receive coordinated transmissions from gNB 180a and gNB 180b (and/or gNB 180c).

[0069] The WTRUs 102a, 102b, 102c may communicate with gNBs 180a, 180b, 180c using transmissions associated with a scalable numerology. For example, the OFDM symbol spacing and/or OFDM subcarrier spacing may vary for different transmissions, different cells, and/or different portions of the wireless transmission spectrum. The WTRUs 102a, 102b, 102c may communicate with gNBs 180a, 180b, 180c using subframe or transmission time intervals (TTIs) of various or scalable lengths (e.g., containing varying number of OFDM symbols and/or lasting varying lengths of absolute time).

[0070] The gNBs 180a, 180b, 180c may be configured to communicate with the WTRUs 102a, 102b, 102c in a standalone configuration and/or a non-standalone configuration. In the standalone configuration, WTRUs 102a, 102b, 102c may communicate with gNBs 180a, 180b, 180c without also accessing other RANs (e.g., such as eNode-Bs 160a, 160b, 160c). In the standalone configuration, WTRUs 102a, 102b, 102c may utilize one or more of gNBs 180a, 180b, 180c as a mobility anchor point. In the standalone configuration, WTRUs 102a, 102b, 102c may communicate with gNBs 180a, 180b, 180c using signals in an unlicensed band. In a non-standalone configuration WTRUs 102a, 102b, 102c may communicate with/connect to gNBs 180a, 180b, 180c while also communicating with/connecting to another RAN such as eNode-Bs 160a, 160b, 160c. For example, WTRUs 102a, 102b, 102c may implement DC principles to communicate with one or more gNBs 180a, 180b, 180c and one or more eNode-Bs 160a, 160b, 160c substantially simultaneously. In the non-standalone configuration, eNode-Bs 160a, 160b, 160c may serve as a mobility anchor for WTRUs 102a, 102b, 102c and gNBs 180a, 180b, 180c may provide additional coverage and/or throughput for servicing WTRUs 102a, 102b, 102c.

[0071] Each of the gNBs 180a, 180b, 180c may be associated with a particular cell (not shown) and may be configured to handle radio resource management decisions, handover decisions, scheduling of users in the UL and/or DL, support of network slicing, dual connectivity, interworking between NR and E-UTRA, routing of user plane data towards User Plane Function (UPF) 184a, 184b, routing of control plane information towards Access and Mobility Management Function (AMF) 182a, 182b and the like. As shown in FIG. 1D, the gNBs 180a, 180b, 180c may communicate with one another over an Xn interface.

[0072] The CN 115 shown in FIG. 1D may include at least one AMF 182a, 182b, at least one UPF 184a, 184b, at least one Session Management Function (SMF) 183a, 183b, and possibly a Data Network (DN) 185a, 185b. While each of the foregoing elements are depicted as part of the CN 115, it will be appreciated that any of these elements may be owned and/or operated by an entity other than the CN operator.

[0073] The AMF 182a, 182b may be connected to one or more of the gNBs 180a, 180b, 180c in the RAN 113 via an N2 interface and may serve as a control node. For example, the AMF 182a, 182b may be responsible for authenticating users of the WTRUs 102a, 102b, 102c, support for network slicing (e.g., handling of different PDU sessions with different requirements), selecting a particular SMF 183a, 183b, management of the registration area, termination of NAS signaling, mobility management, and the like. Network slicing may be used by the AMF 182a, 182b in order to customize CN support for WTRUs 102a, 102b, 102c based on the types of services being utilized WTRUs 102a, 102b, 102c. For example, different network slices may be established for different use cases such as services relying on ultra-reliable low latency (URLLC) access, services relying on enhanced massive mobile broadband (eMBB) access, services for machine type communication (MTC) access, and/or the like. The AMF 162 may provide a control plane function for switching between the RAN 113 and other RANs (not shown) that employ other radio technologies, such as LTE, LTE-A, LTE-A Pro, and/or non-3GPP access technologies such as WiFi.

[0074] The SMF 183a, 183b may be connected to an AMF 182a, 182b in the CN 115 via an N11 interface. The SMF 183a, 183b may also be connected to a UPF 184a, 184b in the CN 115 via an N4 interface. The SMF 183a, 183b may select and control the UPF 184a, 184b and configure the routing of traffic through the UPF 184a, 184b. The SMF 183a, 183b may perform other functions, such as managing and allocating UE IP address, managing PDU sessions, controlling policy enforcement and QoS, providing downlink data notifications, and the like. A PDU session type may be IP-based, non-IP based, Ethernet-based, and the like.

[0075] The UPF 184a, 184b may be connected to one or more of the gNBs 180a, 180b, 180c in the RAN 113 via an N3 interface, which may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between the WTRUs 102a, 102b, 102c and IP-enabled devices. The UPF 184a, 184b may perform other functions, such as routing and forwarding packets, enforcing user plane policies, supporting multi-homed PDU sessions, handling user plane QoS, buffering downlink packets, providing mobility anchoring, and the like.

[0076] The CN 115 may facilitate communications with other networks. For example, the CN 115 may include, or may communicate with, an IP gateway (e.g., an IP multimedia subsystem (IMS) server) that serves as an interface between the CN 115 and the PSTN 108. In addition, the CN 115 may provide the WTRUs 102a, 102b, 102c with access to the other networks 112, which may include other wired and/or wireless networks that are owned and/or operated by other service providers. In one embodiment, the WTRUs 102a, 102b, 102c may be connected to a local Data Network (DN) 185a, 185b through the UPF 184a, 184b via the N3 interface to the UPF 184a, 184b and an N6 interface between the UPF 184a, 184b and the DN 185a, 185b.

[0077] In view of Figures 1A-1D, and the corresponding description of Figures 1A-1D, one or more, or all, of the functions described herein with regard to one or more of: WTRU 102a-d, Base Station 114a-b, eNode-B 160a-c, MME 162, SGW 164, PGW 166, gNB 180a-c, AMF 182a-b, UPF 184a-b, SMF 183a-b, DN 185a-b, and/or any other device(s) described herein, may be performed by one or more emulation devices (not shown). The emulation devices may be one or more devices configured to emulate one or more, or all, of the functions described herein. For example, the emulation devices may be used to test other devices and/or to simulate network and/or WTRU functions.

[0078] The emulation devices may be designed to implement one or more tests of other devices in a lab environment and/or in an operator network environment. For example, the one or more emulation devices may perform the one or more, or all, functions while being fully or partially implemented and/or deployed as part of a wired and/or wireless communication network in order to test other devices within the communication network. The one or more emulation devices may perform the one or more, or all, functions while being temporarily implemented/deployed as part of a wired and/or wireless communication network. The emulation device may be directly coupled to another device for purposes of testing and/or may performing testing using over-the-air wireless communications.

[0079] The one or more emulation devices may perform the one or more, including all, functions while not being implemented/deployed as part of a wired and/or wireless communication network. For example, the emulation devices may be utilized in a testing scenario in a testing laboratory and/or a non-deployed (e.g., testing) wired and/or wireless communication network in order to implement testing of one or more components. The one or more emulation devices may be testing equipment. Direct RF coupling and/or wireless communications via RF circuitry (e.g., which may include one or more antennas) may be used by the emulation devices to transmit and/or receive data.

[0080] The following abbreviations and acronyms are used herein:

5GS	5G System
AF	Application Function
AKMA	Authentication and Key Management for Applications
API	Application Programming Interface
AS	Application Server
CDN	Content Delivery Network
DN	Data Network
DNAI	Data Network Access ID
DNN	Data Network Name

EAS	Edge Application Server
EDN	Edge Data Network
ECS	Edge Configuration Server
EEC	Edge Enabler Client
EES	Edge Enabler Server
FQDN	Fully Qualified Domain Name
GTP-U	Generic Tunneling Protocol User Plane
HTTP	Hypertext Transfer Protocol
ID	Identifier
IE	Information Element
IKE	Internet Key Exchange protocol
IP	Internet Protocol
MASQUE	Multiplexed Application Substrate over QUIC Encryption
MEC	Mobile Edge Computing
MOQ	Media over QUIC
MTU	Maximum Transmission Unit
NACK	Negative Acknowledgement
PDC	PSH Data Channel
PDU	Protocol Data Unit
PS	PDU Set
PSA UPF	PDU Session Anchor UPF
PSDB	PDU Set Delay Budget
PSER	PDU Set Error Rate
PSH	PDU Set Handling (e.g., QoS)
PSII	PDU Set Integrated Indication
QoE	Quality of Experience
QoS	Quality of Service
QUIC	The QUIC protocol (QUIC is a name)
RAN	Radio Access Network

RAT	Radio Access Technology
RTP	Real-Time Protocol
SDAP	Service Data Adaptation Protocol
SEAL	Service Enabler Architecture Layer
SMF	Session Management Function
SPF	Secure Proxy Function (the term SPF is defined herein)
SRTP	Secure Real-Time Protocol
TEID	Tunnel Endpoint ID
UDP	User Datagram Protocol
UE	User Equipment
UPF	User Plane Function
URI	Universal Resource Identifier
URSP	UE Route Selection Policy
XR	Extended Reality

[0081] The terms application server (AS) and Application Function (AF) may be used interchangeably herein. Edge application server (EAS) and edge enabler server (EES) functions may be hosted on the same hardware platform, or may be hosted on different hardware platforms. The terms AS and EAS may be used interchangeably herein.

[0082] The term "certificate" may refer to a public key certificate (e.g., X.509 certificate) as used herein. The terms "protocol data unit (PDU) set IEs" and "PDU set metadata" are used interchangeably herein.

[0083] The term information element (IE) may refer to or represent one or more parameters herein. An IE may include one or more IEs (e.g., other IEs).

[0084] Systems, methods, devices, and instrumentalities are described herein related to wireless transmit/receive unit (WTRU) based PDC operations, such as creation.

[0085] A device (e.g., a wireless transmit/receive unit (WTRU)) may include a processor configured to perform one or more actions. The device may send a first protocol data unit (PDU) message to a first network node, wherein the first PDU session message indicates a request for a protocol data unit (PDU) set handling data channel (PDC). The device may receive a second PDU message from the first network node, wherein the second PDU message indicates a second network node, indicates a PDU session, and comprises one or more candidate PDC setup IEs. The device may send a third PDU message to the second network node using the PDU session. The second PDU request message may indicate the request

for the PDC and comprises the one or more candidate PDC setup IEs. The device may receive a fourth PDU message from the second network node using the PDU session. The fourth PDU message may indicate a third network node and comprises one or more accepted PDU setup IEs based on the one or more candidate PDC IEs. The device may determine a PDU setup IE based on the one or more candidate PDU IEs. The device may send a fifth PDU message to the third network node using the PDU session, wherein the fifth message indicates the request for the PDC and comprises the PDU setup IE.

[0086] In examples, the discovery operation performed by the device to determine the EES information may include a determination of a trigger associated with a WTRU application and performing the discovery operation based on the trigger.

[0087] The trigger may indicate an establishment of an extended reality (XR) application session. The received PDU may be associated with the XR application session.

[0088] The PDU session operation may include receiving one or more of a candidate PDC setup information element, a PDC, or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) proxy.

[0089] The PDC establishment operation may include modifying the established PDU session with a Multiplexed Application Substrate over QUIC Encryption (MASQUE) proxy. The PDC establishment operation may include sending the PDC setup IE to the UPF via the MASQUE proxy.

[0090] The PDC setup IE may be a first PDC setup IE, and the device may perform the PDU session operation to send a second PDC setup IE to the UPF (e.g., via a session management function (SMF)).

[0091] Systems, methods, devices, and instrumentalities are described herein related to NEF-based PDC creation and operation (e.g., by an enabler server, such as an edge enabler server (EES)).

[0092] A device (e.g., an enabler server) may include a processor configured to perform one or more actions. The device may receive a session request message from a second network node. The session request message may indicate a request for a session. The session request message may include a protocol data unit set handling (PSH) data channel (PDC) setup information element (IE) and an indication of a Quality of Service (QoS) associated with the session. The device may determine a PDC should be established based on the request for the session, the PDC setup IE, and the indication of the QoS. The device may send a service request message to a third network node when it is determined that the PDC should be established, wherein the service request message comprises the indication of the QoS and PDC setup IE. The device may receive a service response message from the third network node. The second message may indicate the PDC has been established based on the PDC setup IE. The device may send a session response message to the second network node. The session response message may indicate that

the PDC is associated with the requested session and that the PDC has been established based on the PDC setup IE.

[0093] The device may receive a PDC provisioning IE. The device may receive a request for a PDC configuration from the EAS. The request for the PDC configuration may include a candidate PDC configuration IE. The device may determine an accepted PDC configuration IE based on the PDC provisioning IE and the PDC candidate IE. The device may send a PDC configuration response to the EAS indicating the accepted PDC configuration IE.

[0094] The PDC provisioning IE may include one or more parameters that may be supported by the network for PDCs. The candidate PDC configuration IE may indicate a protocol identifying a PDC supported by the EAS.

[0095] The PDC setup IE may include at least one of a protocol, an IP address, a port used to initiate a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection, an authentication method, or an authentication parameter.

[0096] Systems, methods, devices, and instrumentalities are described herein related to PDC creation and operation (e.g., by a user plane function (UPF)).

[0097] A device (e.g., a UPF) may include a processor configured to perform one or more actions. The device may receive a first message from a second network node. The first message may be associated with a protocol data unit (PDU) session and include a PDU set handling data channel (PDC) setup information element (IE). The device may send a second message to a third network node. The second message may indicate a request to create a PDC and include the PDC setup IE. The device may receive a third message from the third network node. The third message may indicate the PDC has been established. The device may determine that the PDC is associated with the PDU session based on the PDC setup IE. The device may receive a fourth message from the third network node using the PDC. The fourth message may include a PDU set IE and a downlink (DL) PDU. The device may determine that the PDU set IE is associated with the DL PDU. The device may send a fifth message to the second network node. The message may include the DL PDU and a header that includes the PDU set IE.

[0098] The message may include a header. The header may include the associated protocol data unit (PDU) set (PS) IE.

[0099] The message may be a first message including the PS IE. The device may send a second message to the network node. The second message may include the DL PDU.

[0100] Systems, methods, devices, and instrumentalities are described herein related to establishing a secure tunnel with a user plane function (UPF).

[0101] A device (e.g., a wireless transmit/receive unit (WTRU)) may include a processor configured to perform one or more actions. The device may determine a shared key. The shared key may be associated with a first network node. The device may send a first protocol data unit (PDU) message to a second network node. The PDU message may indicate a request for a PDU session and include a PDU set handling (PSH) tunnel security parameter based on the KAF. The device may receive a second PDU message from the second network node. The second PDU message may include a PSH channel security parameter. The device may send a connection request message to a third network node using the PDU session. The connection request message may include a request to establish a PSH tunnel based on the PSH channel security parameter. The device may receive a connection response message from the third network node using the PDU session. The connection response message may indicate that the PSH tunnel has been established. The device may send a PDU to the first network node using the secure PSH tunnel.

[0102] With the second network node, the device may authenticate a hash based on the PSH tunnel security parameter and an indication that a digest-based authentication method has been selected.

[0103] With the second network node, the device may authenticate a transport layer security (TLS) shared secret based on the PSH tunnel security parameter and an indication that a TLS with a shared-key mutual authentication method has been selected.

[0104] The device may authenticate the second network node based on the PSH channel security parameter and an indication that a certificate-based authentication method is selected.

[0105] The device may authenticate the second network node based on the PSH tunnel security parameter and an indication that a transport layer security (TLS) with a shared-key mutual authentication method is selected.

[0106] A device (e.g., a wireless transmit/receive unit (WTRU)) may include a processor configured to perform one or more actions. The device may establish a shared key (KAF) with an application function (AF). The device may send a protocol data unit (PDU) session request to a first network node. The first network node may provide a session management function (SMF). The PDU session request may indicate a request to communicate with the AF and include a PDU set handling (PSH) tunnel security parameter based on the KAF. The device may receive a PDU session response, including a PSH channel security parameter. The device may send a connection request to a second network node to establish a secure PSH tunnel. The second network node may include a user plane function (UPF). The connection request may include a PSH tunnel key based on the KAF and a PSH tunnel key identifier based on the PSH tunnel security parameter. Using the secure PSH tunnel, the device may send a PDU to the first network node. The second network node may be configured with the PSH tunnel security parameter.

[0107] Feature(s) associated with WTRU-based PDU set handling data channel (PDC) creation are provided herein (e.g., as may be applied to WTRU-based PDCs).

[0108] A WTRU may host an enabler client and/or an XR application. The WTRU may establish a PDC between a UPF and EAS (e.g., so the UPF may determine PDU Set information that may be associated with downlink traffic, for example, to the WTRU).

[0109] The WTRU may provide one or more PDC setup IEs to a user plane function (UPF) (e.g., via a multiplexed application substrate over QUIC encryption (MASQUE) proxy that may be collocated with the UPF). The WTRU may provide (e.g., alternatively) the PDC setup IE(s) to the UPF via a session management function (SMF).

[0110] In examples, one or more of the following may be performed (e.g., for a WTRU to provide one or more PDC setup IEs to a UPF).

[0111] A WTRU (e.g., an enabler client on the WTRU) may receive a trigger from a WTRU application. The trigger may be for establishing an extended reality (XR) application session. The WTRU may use policies and/or rules to determine that a PDC may (e.g. needs to) be requested for the application traffic.

[0112] The WTRU enabler client may perform a discovery operation (e.g., with an edge configuration server (ECS). The WTRU enabler client may request to be provisioned with information about an EES (e.g., multiple EESs) that may support PDCs (e.g., as part of the discovery operation). The WTRU enabler client may receive information about the EES (e.g., multiple EESs) that may support PDCs (e.g., as part of the discovery operation).

[0113] The WTRU application or enabler client may trigger the WTRU to send (e.g., to an SMF) a PDU session establishment and/or modification request. The request may include a request to communicate with an EAS and may include an indication that a PDC and/or MASQUE Proxy may be provided (e.g., may be needed).

[0114] The WTRU may receive (e.g., from the SMF) a PDU session establishment and/or modification response that may include PDU Setup IE(s). For example, the PDU Setup IE(s) may be MASQUE proxy IEs (e.g., an IP address, a port, security information, and the like). In examples (e.g., when the WTRU provides the PDC setup IEs through the SMF), MASQUE proxy IEs may not be received (e.g., MASQUE proxy IEs may not be requested and/or required by the WTRU).

[0115] The WTRU may send (e.g., to the discovered EES) a PDC configuration request that may include a candidate PDC setup IE(s). The PDC setup IE(s) may be based on policies, rules, and/or WTRU capabilities (e.g., the capabilities of the WTRU sending the PDC configuration request).

[0116] The WTRU may receive (e.g., from the EES) a PDC configuration response that may include an accepted PDC setup IE(s).

[0117] The WTRU may send (e.g., to the UPF) a MASQUE connection request that may include the MASQUE proxy IE(s) and PDC setup IE(s). The WTRU may (e.g., alternatively) send (e.g., to the SMF) the PDC setup IE(s) (e.g., in another message, for example, a PDU session modification request to the SMF).

[0118] The WTRU may receive a MASQUE connection response and/or a PDU session modification response.

[0119] The WTRU may receive PDU(s) (e.g., on the PDU session and/or, if applicable, over the MASQUE connection). The PDU(s) may correspond to the XR application session (e.g., that may have received a PS QoS handling service from the network).

[0120] Feature(s) associated with NEF-based PDC creation and/or operation (e.g., by an EES) are provided herein. NEF-based PDC creation and/or operation may be (e.g., similarly) implemented by one or more of an EES, a SEAL enabler server, a standalone PSH enabler server, or an XR enabler server.

[0121] In examples, an enabler server (e.g., an EES) may perform one or more of the following (e.g., to create and/or operate NEF-based PDCs). The EES may be provisioned with PDC provisioning IE(s) (e.g., including methods and parameters supported by the network for PDCs, such as protocols (MASQUE, GTP, etc.) and security IE(s), such as certificate(s)). The EES may (e.g., alternatively) receive the PDC provisioning IE(s) from an EAS.

[0122] The EES may receive (e.g., from an EAS) a request for PDC configuration. The request for PDC configuration may include candidate PDC configuration IE(s) (e.g., that may include the protocol(s) and/or parameter(s) identifying PDC(s) supported by EAS (e.g., the requesting EAS). A PDC may be, for example, a standard and/or protocol enabling the EAS to send (e.g., to the UPF) PDU(s) that may be associated with PDU set IE(s).

[0123] The EES may use local policies to determine accepted PDC configuration IE(s) from PDC provisioning IE(s) and/or candidate PDC configuration IE(s). The EES may send (e.g., to the EAS) a PDC configuration response that may include accepted PDC configuration IE(s).

[0124] The EES may receive (e.g., from the EAS) a request to trigger PDC establishment. The request to trigger PDC establishment may include PDC setup IE(s), which may indicate how to communicate with a PDC endpoint on the EAS (e.g., a protocol, an IP address, and/or a port that may be used to initiate a MASQUE/GTP tunnel connection with EAS and/or authentication methods and parameters).

[0125] The EES may send PDC setup IE(s) to the network (e.g., NEF or PCF). For example, the EES may invoke a NEF API for a session with QoS that may be enhanced to include PDC setup IE(s).

[0126] The EES may receive a response (e.g., from the network) indicating that the request (e.g., including PDC IE(s)) was accepted by the network. The EES may send a response (e.g., to an EAS) indicating that the network has been configured with PDC IE(s). The EAS may send downlink PDU(s) and PS IE(s) (e.g., to the WTRU) over the PDC. Sent downlink PDU(s) may receive a PS QoS handling service by the network.

[0127] Feature(s) associated with PDC creation and/or operation (e.g., by a UPF) are provided herein. PDC creation/operation may apply to NEF-based or WTRU-based PDCs. In examples, a UPF may perform one or more actions, such as the actions described herein (e.g., during PDC creation and/or operation).

[0128] The UPF may receive a PDC establishment message with PDC setup IE(s) (e.g., N4 session modification from the SMF and/or a MASQUE connection message from the WTRU). The UPF may initiate PDC creation with an application server (AS). The UPF may send PDC setup IE(s) (e.g., to the AS).

[0129] The UPF may configure itself to associate the PDC with the corresponding PDU session. The corresponding PDU session may be identified based on the PDC establishment message (e.g., the PDU session corresponding to the N4 session and/or the PDU session used to transport the MASQUE connection message). For example, the UPF may configure itself to forward the DL PDU(s) (e.g., received over the PDC) toward the RAN along with associated PS IE(s) (e.g., in a GTP-U header).

[0130] The UPF may receive PS IE(s) from the AS through the PDC. The UPF may receive a DL PDU from the AS through the PDC. The UPF may associate PS IE(s) (e.g., the received PS IE(s)) with the DL PDU. For example, PS IE(s) present in the same message carrying the DL PDU may be associated with the DL PDU. For example, PS IE(s) and DL PDUs that are carried in different messages and contain the same PDU Set ID may be associated together.

[0131] The UPF may forward the DL PDU to the RAN (e.g., in a GTP-U message that may include the corresponding PS IE(s) in its GTP-U header). This may ensure that the DL PDU is forwarded towards the WTRU (e.g., while receiving PS QoS Handling service from the network). Media flow UL PDUs may be forwarded through the tunnel or (e.g., alternatively) may be forwarded towards the AS (e.g., using IP routing).

[0132] Feature(s) associated with a secure tunnel with UPF (e.g., on the WTRU and AF side) are provided herein. In examples, a WTRU may perform one or more actions described herein, for example, to exchange tunnel keying material with a UPF. The WTRU may establish a shared key (KAF) with an application function (e.g., XR enabled server).

[0133] The WTRU may send (e.g., to the SMF) a PDU session establishment or modification request to communicate with an AF. The request from the WTRU may include PSH tunnel security parameters (e.g.,

PSH tunnel key/identifier). A PSH tunnel key may be set to the KAF, or a key derived from the KAF. The key identifier may be set to A-KID.

[0134] The WTRU may receive a PDU session establishment or modification response (e.g., from the SMF). The response may include PSH channel security parameters (e.g., authentication method(s) supported, such as certificate and/or shared key based authentication method(s), or a PSH server certificate).

[0135] The WTRU may send (e.g., to a UPF) a connection request (e.g., for the PSH tunnel security establishment). The WTRU may perform one or more of the following: the WTRU may authenticate with the UPF using a PSH tunnel key and an identifier (e.g., as a password and a username, respectively) to generate a hash to be verified by the UPF (e.g., if a digest-based authentication method is selected); the WTRU may authenticate with the UPF using a PSH tunnel key and an identifier to generate a TLS shared secret (e.g., if a TLS with shared-key mutual authentication method is selected); or the WTRU may authenticate with the UPF using the PSH server certificate (e.g., if certificate-based authentication is selected) or using a PSH tunnel key and an identifier (e.g., if TLS with shared-key mutual authentication is selected). The WTRU may send and/or receive PDU over the secure PSH tunnel.

[0136] In examples, a WTRU may perform one or more actions described herein to, for example, establish a tunnel shared key with a UPF (e.g., with AF assistance). The WTRU may establish a shared key (KAF) with an Application Function (e.g., an XR enabled server). The WTRU may send a PDU session establishment or modification request (e.g., to an SMF). The request may be a request for the WTRU to communicate with an AF. The request may include PSH tunnel security parameter(s) (e.g., KAF ID). The UPF may be configured (e.g., by the SMF) with PSH tunnel security parameters (e.g., a PSH tunnel key/identifier) provided by the AF (e.g., via a PCF/NEF). The PSH tunnel key may be set to the KAF, or a key based on (e.g., derived from) the KAF. The key identifier may be set to A-KID.

[0137] The WTRU may receive (e.g., from the SMF) a PDU session establishment or modification response including PSH channel security parameters (e.g., may include a supported authentication method such as a certificate-based and/or shared key-based authentication method, or a PSH server certificate).

[0138] The WTRU may use KAF or a derivation thereof as a PSH tunnel key. The WTRU may use the KAF ID as a PSH tunnel key identifier. The WTRU may send (e.g., to the UPF) a connection request for the PSH tunnel security establishment (e.g., as described above).

[0139] The WTRU may send and may receive PDU over the secure PSH tunnel. The establishment of a secure tunnel between the UPF and the AF may occur as described herein. For example, the UPF may use a key that may be provisioned from the AF (e.g., via NEF/PCF/SMF) to authenticate with the AF. Different

keys may be derived for each tunnel to ensure proper key separation between the WTRU-UPF and the UPF-AF tunnels (e.g., based on common KAF).

[0140] Feature(s) associated with PDC Creation/Operation (e.g., by an SMF) are provided herein. PDC creation/operation may be performed by an SMF and may apply to NEF-based or WTRU-based PDCs.

[0141] The SMF may receive UPF capabilities that may include, for example, PDC capabilities of the UPFs (e.g., in management plane messages or UPF capabilities messages). The SMF may receive a PDU session establishment message from the WTRU (e.g., that may include a PSH indication or PDC indication). The SMF may determine that a PDC may be used for this session, for example, based on the presence of a PSH and/or PDC indication in a message from the WTRU (e.g., a PDU session establishment message, such as described herein), and/or from the PCF (e.g., in a PCC rule).

[0142] The SMF may select a UPF that is PSH-capable and, using this UPF, may proceed with the PDU session establishment method. The SMF may receive a message with PDC setup IE(s) (e.g., in a PCC rule from PCF, in a PDU session modification request from the WTRU, etc.). The SMF may send a message to the UPF that may include the PDC setup IE(s) (e.g., a N4 session modification request message). The UPF may use the PDC setup IE(s) to establish the PDC with the AS.

[0143] The SMF may receive, from the UPF, a response message (e.g., an N4 session modification response message) indicating the status (e.g., success or failure) of the PDC establishment operation. The SMF may send a response message indicating the status (e.g., success or failure) of the PDC establishment operation (e.g., to the WTRU or to the PCF).

[0144] Feature(s) associated with PDC creation/operation (e.g., by an EAS or AS) are provided herein. PDC creation/operation may be performed by an EAS or AS and may apply to NEF-based or WTRU-based PDCs.

[0145] The EAS may receive an application session initiation request from a WTRU. The EAS may use information (e.g., from the application session initiation request) to determine whether to use a PDC.

[0146] If the \ EAS-initiated, the EAS sends a request for PDC configuration (e.g., including candidate PDC configuration IEs) to an EES. The EES may be a SEAL enabler server, a standalone PSH enabler server, an XR enabler server, or the like.

[0147] The EAS may receive (e.g., from the EES), a PDC configuration message with accepted PDC configuration IE(s). The EAS may configure a PDC endpoint (e.g., using the accepted PDC configuration IE(s)). The EAS may send (e.g., to the EES) a PDC establishment message (e.g., including PDC setup IE(s)). The EES may provide PDC setup IE(s) to a WTRU or network. PDC setup IE(s) (e.g., provided by the EES to a WTRU or network) may reach the UPF.

[0148] The EAS may receive (e.g., from UPF) a request to establish a PDC (e.g., a connection establishment request or key generation request). The EAS may perform an establishment method (e.g., a protocol-dependent establishment method), which may include sending and/or receiving additional message(s). The EAS may send media data PDUs and associated PS IEs through the PDC. The PDUs may be transported by the network to the WTRU application (e.g., while applying the PDU set QoS handling service).

[0149] Feature(s) associated with the service provisioning of an EES with PSH Support (e.g., by an ECS) are provided herein. Service provisioning of an EES with PSH Support (e.g., by an ECS) may apply to NEF-based or WTRU-based PDCs.

[0150] The EES may be configured for PSH or PDC support (e.g., the EES may host software supporting PDC-related methods as described herein). The EES may be deployed in a DN accessed through UPF(s) that supports PDC. Such an EES may be referred to as a PSH-enabled or PDC-enabled EES.

[0151] The WTRU may be configured with a PSH or a PDC indication (e.g., PDC requested/preferred/allowed/disallowed indication) for media flow (e.g., in a policy rule such as a UE Route Selection Policy (URSP) rule).

[0152] The ECS may receive EES registration. The received EES registration may include a PSH or PDC support indication. The ECS may store the PSH or PDC support indication with other EES registration state information. The ECS may receive a discovery request (e.g., from the WTRU), including a PSH or PDC indication (e.g., such as a requested, preferred, allowed, or disallowed indication).

[0153] The ECS may select one or more EES using EES registration state information (e.g., that may include a PSH or PDC support indication). The ECS may respond (e.g., to the WTRU) with a list of selected EES and related EDN information (e.g., including PSH or PDC support indications).

[0154] Feature(s) associated with XR traffic handling by wireless networks and PDU sets are provided herein. Wireless networks may carry media flows (e.g., for applications with high-throughput and low latency requirements, such as video conferencing and XR). Wireless networks may implement techniques to improve network capacity and energy efficiency. Wireless networks may implement techniques to reduce the impact of packet losses on user experience. For example, wireless networks may handle groups of packets based on how critical the groups of packets are to the user experience. Some groups of data packets may hold application data units that are handled together (e.g., decoded) by the application, which may be referred to as PDU set. A PDU set may, for example, correspond to the PDUs carrying a Network Application Layer (NAL) unit (e.g., a single complete NAL unit).

[0155] The network (e.g., RAN) may perform differentiated/integrated QoS handling of XR traffic to support high-throughput, low-latency media flows. This may include prioritizing PDU sets over others (e.g., other data packets) in case of congestion. The network handling may be based partly on the dependency of application data units (e.g., on other application data units) to be handled or decoded by the application (e.g., P-frames depend on I-frames, and enhancement layers depend on base layers). The network may (e.g., selectively) drop data packets that depend on an application data unit that has already been lost. The network may limit wake-up time (e.g., of radios) to transmit and receive data. For example, the packet scheduler (e.g., in RAN nodes) and/or WTRUs may synchronize their transmission and listening times using information on one or more of a traffic size, a periodicity of traffic, a delay budget, and/or an expected jitter specific to the application.

[0156] The RAN may perform differentiated/integrated QoS handling of XR traffic based on differentiated/integrated handling IEs associated with a flow and/or PDU sets inside the flow. Differentiated/integrated Handling IEs may include PDU Set QoS parameter(s) (e.g., received via the control plane) and PDU set information (e.g., received via the user plane). For downlink traffic, PDU set information may be sent by the UPF to the RAN node (e.g., via a GTP-U header of a user plane packet). For uplink traffic, PDU set information may be provided by a WTRU application (e.g., through the SDAP interface).

[0157] The term protocol data unit set information element (PDU set IE) may be used to represent IE(s) described herein as PDU set information and PDU set QoS parameters. The term PDU set IE may be abbreviated PS IE.

[0158] PDU set information may include one or more of the following: PDU Set ID; start/end of a PDU set indication; PDU sequence number; PDU set size; PDU set importance; end-of-burst indication; XR application session ID; XR session priority; XR flow ID; XR flow priority; XR synchronization group ID; list of applicable network services; PDU set type; PDU FEC parameters; PDU parent set ID; and/or timing IEs.

[0159] PDU set ID may be an IE that is an identifier of a PDU set, which may identify (e.g., uniquely identify) the PDU set within a flow (e.g., at least for a duration corresponding to the transmission time of PDUs between sender and receiver). PDU set ID may be, for example, a numerical ID, a timestamp, a combination thereof, and/or the like.

[0160] Start/end of a PDU set indication may be IEs that identify the first/last PDU(s) of a PDU set.

[0161] A PDU sequence number within a PDU Set may be an IE that identifies a PDU within a PDU set (e.g., a numerical ID starting at 0 for the first PDU and incremented by 1 for each PDU in the set).

[0162] PDU set size may be an IE that holds one or more of the total number of PDUs, the cumulative length of all the PDUs in a set, or the cumulative length of all PDU payload(s) (e.g., transport payload) in the PDU set.

[0163] PDU set importance may be an IE that is a value (e.g., numerical value) indicative of the importance level of a PDU set within a service flow (e.g., from highest priority value 0 to lowest priority value 255). RAN may use PDU set importance for PDU set level packet discarding (e.g., during a period of congestion).

[0164] An end-of-burst indication may be an IE that indicates a PDU or a PDU set is the last PDU or PDU set of a burst. The end-of-burst indication may also include IEs indicating an amount of time before a next burst. PDU set information may include XR session information and/or XR parameters.

[0165] An XR application session ID may identify the session (e.g., to provide a scope for prioritizing, scheduling, and synchronizing flows, packets, and PDU sets). An XR application session priority may provide a priority for inter-session prioritization. In examples, priority may be used to prioritize between flows belonging to different application sessions (e.g., that have a same flow priority).

[0166] An XR flow ID may identify the flow (e.g., for applying XR service on the flow). An XR flow ID may be provided by the mobile network (e.g., it may be a PDU Session ID). An XR flow priority may provide a priority for inter-flow prioritization. A data type (e.g., audio, video, haptic, data) may be used for inter-flow synchronization (e.g., to determine the acceptable synchronization delay between flows). An XR synchronization group ID may indicate which flows of the application session may be synchronized (e.g., with each other).

[0167] A list of applicable network services may indicate which network services (e.g., including PDU QoS set handling) may be applicable and/or may include additional services, such as increased reliability (e.g., using multipath connectivity such as provided by access traffic steering, switching, and splitting (ATSSS)), low-latency delivery, etc. The list of applicable network services may be used by the network to determine which level of service may be provided to a given PDU set.

[0168] A PDU set type may be used to associate a domain-specific meaning with a PDU set (e.g., I-frame, P-frame, B-frame). PDU set type may be useful to provide XR services (e.g., where specialized processing may be required for selected types of PDU sets).

[0169] PDU FEC parameters may include an FEC algorithm and its parameters. PDU FEC parameters may be used (e.g., by WTRU/UPF/AS) to recover lost packets in a PDU set protected by FEC.

[0170] A PDU parent set ID may identify a parent PDU set that is to be received (e.g., is required to be received) by the application (e.g., for the child PDU set to be usable by the application).

[0171] Timing IEs may include one or more of a media unit timestamp, a presentation timestamp, a sending time timestamp, an accumulated transmission delay, or a PDU synchronization ID. A PDU synchronization ID may identify a group of inter-related PDUs that may be presented to the user at a similar time, within the same flow (e.g., a set of frames that must be presented to the user at the same time in a multi-screen setup), and/or between different flows (e.g., a video PDU that must be presented to the user together with a haptic PDU).

[0172] PDU set QoS parameters may be a set of parameters to configure the QoS handling of a flow. PDU set QoS parameters may include one or more of: a PDU set error rate, a PDU set delay budget, PDU set integrated indication (PSII), and/or a burst periodicity.

[0173] A PDU set error rate may be an IE value that corresponds to error rates applicable to PDU sets (e.g., where a PDU set loss corresponds to an event where at least a PDU of the set could not be transmitted successfully). A PDU set error rate may be used to configure the acceptable error rate for PDU sets of a service flow or QoS flow in the RAN.

[0174] A PDU set delay budget may be an IE value that corresponds to the acceptable delay for transmitting a full PDU set (e.g., from the reception of the first PDU of the set to the transmission of the last PDU of the set). PDU set delay budget may be used to configure the delay budget for a service flow or QoS flow in the RAN. A PDU set integrated indication (PSII) may be an IE that indicates whether one or more PDUs (e.g., all PDUs) of the set are needed by the application.

[0175] A burst periodicity may be an IE value that designates the period of a data burst for this flow (e.g., transmission period for consecutive independent frames in a video stream; e.g., transmission period for a group of pictures).

[0176] A PS identification may indicate which PDU set a PDU belongs to and may include the identification of PS IEs that may be associated with the PDU set. For media over the RTP protocol, The UPF may perform this operation for downlink flows. Identification of PS IEs may include one or more of inspecting traffic, detecting information elements, or determining the value of IEs that may be associated with the PDU set.

[0177] PS QoS handling (also called herein, for simplicity, PS Handling or PSH) may designate the operation (e.g., in RAN and/or in UPF) that includes providing differentiated handling depending on PS IEs (e.g., dropping PDUs of lower PS importance in case of congestion).

[0178] Feature(s) associated with encrypted media transport are provided herein. An encrypted media transport protocol may prevent certain intermediaries (e.g., intermediaries not explicitly trusted by an endpoint and inserted in the connection) from performing PDU set identification. Encrypted media protocols may include HTTP-based stream protocols (e.g., when using TLS for transport), SRTP when used with

encrypted RTP extensions (e.g., such as described in RFC9335), and media over QUIC protocols (MOQ). MOQ protocols may be a family of protocols that carry media over QUIC, including WARP and RTP over QUIC. An intermediate node that terminates the QUIC connections and relays the MOQ protocol between these connections may be called a MOQ relay or (e.g., equivalently) a MOQ proxy. A MOQ relay may be an intermediary trusted by an endpoint, which may access transport-layer metadata in the flow and may perform PDU set identification.

[0179] Feature(s) associated with multiplexed application substrate over QUIC encryption (MASQUE) are provided herein. The MASQUE protocol may be used to configure and run multiple proxied flows in an HTTP connection (e.g., using HTTP/3 over QUIC). The MASQUE services may include a CONNECT-UDP service, which enables transporting UDP traffic between a client and a proxy, or between two proxies. The transported UDP traffic may be, for example, an MOQ traffic. To initiate a CONNECT-UDP service, the client may send an HTTP CONNECT request to a proxy (e.g., using a URI such as `https://masque.example.org/{target_host}/{target_port}/`, where `masque.example.org` is an FQDN resolving into a MASQUE proxy, where `{target_host}` is a remote server FQDN or IP address, and where `{target_port}` is the target UDP port on the remote server). The HTTP CONNECT may include a CONNECT-UDP service label (e.g., as a protocol pseudo-header value or as an upgrade header value). A MASQUE proxy may send a CONNECT-UDP request to the next proxy (e.g., in a chain of proxies), or, if there is no additional proxy, the MASQUE proxy may forward UDP traffic between the client and the remote server (e.g., upon accepting such a request). During operation, the UDP payload may be sent over the proxied connection (e.g., between client and proxy, and/or between proxy and proxy), in an HTTP datagram or in a datagram CAPSULE message in cases where HTTP datagrams may not be supported. The UDP payload may be sent over UDP between the last proxy and the server. Data traffic between the MASQUE proxy and the remote server may be typically transmitted over UDP/IP. A MASQUE proxy may provide other services: for example, IP proxying may be initiated with a CONNECT request (e.g., including a CONNECT-IP service label).

[0180] Feature(s) associated with edge computing and service enabler architecture layer (SEAL) framework are provided herein. The edge computing capabilities may be supported by mobile networks. Edge computing capabilities may allow WTRU applications to locate and connect with the most suitable application server available in an edge data network. An edge enabler layer in mobile networks may expose APIs to support such capabilities. The edge enabler layer may be enhanced (e.g., to support the methods defined herein), and the network functions defined as part of the architecture for enabling edge applications in mobile networks may be used (e.g., in the methods defined herein). The architecture that may enable edge applications in mobile networks may define one or more of the following network

functions: an application client (AC); an Edge Enabler Client (EEC) (e.g., in the WTRU); or an edge configuration server (ECS).

[0181] An AC (also referred to herein as a WTRU application) on a WTRU may need to communicate with an edge application server (EAS) located in an edge data network (EDN).

[0182] An EEC (e.g., in the WTRU) may provide supporting functions that may be needed for ACs, such as supporting retrieval of configuration information to enable the exchange of application data traffic with EAS, discovery of EAS, and/or detecting WTRU mobility events. In the EDN, an edge enabler server (EES) may provide supporting functions for EAS and EEC, such as provisioning of configuration information to EEC, providing APIs to EAS for accessing mobile network services and events, facilitating WTRU mobility support, registering with ECS to enable discovery by WTRU, and/or the like.

[0183] ECS may provide supporting functions for an EEC to discover and connect with an EES.

[0184] Feature(s) associated with enabling edge applications in mobile networks are provided herein. In examples, one or more of the following may be performed when enabling edge applications in mobile networks: service provisioning, EES registration, EEC registration, and/or EAS discovery.

[0185] Service provisioning may include an EEC requesting service provisioning from an ECS. Service provisioning may include ECS identifying suitable EES(s) (e.g., using information such as WTRU location and AC profile). Service provisioning may provide the EEC with a list of suitable EES(s). Related EDN configuration information, which may include one or more of an identification (e.g., DNN), an EDN service area, or information for establishing a connection to the EES (e.g., URI, IP address), may be provided (e.g., for each EES).

[0186] EES registration may include an EES sending a registration request to an ECS. The ECS may store the registration information provided in the request (e.g., EES profile and EES security credentials) for future use (e.g., for service provisioning methods).

[0187] EEC registration may include an EEC sending a registration request to the EES (e.g., which may include security credentials and may include other information, such as an AC Profile). The EES may create an EEC context. The EES may return an EEC context ID to the EEC. The EEC context ID may be later used to facilitate the transfer of the EEC context to another EES (e.g., when the WTRU moves to a new location).

[0188] EAS discovery may include an EEC sending an EAS discovery request to an EES (e.g., including a requestor identifier, security credentials, and/or other information, such as WTRU location). The EES may validate the request. The EES may identify EAS(s) and may send a response including information about the discovered EAS(s), such as endpoint information (e.g., IP address, FQDN, port, protocol, and/or URI to enable communication establishment).

[0189] SEAL may be a framework and a set of services to support vertical applications (e.g., over the 3GPP system). SEAL services may include management services for groups, configurations, locations, identities, keys, network resources, notifications, and/or enablement services for network slice capabilities, data delivery, and/or application data analytics. SEAL architecture may request (e.g., require) a SEAL client (e.g., on the WTRU) and a SEAL server (e.g., in the network), which may be communicating with each other and with, respectively, an application client (e.g., on the WTRU) and an application server (e.g., in the network). SEAL may be used independently to support an application. SEAL may be used with an edge computing framework to support an application.

[0190] Feature(s) associated with authentication and key management for applications (AKMA) are provided herein. AKMA mechanisms may be provided to allow a WTRU and an application function (AF) to establish a shared key (KAF) based on subscription credentials. The WTRU may generate an AKMA key and/or an identifier (A-KID) following a primary authentication with an authentication server function (AUSF). The AKMA key may be stored (e.g., in the WTRU and in an AKMA Anchor Function (AAnF)). The WTRU may establish the shared application key KAF with the AF by providing the A-KID. The AF may obtain a KAF from the AAnF. The WTRU and AF may establish the application layer security based on the KAF (e.g., using TLS based protocols with shared key).

[0191] FIG. 2 depicts example processes (e.g., process families) for PS identification of downlink encrypted traffic. The depicted example processes may be used alone or in combination to perform PS identification of downlink encrypted traffic.

[0192] At 201, which may be referred to as process family one, the UPF may act as a proxy for MOQ traffic. The proxy may be used to have access to transport signaling, which may be used to perform PDU set identification.

[0193] At 202, which may be referred to as process family two, the proxy or the AS, located in a DN, may perform PDU set identification. The proxy or the AS may transmit PDU set information to the PSA UPF (e.g., with encrypted PDUs), for example, using header fields accessible by the UPF (e.g., either without encryption or with encryption that is decryptable by the UPF).

[0194] At 201 (e.g., process family one) the network may be requested (e.g., UPF) to be a media intermediary node trusted by the application client and server. At 202, the trust relationship (e.g., of process family two) may be associated with the exposure of specific metadata between the AS and the UPF.

[0195] At 202, (e.g., process family two) an AS may provide the necessary metadata to the network (e.g., 5G system) without requesting the network to be an intermediary trusted by the endpoints. This may include one or more of the following use cases: when the AS is an edge CDN node (e.g., MOQ relay

operated by an entity in the 5G operator's edge network); when the AS is a media server at the edge; or when the AS is a media server or CDN node in the distant cloud.

[0196] The EAS may use UDP transport layer options to carry unencrypted PDU set information to the PSA UPF. The PDU set information IEs may be placed in a UDP option in a UDP datagram (e.g., where the payload of the UDP datagram may be a PDU associated with the PDU set information IEs). The EAS may establish a tunnel with a UPF whose identity and IP Address may be known by configuration.

[0197] Feature(s) associated with a secure and flexible provision of PDU set information (e.g., by the EAS) to the PSA UPF that may be used for a connection are provided herein. Feature(s) associated with PDC establishment and operation are provided herein.

[0198] A PDC may be a logical connection between a first node and a second node. The first node may use the connection to send PDU sets and/or PS IEs to the second node. The PS IEs may be associated with the PDU sets. The PS IEs may be identified by the second node. The second node may use the PS IEs to determine what QoS treatment is requested (e.g., required) for the PDUs of the PDU set.

[0199] When the PDC connection between the first and second nodes uses a tunneling protocol, the PDC may be referred to as a PSH Tunnel. A PDC may be described by a combination of one or more of the protocols that may be used by the first and second nodes to communicate, the security protocols that may be used by the first and second nodes, a tunnel identifier, or the format of the media data that is sent between the first and second nodes.

[0200] The first node and second node may participate in methods to configure and establish the PDC. Configuring and establishing the PDC may mean that the first and second nodes determine the description of the data channel. The description of the data channel may include one or more of the protocols that may be used, the format of the media that may be sent in the PDC, or the IP addresses of where data may be sent.

[0201] A third node may participate in the methods to configure and establish the PDC. For example, the third node may be known or trusted by both the first and second nodes. The first and second nodes may communicate with the third node to discover capability information and establish the PDC.

[0202] The first node may be an application server or an application function, such as an EAS. The first node may be an application that is hosted (e.g., on a WTRU), such as an application client or an enabler client. The first node may be a proxy function.

[0203] The second node may be a UPF. The second node may be a proxy function.

[0204] The third node may be an enabler server, such as an EES.

[0205] A PDC may be established on-demand between the AS (e.g., a media server or a proxy CDN node) and the PSA UPF. Multiple types of PDC may be used. Feature(s) associated with some exemplary PDC implementations are provided herein. Once the PDC is established, the AS may send media data along with related PS IEs over the PDC, and the network (e.g., 5G system) may use PS IEs to provide a PS QoS handling service on downlink media traffic.

[0206] The mechanisms and methods described herein may use a PSH enabler server component and a PSH enabler client component. The PSH enabler server component may be in the same DN as the application server and interwork with a PSH enabler client (e.g., on the WTRU). The PSH enabler components' role may be to facilitate the configuration and establishment of a PDC. The PSH enabler server component may be integrated with other enabler functions, such as an EES or a SEAL server. The PSH enabler client component may be integrated with other enabler functions, such as an EEC or a SEAL client.

[0207] The mechanisms and methods described herein may be described in the context of the edge computing framework, and the terms EES and EEC may be used to designate, respectively, an EES enhanced to include a PSH enabler server component, and an EEC enhanced to include a PSH enabler client component. In examples, the mechanisms and methods described herein may be applied to other types of enabler servers and clients (e.g., a SEAL server and client, or an XR enabler server and client). It should be appreciated that the terms EEC, EES, EAS may be replaced with enabler client, enabler server, and AS, to describe these mechanisms and methods as used here.

[0208] FIG. 3 depicts an example of configuring, establishing, and operating PDCs. At 1, the network operator and/or application provider may provision PDC provisioning IEs (e.g., in the network and EES) to enable future decisions to use PDCs and to enable setting up PDCs.

[0209] At 2, the WTRU and/or EAS may decide to use a PDC for media delivery (e.g., based on application logic and/or policy). The WTRU may indicate a parameter (e.g., requirement) for PDC when discovering EES and/or EAS.

[0210] At 3, the EAS and/or EES may configure the PDC (e.g., by determining the PDC configuration IEs based on PDC provisioning IEs). The PDC endpoint may be ready for connection on EAS, and PDC setup IEs may be available for the next process (e.g., as an outcome of the EAS and/or EES configuring the PDC).

[0211] At 4, the PDC may be established. For example, establishment may be initiated by the PSA UPF or by the WTRU through the PSA UPF. The establishment of the PDC may be based on PDC setup IEs.

[0212] At 5, the EAS may identify a PDU set and send PDUs and associated PDU set IEs over the PDC. The UPF may receive (e.g., from the PDC) PDUs with associated PDU set IEs. The UPF may forward PDUs toward the RAN. The RAN may apply (e.g., using the PDU set IEs) a PDU set QoS handling service while forwarding the PDUs toward the WTRU. At 6, the PDC may be closed (e.g., from either side of the connection).

[0213] Types of IEs may include PDC provisioning IEs, PDC configuration IEs, PDC setup IEs, and UPF MASQUE proxy IEs. NEF-based PDC establishment and operation may be performed (e.g., where PDC setup IEs may be provided to the network through a NEF API or through a PCF API). WTRU-based PDC establishment and operation may be performed (e.g., where PDC setup IEs may be provided to the network through the WTRU). A PDC may be established for a single flow, multiple flows, and/or one or more types of PDU sets. Traffic (e.g., for an XR application) may be carried over one or more PDCs. A PDC (e.g., each PDC) may carry a set of flows or PDU sets, which may enable different QoS to be applied (e.g., on the PDCs). In examples, a single PDC may carry all PDU sets between the AS and the UPF (e.g., for all flows corresponding to a WTRU application).

[0214] FIGs. 4A-4B depict an example of PDC operation on the data plane. The operational state of a PDC (e.g., as represented at 5 in FIG. 3) may be depicted as the flow B in FIG. 4A. At A-B, PDU set IEs may be identified by the application on EAS, associated with downlink PDUs, and sent (e.g., along with their corresponding PDUs) towards the UPF through the PDC endpoint on the EAS. The term "PDC endpoint" may correspond to a network node functionality, such as a tunnel endpoint, which may expose a network interface to the network (e.g., to send/receive PDUs to/from a remote PDC endpoint), and may expose an interface (e.g., network interface or programmatic interface) to an EAS application. At C-D, the UPF may obtain the PDUs and related PDU set IEs from the PDC. The UPF may forward the PDUs and related PDU set IEs toward the RAN (e.g., over the PDU session GTP tunnel). At E, the RAN may use the PDU set IEs to apply PDU set handling. The RAN may forward the PDUs toward the WTRU.

[0215] As described herein, the PDUs and PDU set IEs sent in A and B of FIG. 4A may use different messages (e.g., a sequence of one PDU set IEs message associated with a PDU set ID, and one or more PDUs each associated with the same PDU set ID), or use associated PDU set IEs and PDUs in one message (e.g., the same message) (e.g., each PDU is sent with a header containing the PDU set IEs).

[0216] Feature(s) associated with PDC provisioning are provided herein. A PDC may be a transport mechanism that enables transporting PDUs associated with metadata such as PS IEs. The PDC may be between the UPF, or a node collocated with the UPF and an AS (e.g., EAS, or MEC platform hosting an EAS). Feature(s) associated with several exemplary PDCs and with PDC setup information are provided

herein (e.g., GTP, MASQUE, UDP option based PDC, and other technologies may be used to securely transport PDUs and related PS IEs between AS and UPF).

[0217] A PDC may be a GTP tunnel (e.g., between UPF and AS) using a PDU set metadata extension, which may define new fields in the GTP packet header to hold PS IEs. IPSec or other mechanisms may be used to secure the GTP tunnel.

[0218] To set up a GTP-based PDC (e.g., between AS and UPF), both endpoints may obtain (e.g., from the other endpoint) a tunnel endpoint identifier (TEID). Certificates may be configured on endpoints (e.g., UPF and AS) to enable the establishment of a security association for the secure tunnel (e.g., using the IKEv2 protocol).

[0219] A PDC may be a "CONNECT-UDP" MASQUE connection (e.g., between UPF and AS) using a PDU set metadata extension. "CONNECT-UDP" MASQUE may be well suited for carrying UDP-based media traffic such as MOQ and SRTP. An endpoint (e.g., UPF) may send an HTTP CONNECT (e.g., HTTP extended CONNECT request with "connect-udp" protocol pseudo-header) to the MASQUE proxy (e.g., AS), indicating the target URI, for example, a URI pointing to an AS or an origin server beyond the AS. In a typical example, the AS may act as a MASQUE proxy and a target server. If the request is accepted by the MASQUE proxy, UDP payload PDUs may be carried between the UPF and AS (e.g., in datagram messages). A MASQUE extension for carrying PS IEs may be used. When the application on the AS sends a downlink media PDU to the WTRU, the AS may perform PS identification and may obtain the PS IEs for the PDU. Acting as a MASQUE proxy, the AS may send (e.g., to the UPF) the PS IEs and the associated UDP payload PDU in a datagram message. The AS may (e.g., alternatively) send the PS IEs and associated UDP payload PDU in separate messages (e.g., using the same value in an ID field in each message to allow the UPF to retrieve the association between the PDU and related PS IEs). When the UPF receives the UDP payload PDU and associated PS IEs, the UPF may add an IP header and UDP header to re-create the IP packet PDU to send to the WTRU. The UPF may send the IP packet PDU and associated PS IEs in a GTP-U message toward the RAN. The RAN may obtain and use the GTP-U message (e.g., as usual) to provide the PS QoS handling service. The RAN may forward the PDU toward the WTRU.

[0220] A PDC may be a CONNECT-IP MASQUE connection using a PDU set metadata extension. CONNECT-IP MASQUE may carry a (e.g., any) IP-based media protocol. The CONNECT-IP MASQUE connection may be similar to the "CONNECT-UDP" MASQUE connection scenarios. The CONNECT-IP MASQUE connection may use a CONNECT-IP protocol pseudo-header in the initial CONNECT request, and the MASQUE connection may carry IP packet PDUs in datagram messages (e.g., instead of UDP payload PDUs).

[0221] To set up a MASQUE-based PDC between AS and UPF, the initial sender of the HTTP CONNECT (also called the MASQUE client) may be configured with some IEs, which are used to create the HTTP CONNECT request and send it to the MASQUE proxy. These IEs may include the IP address or FQDN and port of the MASQUE proxy, a template URI (e.g., that describes how to build the target URI), target server IP address or FQDN, port, and resource path (e.g., used along with the template to build the target URI). Certificates may be configured on endpoints (e.g., to enable peer authentication between AS and UPF).

[0222] A PDC may use a UDP option to carry (e.g., between UPF and AS) PDU set metadata associated with the PDU present in the corresponding UDP payload. Carrying PDU set metadata in cleartext may be a security vulnerability. A secure tunnel (e.g., IPSec) may be used to provide confidentiality. In an example, another PDC may use an IP option (e.g., instead of a UDP payload option).

[0223] To set up a UDP or IP option-based PDC between AS and UPF, certificates may be configured on AS and UPF (e.g., to enable peer authentication when establishing a security association for the secure tunnel).

[0224] A PDC may be a CONNECT-UDP MASQUE connection initiated by the WTRU through UPF and may use a PDU set metadata extension between the UPF and EAS. The WTRU (e.g., after discovering the EAS) may initiate the establishment of a MASQUE connection with UPF. The UPF may send a CONNECT-UDP request to the EAS to create a MASQUE connection with two legs (e.g., WTRU-UPF and UPF-EAS). On the UPF-EAS leg, a PDU set metadata extension may be used. This scenario operates similarly to the MASQUE scenario described herein. For example, this scenario may include one or more of the following: a MASQUE proxy may be instantiated on the UPF, and the WTRU may (e.g., should) be made aware of the UPF MASQUE proxy IP address and port; the WTRU may directly or indirectly provide (e.g., to the UPF) the EAS IP address and port (e.g., obtained from EES) (e.g., for example using the CONNECT-UDP message to UPF) using a PDU session modification request to SMF; the UPF may send a CONNECT-UDP message towards the EAS to establish the second leg of the MASQUE connection, and may include a PDU set metadata extension indicator in the CONNECT-UDP message to request this extension to be used on this leg; during operation, the UPF may obtain PS IEs associated with DL PDUs, and may forward PDUs between the MASQUE connection legs (e.g., placing PS IEs in GTP-U headers encapsulating DL PDUs forwarded to the RAN). In examples, the WTRU-UPF leg of the MASQUE connection may also support a PDU set metadata extension, and the UPF may send the PDU set IEs to the WTRU. This may allow the WTRU to perform a PDU Set QoS handling operation (e.g., where the WTRU is not the final destination of the PDUs, such as when the WTRU is used as a relay). For example, in case of congestion, the WTRU may drop PDUs from low importance PDU sets to preserve the application QoE.

[0225] Feature(s) associated with PDC provisioning IEs are provided herein.

[0226] PDC provisioning IEs may include PDC security provisioning IEs and PDC capabilities IEs. PDC provisioning IEs may be used to determine whether a PDC may be used (e.g., a WTRU may decide to use a PDC if the mobile network supports PDCs), and/or to determine the PDC configuration (e.g., which protocol and which certificates to use for a specific channel).

[0227] PDC security provisioning IEs may include one or more of the following: a list of supported methods for authenticating and securing PDC, a list of public key certificates, and/or a list of identifiers.

[0228] PDC security provisioning IEs may include a list of supported methods for authenticating and securing PDC, e.g., that may include public key certificates and shared key methods. The supported methods may be associated with a UPF, DN, EES, EAS, AS, or AF (e.g., one method to authenticate UPF to EAS, another method for authenticating EAS to UPF, etc.; a method associated with an EES may apply to all EAS associated with this EES; a method associated with a DN may apply to all EAS deployed in this DN).

[0229] PDC security provisioning IEs may include a list of public key certificates (e.g., X.509 certificates) and related private keys, that may be deployed on UPF and EES (e.g., to enable EES and UPF to authenticate each other, for example, a public key certificate A and related private key may be deployed on EES, and UPF may be provisioned with A as a trusted certificate, which may enable UPF to authenticate EES, and vice-versa with public key certificate B and related private key deployed on UPF, and EES provisioned with B as a trusted certificate). The element(s) of the list of certificates and related private keys may be associated with a preference order (e.g., to progressively phase out or replace a certificate). PDC security provisioning may be made by the UPF and EES (e.g., directly on the UPF and EES) or may be indirectly configured. For example, PDC security provisioning IEs may be configured in the UPF by the SMF. The SMF may be provisioned by the operator (e.g., through a network management system).

[0230] PDC security provisioning IEs may include a list of identifiers that may be used (e.g., by UPF, AF) to establish shared keys with the network (e.g., from an AANF) or with a third-party system (e.g., an AAA server).

[0231] PDC capabilities IEs may include an indicator that PDCs may be supported, and/or a list of supported PDC protocols (e.g., GTP, MASQUE, UDP option). The elements of this list may, in some cases, be associated with a preference order (e.g., this may make it possible to progressively phase out or phase in a protocol in a network). The PDC capabilities of UPF and EAS and their underlying platform may be configured by network operators in EES, EAS, UPF, SMF, and/or PCF. The SMF may use the PDC capabilities of UPFs during UPF selection (e.g., to select a PSH-enabled UPF). The SMF may determine to select a PSH-enabled UPF based on input from the WTRU (e.g., PSH indication present in a PDU session

establishment or modification message) and/or based on policy (e.g., PSH indication present in a PCC rule).

[0232] PDC provisioning IEs may be provisioned (e.g., by a network operator) in the network (e.g., SMF, UPF, PCF), in the edge network (e.g., EES), and/or in WTRUs (e.g., UEs). PDC provisioning may be performed by the 5G network operator, or (e.g., for EES) by an edge network operator with a business agreement with the 5G network operator. PDC provisioning may be performed through a network management operation (e.g., using a protocol such as NETCONF or SNMP) or through a policy configuration API (e.g., network exposure function (NEF) API). Based on an agreement with an application provider, the network operator may provision some PDC provisioning IEs in policy entries (e.g., PCC rules), for example, to indicate that an application may be used with a PDC. The application provider may also be involved in provisioning (e.g., a WTRU application or EAS application may be provisioned with a "PDC supported" indication, which indicates to the application that it may attempt to set up a PDC).

[0233] Feature(s) associated with determining to use a PDC and EES/EAS discovery are provided herein. The decision to use a PDC may originate from the WTRU and/or the EAS.

[0234] A WTRU may determine that a PDC may be used or not (e.g., should be allowed, disallowed, required, or preferred) for a given service data flow through policy, and/or based on an indication from the WTRU application.

[0235] In examples of policy-based determination, the WTRU may determine that a service data flow (e.g., based on traffic descriptor IE such as application descriptor, IP descriptor, domain descriptor, etc.) matches a URSP rule that may include a PDC required, PDC preferred, PDC allowed, or PDC disallowed indication. The PDC indication (e.g., PDC required/preferred/allowed/disallowed indication) may be configured by an AF by associating the PDC indication with a service data flow or QoS flow in a NEF API. The PDC indication may be configured by the network operator in a PCC rule in PCF (e.g., in association with a service data flow or a QoS flow) based on AF configuration or based on an operator determination (e.g., an operator may by default always configure a PDC required/preferred/allowed/disallowed indication for specific XR applications or media protocols served from edge networks). The operator may also consider subscriber information when determining whether a PDC is required, preferred, allowed, and/or disallowed (e.g., a PDC required/preferred/allowed/disallowed indication may be stored in the subscriber profile to reflect a business agreement between the subscriber and the operator).

[0236] In examples of WTRU application-based determination, the WTRU application may determine that a downlink XR flow is eligible for PS QoS handling by the network because the downlink XR flow transports live XR media to be displayed in real-time to the user. An enabler client (e.g., EEC) may make the determination to use PSH and/or to use a PDC, based on the WTRU applications in use, user

preference, user profile, or based on the media protocol used by the WTRU application. Based on this determination, the WTRU application or enabler client may use a local API to convey a "PDC requested" or "PSH requested" indication to the WTRU (e.g., the indication may be a socket option).

[0237] The WTRU may set a PDC indication IE or a PSH indication IE in a message(s) to provision an EES and/or discover an EAS. For example, when a PDC is required, the WTRU may discover a nearby EAS that supports a PDC. For example, when PSH is required, the WTRU may discover a nearby EAS that supports PSH (e.g., in this last case, the EAS may decide, based on its capabilities, to use a PDC or another way to support PSH, such as by using a non-encrypted protocol enabling PSH, for example RTP).

[0238] In examples, the WTRU may send a PSH or PDC indication (e.g., PDC required/preferred/allowed/disallowed indication) to the EAS.

[0239] A PSH or PDC indication may be sent at the application layer (e.g., using a pre-existing connection between the WTRU and EAS), or between the WTRU and a remote cloud AS. In this last case, the remote cloud AS may convey the PSH indication (e.g., a PSH required/preferred/allowed/disallowed indication) to EAS over a backend AS-EAS application connection.

[0240] A PSH or PDC indication (e.g., PSH or PDC required/preferred/allowed/disallowed indication) may be sent through the EES (e.g., the EEC on the WTRU may send the indication when registering with the EES, and the EES may send the indication to the EAS).

[0241] The EAS may determine if a PDC is required/preferred/allowed/disallowed based on WTRU input or based on an indication from the EAS application (e.g., an EAS application may send to EAS a PDC requested indication for live XR downlink flows; e.g., an EAS application could additionally take into account the user's application preferences and service level agreement when determining whether to send a PDC requested to EAS).

[0242] Feature(s) associated with configuring a PDC and definition of PDC configuration IEs are provided herein. PDC configuration IEs may hold the same IEs as PDC provisioning IEs. Different names for these sets of IEs may be used because the PDC provisioning IEs may reflect the long-term capabilities of a system or node, while the PDC configuration IEs may be selected for a specific connection. For example, a set of PDC configuration IEs may, in some examples, include a single protocol, a client certificate, and a server certificate, while a set of PDC provisioning IEs may include lists of supported protocols, client, and server certificates.

[0243] The term PDC Configuration IEs may be used when referring to information elements that describe the characteristics of a PDC. The term PDC provisioning IEs may be used when referring to the capabilities of a client or a server. For example, an information element may indicate that a client or a server is capable of using the MASQUE and GTP protocols to communicate, and another information

element may indicate that one or more communications (e.g., all communications) in a PDC use the MASQUE protocol.

[0244] PDC configuration may follow one or more processes (e.g., two phases). In a first process (e.g., phase one), the PDC configuration IEs may be determined. A node (e.g., WTRU or EAS) may send a message to an EES including its PDC provisioning IEs (e.g., that may be named candidate PDC configuration IEs). The EES, based on the received message and its own PDC provisioning IEs, may determine a set of accepted PDC configuration IEs. In a second process (e.g., phase two), the PDC configuration IEs may be provided to the EAS. The EAS may use the PDC configuration IEs to configure the PDC endpoint.

[0245] The EAS may initiate PDC configuration (as shown at 7-10 in FIG.5). The EAS may determine (e.g., as a pre-requisite) that a PDC is required/preferred/allowed/disallowed (e.g., as described herein). The EAS may determine a set of candidate PDC configuration IEs; for example, the IEs may include a list of supported PDC protocols (e.g., PDC protocols supported by EAS, such as MASQUE or GTP) and a security configuration already configured in the EAS (e.g., a set of certificates installed on EAS). The elements of these lists may be associated with a preference order. The EAS may send a PDC configuration request message to the EES (e.g., including the candidate PDC configuration IEs). The EES (e.g., upon receiving the PDC configuration request message) may determine accepted PDC configuration IEs. For example, the EES may accept a PDC protocol that is common and, if applicable, preferred, between the PDC capabilities provisioned earlier by the EES (e.g., a set of PDC protocols supported by the 5G operator) and the PDC capabilities provided by the EAS in the configuration request message (e.g., a set of PDC protocols supported by the EAS). For example, the EES accepts security configurations that may be common and, if applicable, preferred between the PDC security information configured earlier by the EES (e.g., a set of certificates trusted by the 5G operator) and the PDC security information provided by the EAS in the configuration request message (e.g., a set of certificates trusted by the EAS). The EES may send a PDC configuration response message to the EAS, including the accepted PDC configuration IEs. The EAS, using the accepted PDC configuration IEs, may perform the local (e.g., server-side) configuration of the PDC endpoint (e.g., the EAS may create a (e.g., PDU set metadata-enabled) MASQUE proxy instance, a (e.g., PDU set metadata-enabled) GTP tunnel endpoint, IPsec tunnel endpoint, and/or may configure the EAS application to send PDU set metadata UDP-options).

[0246] The WTRU may initiate a PDC configuration (as shown at 6-10 in FIG. 6A). The WTRU may determine (e.g., as a pre-requisite) that a PDC is required/preferred/allowed/disallowed, as described herein. The WTRU (e.g., the EEC) may determine the candidate PDC configuration IEs, for example, based on a URSP rule including PDC configuration IEs and/or based on WTRU configuration and/or an

indication from the WTRU application. The WTRU may send a PDC configuration request to the EES (e.g., including the candidate PDC configuration IEs). The EES may determine the accepted PDC configuration IEs (e.g., as may be done with EAS-initiated PDC configuration). The EES may send a PDC configuration request message to EAS, including the accepted PDC configuration IEs (e.g., to enable the EAS to perform PDC local endpoint configuration). The EAS may gather information needed to communicate with the endpoint. The gathered information may be referred to herein as the PDC setup IEs. The EAS may send the PDC setup IEs in response to the EES. The EES may send the PDC setup IEs in a PDC configuration response to the WTRU (e.g., EEC on WTRU).

[0247] A PDC endpoint may be locally configured on the EAS (e.g., after configuring a PDC configuration using the EAS-initiated or WTRU-initiated method). The PDC may be established.

[0248] Feature(s) associated with establishing a PDC and definition of PDC setup IEs are provided herein. PDC setup IEs may describe a PDC endpoint (e.g., on EAS) and may include IEs needed to establish a PDC with this endpoint. The PDC endpoint may be locally configured on the EAS. The EAS may determine the PDC setup IEs for this endpoint. The EAS may provide the PDC setup IEs to the EES in a message (as represented at 11 in FIGS. 5 and 6). PDC setup IEs may include one or more of the following: a PDC protocol (e.g., MASQUE using a PS metadata extension, GTP using a PS metadata extension, UDP option-based protocol); an IP address and port for the PDC endpoint (e.g., on EAS); security parameters for PDC establishment (e.g., an authentication method and/or identities for the selection of a certificate or shared key); or any other protocol parameter (e.g., tunnel endpoint ID, TEID, for GTP).

[0249] FIGS. 5A-5B depict an example method for PDC establishment and operation. An example NEF-based establishment method is represented in FIGS. 5A-5B at 11-24. The EES may convey the PDC setup IEs to the network (e.g., via NEF or PCF). The NEF-based establishment method may be initiated when the EAS sends a PDC establishment request message to EES. For example, the establishment request message may be a Session with QoS create request message, which may be enhanced to hold PDC setup IEs. The EES may determine (e.g., upon reception of the establishment request message) that a PDC may be established (e.g., because PDC setup IEs may be provided). The EES may start implementing the session with QoS method (e.g., including packet flow description (PFD) management and invoking event monitoring service). The EES may send an AF session with a QoS service message to NEF. The AF session with the QoS service message may include existing IEs, such as IP flow description and requested QoS, and/or IEs, such as PDC setup IEs. The NEF may send a policy authorization create service message to the PCF (e.g., including IP flow description requested QoS and PDC setup IEs). In examples, the EES may directly send a policy authorization create service message to the PCF (e.g., as an alternative

to passing through the NEF). The PCF may configure a policy rule including the PDC setup IEs (e.g., upon receiving the message from the EES or the NEF). Then the PCF may send a response message to the NEF. The NEF may send a response message to the EES. The EES may send a response message to the EAS. The response message(s) may hold status information that indicates if the operation was successful. The response message(s) may hold additional IEs to enable setting up the PDC (e.g., for a GTP-based PDC, a TEID may be reserved by the NEF or the PCF, added in the PDC setup IEs set in the policy rule, and sent back to the EAS to enable the EAS to accept the TEID, such as shown at 22 in FIG. 5B). The PCF may send (e.g., to the SMF) a notification message including PDC setup IEs (e.g., a Npcf_SMPolicyControl_UpdateNotify message). The SMF may send an N4 message to request UPF to set up the PDC, including PDC setup IEs (e.g., a N4 session modification request message). The UPF may (e.g., upon reception) trigger a PDC establishment using the PDC setup IEs. PDC establishment may depend on the PDC protocol. For example, PDC establishment may be a MASQUE connection establishment, an IPSec security association used to protect a GTP session or UDP datagrams. The UPF may configure itself (e.g., downlink and/or uplink) to forward PDUs and related PDU set IEs between the PDU session and the PDC. For example, the UPF may configure itself to forward downlink PDUs, and related PDU set IEs, from the WTRU, over the PDU session (e.g., through the GTP tunnel towards the RAN, with PDU set IEs in the GTP header). The UPF may send a response message to the SMF (e.g., an N4 session modification response message).

[0250] FIG. 6 depicts an example method for WTRU-initiated PDC establishment and operation. FIGS. 6A-6B depict a WTRU-based establishment method at 12-22. The EES may convey the PDC setup IEs to the network via the WTRU (e.g., via EEC on the WTRU). The WTRU-based establishment method may be initiated when the EES sends, to the WTRU (e.g., EEC), a message (e.g., PDC configuration response), including PDC setup IEs. The WTRU (e.g., EEC) may check that this request is valid (e.g., it originates from a known EES and corresponds to a known PDC configuration request). The WTRU may trigger the PDC establishment, which may be a MASQUE request. The UPF MASQUE proxy IEs may inform the WTRU how to communicate with a MASQUE proxy collocated with the UPF. MASQUE proxy IEs may be an example of PDC setup IEs. The WTRU may send (e.g., to the UPF) a first MASQUE connection request. The first MASQUE connection request may include the UPF MASQUE proxy IEs (e.g., the request destination IP address and port may be the UPF MASQUE proxy IP address and port; the target URI may be built using a template URI that is included in the UPF MASQUE proxy IEs), and/or the PDC setup IEs (e.g., the target URI may include the IP address and port of a MASQUE proxy on EAS). The MASQUE proxy on the UPF may receive the first MASQUE connection request. Based on the PDC setup IEs in the request, the MASQUE proxy on the UPF may send a second MASQUE connection request to the MASQUE proxy on the EAS. The UPF may include an explicit "PDU set metadata indication" (e.g., a new

IE in the transport parameters) in the second MASQUE connection request (e.g., to request PDU set metadata messages support for this connection). The EAS (e.g., upon receipt of the second MASQUE connection request) may complete the PDC endpoint configuration (e.g., the EAS may indicate to the EAS application that the MASQUE connection is available for sending and receiving PDUs and related PDU set IEs). The EAS may send a MASQUE connection response (e.g., indicating success, such as with a 200OK status code) to the UPF. The UPF may configure itself to forward (e.g., downlink and/or uplink) PDUs and related PDU set IEs between the first and second MASQUE connection legs, where the first leg WTRU-UPF may be over the PDU session, and the second leg UPF-EAS may carry PDU set metadata alongside related PDUs. For example, the UPF may configure itself to forward downlink PDUs and related PDU set IEs from the EAS over the WTRU-UPF MASQUE connection (e.g., downlink PDU is encapsulated in an HTTP message and sent through the GTP tunnel toward the RAN, with PDU set IEs in the GTP header). The UPF may send a MASQUE connection response to the WTRU.

[0251] In examples, the WTRU may send the PDC setup IEs to the SMF over the control plane (e.g., in a PDU session modification request instead of passing the PDC setup IEs to the UPF in the MASQUE request). Upon receiving the PDU session modification request, the SMF may send the PDC setup IEs to the UPF (e.g., in an N4 session message).

[0252] The UPF may establish the PDC using the PDC setup IEs. There may be no need for the WTRU to establish the MASQUE connection through UPF. Traffic from the AS may be sent through the PDC and forwarded by the UPF over the PDU session.

[0253] The UPF may store the PDC setup IEs (e.g., instead of immediately establishing the PDC). When the WTRU establishes a MASQUE connection with the UPF, the UPF may use the stored PDC setup IEs to determine to use a MASQUE proxy as a next hop for the connection. The rest of the method may be similar to the WTRU-based establishment method described herein.

[0254] The several proposed establishment methods have different sets of usage.

[0255] When the EAS initiates the PDC configuration and uses a "NEF-based" establishment method, the EAS may have more control over the usage of a PDC. In some cases, the WTRU may be left unaware of the usage of a PDC.

[0256] When the WTRU initiates the configuration and establishment of the PDC, the WTRU (e.g., and a user) may have more control over PDCs and the QoE of the application. In cases where the WTRU initiates a MASQUE connection (e.g., as depicted in case A in FIGS. 6A-6B), the WTRU-UPF leg of the MASQUE connection simplifies the network control plane (e.g., because PDC related IEs may be exchanged directly between WTRU and UPF over the user plane). For example, the MASQUE connection allows for downlink PDU set IEs to be forwarded by the UPF to the WTRU and for PSH on the WTRU.

[0257] A MASQUE proxy instance may be created on the UPF or collocated with the UPF (e.g., for the WTRU-based establishment method). UPF MASQUE proxy IEs, such as UPF MASQUE proxy IP address, port and protocol, and/or a template URI understood by the MASQUE proxy, may be provided to the WTRU for the WTRU to connect to the UPF MASQUE proxy. UPF MASQUE proxy IEs may be provided to the WTRU during the PDU session establishment (e.g., as shown at 3 in FIG. 6A). The WTRU may set a MASQUE proxy requested, or PDC requested indication in a PDU session establishment request or modification message based on a URSP rule (e.g., a URSP rule including a MASQUE proxy indication or a URSP rule including a PDC indication), a local configuration, and/or an indication by the WTRU application. The SMF may determine that a MASQUE proxy may be requested, based on one or more of the following: a MASQUE proxy requested indication or a PDC requested indication in a PDU session establishment request or modification message; and/or a policy (e.g., PCC) rule, which may include a MASQUE proxy indication or PDC indication. The indication may be configured in the rule by the network operator and/or by an AF (e.g., through NEF or PCF).

[0258] The SMF may determine that a MASQUE proxy instance may be created by the UPF. The SMF may send to the UPF an N4 message (e.g., including a MASQUE proxy requested indication). Based on the indication, the UPF may create the MASQUE proxy instance or may select an existing MASQUE proxy instance. The UPF may send the UPF MASQUE proxy IEs corresponding to the instance to the SMF. The SMF may send the UPF MASQUE proxy IEs to the WTRU (e.g., in a PDU session establishment or modification response).

[0259] After using the NEF-based or WTRU-based establishment method, the PDC may be used for carrying PDUs and related PDU session IEs (e.g., between the UPF and the EAS). The EAS may send media flows through the PDC. The UPF may forward media flows over the corresponding PDU session downlink towards the WTRU. The same PDU session may carry different flows (e.g., some of which may be carried over a PDC and some of which may not).

[0260] Uplink PDUs may be forwarded by the UPF through or outside of the PDC (e.g., using IP routing). Forwarding uplink PDUs through PDC may not be requested (e.g., required) because PDU session metadata may not be used in uplink from UPF to EAS (e.g., as there may be no RAN between UPF and EAS). Forwarding uplink PDUs outside of the PDC may be more efficient (e.g., as there is no need to encapsulate/decapsulate PDUs).

[0261] Forwarding uplink PDUs outside of the PDC may result in an asymmetric path between UPF and EAS, for example, where uplink and downlink PDUs may be forwarded over a different path. The UPF may determine to use PDC for uplink PDUs based on an N4 message from the SMF. The N4 message may be

sent by SMF based on a policy rule including a "use PDC for uplink" indication. The N4 message may be configured in PCC rules by the operator (e.g., based on an AF request).

[0262] Feature(s) associated with operating a PDC are provided herein. The EAS may perform PDU set identification. The EAS may be an origin server with media data and metadata access. The EAS may use media metadata to identify PDU sets (e.g., as individual temporal or spatial layers within one frame) and PDU set IEs (e.g., by using the encoder-provided metadata to obtain the size of a PDU set, calculating importance based on layer IDs and dependency between PDU sets, identifying start/end PDUs of a PDU set, and numbering the PDUs in a PDU set). The EAS may determine, based on application logic, additional related IEs such as an "end of burst" indication (e.g., that indicates that no other PDUs may be sent for a period, such as until the start of the next frame), and/or other PDU set IEs (e.g., as described herein).

[0263] The EAS may be a media proxy (e.g., operated by a CDN provider in an edge network), such as a MOQ relay or an RTP media proxy, which may access media transport metadata but may not have access to media data (e.g., may only have access to media PDUs, which may be encrypted end-to-end). In this example, the EAS may derive PDU set IEs from the media transport metadata associated with PDUs (e.g., MOQ transport metadata including media object priority, or RTP header extension for PDU set metadata); the EAS may then send the PDUs and associated PDU set IEs over the PDC.

[0264] The EAS may send PDU set IEs in association with the PDUs. For example, the EAS may encode the PDU set IEs and related IEs in the GTP header that encapsulates the associated PDU. For example, EAS may send PDU set IEs in an HTTP message including a PDU set ID, and the EAS may send PDU in another HTTP message including a PDU set ID (e.g., all PDUs that belong to the same PDU set may be sent with the same PDU set ID, and another message, holding the same PDU set ID, may include the PDU set IEs related to this PDU set). For example, EAS may encode the PDU set IEs in UDP options in the same UDP datagram that carries a related PDU.

[0265] The UPF may receive PDU set IEs, related IEs, and associated PDUs. The UPF may use the PDU set IEs for local processing (e.g., to detect the end-of-burst). The UPF may forward a PDU using a GTP-U packet toward the RAN. The UPF may encode the related PDU set IEs in the header of the GTP-U packet. The RAN may use the PDU set IEs in the GTP-U header to apply the PS QoS handling service, including, for example, determining which PDU to drop in case of congestion (e.g., using PDU set importance) and/or placing the WTRU in a low-power state (e.g., based on end-of-burst indication). The RAN may forward the PDUs toward the WTRU.

[0266] Feature(s) associated with closing a PDC are provided herein.

[0267] If the EAS application tears down the service data flow, the EAS application may close the PDC (e.g., close the GTP tunnel, close the CONNECT stream on the MASQUE connection, or close the UDP socket). The UPF may detect that the PDC is closed (e.g., when receiving a message to close the connection or when receiving a message indicating that a port is not reachable). The UPF may communicate to the WTRU as if the traffic was no longer routable (e.g., the UPF may send a "host unreachable" ICMP message back to the WTRU in response to an uplink PDU from the WTRU).

[0268] If the WTRU or network tears down the PDU session or the QoS flow carrying the traffic receiving PSH (e.g., XR media traffic), the UPF may tear down the PDC corresponding to the PDU session or QoS flow (e.g., close the GTP tunnel, close the CONNECT stream on the MASQUE connection, or close the UDP socket). The EAS may detect the connection loss and proceed accordingly. PS identification of downlink encrypted traffic may be performed. NEF-Based PDC establishment and operation may be performed.

[0269] FIGS. 5A-5B depict an example method for establishing and operating a PDC (e.g., to enable PS QoS handling to be applied to an encrypted media flow). At 0a-0b, PDC provisioning may be performed. The UPF and the EES may be configured with PDC security information and PDC capabilities. At 1-6, decision aspects and service provisioning aspects may be performed.

[0270] At 1, the WTRU application may trigger the establishment of an XR application session. The WTRU may determine that a PDC is requested/preferred/allowed/disallowed. The WTRU may (e.g., alternatively) determine that PSH may be used or requested (e.g., from a URSP rule including a PSH indication, without necessarily being aware that PDC is needed).

[0271] At 2, the WTRU may trigger a service provisioning method involving an ECS to identify an EES for the XR application session. The WTRU may include a PSH-enabled indication in the service provisioning request to the ECS to identify PSH-enabled EES.

[0272] At 3, the WTRU may trigger a PDU Session establishment/modification method to communicate with the EES and the EAS. For example, the DNN used for this PDU session may have been received from the ECS in the service provisioning method (e.g., at 2). During the PDU session establishment/modification method, the SMF may determine that PSH may be used for this PDU session (e.g., based on an indication from the WTRU and/or from a policy). The SMF may select a UPF that has the capability to use PDCs. The SMF may send to the WTRU an indication of the UPF selection (e.g., an indication of whether PDCs may be supported or not in the PDU session). The indication of UPF selection may depend on whether a PSH-enabled UPF was selected or, respectively, that the selected UPF does not support PDCs. The SMF may have obtained the UPFs capabilities from the configuration by the operator (e.g., through a network management system). The UPFs may be provisioned with PDC capabilities (e.g., through a network

management system), and the UPFs may send their PDC capabilities to the SMFs (e.g., at SMF-UPF communication session initiation time).

[0273] At 4, the WTRU may initiate the edge computing session setup (e.g., this may include EEC registration and EAS discovery). At 5, the WTRU may send an application service request to EAS (e.g., an application layer message that requests an XR media session to be created). At 6, the EAS may decide to use PDC.

[0274] At 7-10, PDC configuration may be performed (e.g., the EAS may initiate PDC configuration), and candidate IEs and accepted IEs may be determined. At 7, the EAS may send a PDC configuration request to the EES, including candidate PDC configuration IEs. At 8, the EES may determine accepted PDC configuration IEs. At 9, the EES may send, to the EAS, a PDC configuration response including the accepted PDC configuration IEs. At 10, the EAS, using the accepted PDC configuration IEs, may configure the local endpoint of the PDC.

[0275] At 11-22 PDC establishment may be performed (e.g., using a NEF-based establishment method).

[0276] At 11, the EAS may send, to the EES, a Session with QoS create request message, including PDC setup IEs. At 12, the EES may perform processes related to the session with a QoS method (e.g., including PFD management and invoking event monitoring service). At 13, the EES may send, to the NEF, an AF Session with a QoS service message (e.g., including IP flow description, requested QoS, PDC setup IEs). At 14, NEF may send, to the PCF, a policy authorization create service (e.g., including IP flow description, requested QoS, PDC setup IEs). At 15, PCF may configure a policy rule that may include PDC setup IEs

[0277] At 16-18, the PCF may send, to the NEF, a Policy Authorization Create service response. The NEF may send, to the EES, an AF Session with QoS service response. The EES may send, to the EAS, a Session with a QoS create response. At 19, the PCF may send, to the SMF, a Npcf_SMPolicyControl_UpdateNotify message (e.g., including a rule that may include PDC setup IEs). At 20, the SMF may send, to the UPF, an N4 Session modification request (e.g., including PDC setup IEs).

[0278] At 21-22, the UPF may trigger a PDC establishment sub-method using PDC setup IEs. The PDC establishment sub-method may be based on the PDC protocol. At 23, the UPF may configure itself to forward PDUs and PS IEs between the PDC and the PDU (e.g., using the session established at 3).

[0279] At 24, the UPF may send, to the SMF, an N4 Session modification response (e.g., indicating the success of the PDC establishment). The SMF may send a (not depicted) response or notification message (e.g., indicating the success of the PDC establishment, for example, to the PCF).

[0280] At 25-30, PDC operation may be performed. At 25-26, the EAS, which may perform PDU set identification on the downlink traffic, may send a downlink media data flow PDU and associated PS IEs. At

27-28, the UPF may forward the PDU and associated PS IEs from the PDC onto the PDU session GTP tunnel to the RAN. At 29, the RAN may provide the PS QoS Handling service to the PDU, using PS IEs. At 30, the RAN may send the PDU toward the WTRU.

[0281] Feature(s) associated with WTRU-based PDC establishment and operation are provided herein. As depicted in FIGS. 6A-6B, the WTRU may initiate the establishment of the PDC through a proxy at the UPF (e.g., instead of having the UPF initiate the PDC establishment). The establishment of the PDC may be performed using a tunneling method supporting tunnel establishment through a proxy (e.g., a MASQUE connection). The WTRU-initiated PDC establishment may not request (e.g., require) a network NEF API to be used and may not request (e.g., require) policy rules to be enhanced to include PDC IEs, simplifying the deployment of this process.

[0282] FIGS. 6A-6B depict an example of WTRU-initiated PDC establishment and operation. At 0a-0b PDC provisioning may be performed. At 1-6, decision aspects and service provisioning aspects may be performed. These aspects may be similar to the corresponding phase in FIGS. 5A-5B, with one or more of the following differences.

[0283] At 3, a MASQUE proxy may be created in the UPF, and the corresponding UPF MASQUE proxy IEs may be provided to WTRU (e.g., IP address and port of the MASQUE proxy). A MASQUE proxy may be created if MASQUE is used between WTRU and UPF (e.g., as described in case "A" below). For example, the WTRU may send a PDU session establishment (or modification) request to communicate with EAS. The WTRU may include a PDC indication or a "MASQUE requested" indication in the PDU session establishment/modification request. The SMF, based on PDC indication or MASQUE requested indication in the PDU session establishment/modification request and/or in a policy rule (e.g., PCC rule), may request the UPF to create a MASQUE proxy. The SMF may send an N4 message to the UPF that may include a MASQUE proxy indication. The UPF may create a MASQUE proxy instance. The UPF may send the corresponding UPF MASQUE proxy IEs to the SMF. The SMF may send to the WTRU a PDU session establishment/modification response that may include the UPF MASQUE proxy IEs.

[0284] When the EAS instance is created, e.g., at 4 or 0-3, the EAS may subscribe with the EES for receiving notifications related to PDCs. At 6, the WTRU may determine to use a PDC (e.g., instead of the EAS as depicted in FIGS. 5A-5B).

[0285] At 7-12, PDC configuration may be performed (e.g., the WTRU may initiate PDC configuration), and candidate IEs and accepted IEs may be determined. At 7, the WTRU may send, to the EES, a PDC configuration request that may include candidate PDC configuration IEs. The message may be sent over the PDU session established at 3. At 8, the EES may determine the accepted PDC configuration IEs. At 9, the EES may send, to the EAS, a PDC configuration notification or request message that may include the

accepted PDC configuration IEs. At 10, the EAS, using the accepted PDC configuration IEs, may configure the local endpoint of the PDC. At 11, the EAS may send, to the EES, a PDC configuration message, including PDC setup IEs. At 12, the EES may send, to the WTRU, a PDC configuration response message, including PDC setup IEs. A status code or the presence of PDC setup IEs may indicate the success of the configuration operation.

[0286] At 13-22, PDC establishment (e.g., a WTRU-based establishment method) may be performed. At 13, the WTRU (e.g., the EEC) may trigger PDC establishment (e.g., based on the success of the configuration phase indicated by the message at 12).

[0287] In example A (e.g., case A), the WTRU may use a MASQUE connection to convey the PDC setup IEs to the UPF. At 14a, the WTRU may send to the UPF (e.g., to the MASQUE proxy on the UPF) a MASQUE connection request (e.g., including UPF MASQUE proxy IEs and PDC setup IEs).

[0288] In example B (e.g., case B, which may be an alternative to case A), the WTRU may use the control plane to provide the PDC setup IEs to the UPF (e.g., through SMF in a PDU session modification request message). At 14b1, the WTRU may send, to the SMF, a PDU session modification request message (e.g., including PDC setup IEs). The PDU session modification request message may request a modification of the PDU session established at 3. At 14b2, the SMF may send, to the UPF, a N4 session modification message, related to the modified PDU session, including PDC setup IEs.

[0289] At 15, the UPF (e.g., MASQUE proxy on UPF) may determine the EAS PDC endpoint IP address, port, and URI based on PDC setup IEs. The PDC endpoint may be another MASQUE proxy. The PDC endpoint may (e.g., alternatively) use another protocol (e.g., GTP with PDU set metadata extension, or UDP-options). The UPF may determine how to reach the EAS endpoint and what protocol to use based on the PDC setup IEs included in the endpoint connection IEs (protocol, IP address, port, etc.).

[0290] At 16 and 18 MASQUE may be used between UPF and EAS. At 16, the UPF may send, to EAS, a MASQUE connection request (e.g., including a PS metadata indication indicating that a PS metadata extension should be used on this connection). At 17, the EAS completes the PDC local endpoint establishment. PDC local endpoint establishment may include creating a socket interface and notifying the EAS application that the socket interface may be used to send media PDUs and associated PDU set IEs. At 18, the EAS may send, to the UPF, a MASQUE connection response (e.g., indicating success with a 200OK status code). At 19, the UPF may configure itself to forward PDUs and PS IEs between the PDC and the PDU session.

[0291] In example A (e.g., case A, as introduced at 14a), at 20a, the UPF may send, to the WTRU, a MASQUE connection response (e.g., indicating success with a 200 OK status code).

[0292] In example B (e.g., case B, as introduced at 14b1 and 14b2), at 20b1 the UPF may send an N4 session modification response to the SMF. At 20b2 the SMF may send a PDU session modification response to the WTRU.

[0293] At 25-30, PDC operation may be performed. PDC operation may be similar to the corresponding "PDC operation" phase depicted in FIGS. 5A-5B.

[0294] At 26, PDUs and related PDU set IEs may be sent over the UPF-EAS leg of the MASQUE connection. At 28 and 30, PDUs may be sent over the WTRU-UPF leg of the MASQUE connection. At 28, the PDU set IEs may be sent in the GTP-U header of the GTP packet that encapsulates the MASQUE connection packet that carries the PDU.

[0295] Feature(s) associated with service provisioning of PSH-enabled EES, and discovery of PSH-enabled EAS are provided herein. PSH-enabled EES and/or EAS support PDC establishment and operation may be performed. A WTRU may request a PSH-enabled EES and/or EAS when performing Service Provisioning and/or EAS discovery to receive XR traffic over an encrypted media transport protocol that receives PS QoS handling service by the network. Service provisioning of PSH-enabled EES may be performed. Discovery of PSH-enabled EAS (e.g., where the WTRU sends to EES an EAS discovery request including a "PDC requested" indication, and where the EES selects and may send back to the WTRU a list of EAS that support PDCs) may be performed.

[0296] At 0, the EES may be configured with PDC security information and PDC capabilities. At 1, the EES may send to the ECS a registration message that may include a PSH support indication.

[0297] At 2, the ECS may store the PSH support indication (e.g., along with any other EES registration state information provided in the registration message). At 3, the WTRU may determine to communicate with an EAS to obtain a media service using a PS QoS Handling by the network. The WTRU may determine that the media transport protocol is encrypted and/or may not use the UPF-based PDU set identification. For example, the WTRU may make this determination when the WTRU determines a MOQ connection for an XR application may be used. For example, the WTRU may determine that the media transport protocol is encrypted and/or may not use the UPF-based PDU set identification when the URSP rules corresponding to the session include a PDC required or PDC preferred indication.

[0298] At 4, the WTRU may send, to the ECS, a service provisioning request message that may include a PDC requested indication. At 5, the ECS may select one or more EES using EES registration state information (e.g., including PSH support indication associated with each EES based on registration at 2).

[0299] At 6, the ECS may send a service provisioning response message to the WTRU, including a list of selected EES identities that include, for a EES (e.g., each EES), related EDN information and associated

PSH support indication (e.g., where the presence of such an indication indicates that the EES is a PSH-enabled EES).

[0300] At 7, the WTRU may select a PSH-enabled EES using the list provided by the ECS. If no suitable PSH-enabled EES is available, the WTRU may decide to select a non-PSH-enabled EES (e.g., after prompting the user to ask to proceed with a possibly lower QoE, if the user accepts). If the WTRU selects a PSH-enabled EES, the WTRU may proceed with PDC establishment and operation (e.g., as described with regard to FIGS. 5A-5B and FIGS. 6A-6B).

[0301] Feature(s) associated with PSH tunnel security establishment are provided herein. FIG. 7 depicts an example method for WTRU-initiated PSH tunnel security establishment. FIG. 8 depicts an example method for AF-initiated PSH tunnel security establishment. FIG. 9 depicts an example method for PSH tunnel security establishment using an EAP based authentication method between WTRU, SMF, and AF.

[0302] In the methods represented in FIGS. 7-9, security parameters may be established and may be communicated to enable a secure connection (e.g., tunnel) to be established. The secure connection may be established over two legs, with one leg between WTRU and UPF and a second leg between UPF and AF, or over a single leg between UPF and AF. The methods represented in FIGS. 7-9 may be described for establishing two legs or establishing a UPF-AF leg (e.g., a UPF-AF leg).

[0303] The methods represented in FIGS. 7-9 may be used to enable PDC establishment over two legs (e.g., using a MASQUE connection from WTRU through UPF to AS) or over one leg (e.g., using a MASQUE connection or GTP tunnel or IPSec tunnel between UPF and AS).

[0304] The methods represented in FIGS. 7-9 may be used to enable a media transport proxy (e.g., a MOQ relay) at the UPF, such as the process family one depicted in FIG. 2. The media transport proxy at the UPF may perform PDU set identification on downlink media traffic from the AS (e.g., by using media transport metadata accessible by proxies). The methods represented in FIGS. 7-9 may be used to enable other types of transport or application proxies through the UPF. For example, the methods may enable a MASQUE proxy to be deployed in a network to provide services such as transport optimization (e.g., using a UPF MASQUE proxy to optimize transport protocol efficiency over some access network such as non-terrestrial networks or high-loss access networks).

[0305] FIGS. 7-9 describe how the UPF may receive security parameters. The security parameters may be used by the UPF to establish a PDC with an AF. For example, in each of FIGS. 7-9, a function in the network may be used to configure the security parameters in the UPF. The secure communication connections of the network may be used to securely configure the security parameters in the UPF. The UPF may then use them to establish a secure connection with an Application Server, which may be hosted outside of the 5G System and may be outside of the 5G System's security domain. It should be understood

that the security parameters may be received and used by a proxy function hosted in the UPF or associated with the UPF.

[0306] FIG. 7 depicts an example method to establish a secure tunnel with a UPF initiated by a WTRU. The UPF may act as a secure proxy function (SPF) for handling encrypted transport or application traffic (e.g., for acting as a transport proxy or application proxy) between the WTRU and the AF over the secure tunnel.

[0307] At 1, the WTRU may perform a registration method with the network. The WTRU may indicate its capability to communicate via a network secure proxy in a registration request message. The WTRU may derive an AKMA key and its identifier A-KID to be used to establish an application key with AF (e.g., following the primary authentication).

[0308] At 2, the WTRU may establish a PDU Session to communicate with the AF. The WTRU may include an indication to use a network provided SPF for the communication in the PDU Session establishment request message. The WTRU may include the indication at 4. The AMF may select an SMF that supports secure tunneling functionality based on a DNN/S-NSSAI combination provided in the PDU Session establishment request message.

[0309] At 3, the WTRU may establish an application session with the AF. The WTRU and AF may establish an application key KAF using the AKMA key and A-KID. The WTRU and AF may exchange keying material (e.g., freshness parameters) to be used to establish a secure tunnel with the network (e.g., derive tunnel specific keys using KAF).

[0310] At 4, the WTRU may send a PDU Session modification message to the SMF. The message may include tunnel security parameters. The tunnel security parameters may include one or more of the following (e.g., for authentication and security establishment for the tunnel with the UPF): a tunnel end point key (e.g., KAF or a key derived from KAF using the keying material); a tunnel end point key identifier (e.g., A-KID); or tunneling security capabilities (e.g., authentication methods supported).

[0311] At 5, the SMF may verify session management subscription data (e.g., to determine if secure tunneling is authorized for the WTRU). The SMF may send tunnel security parameters in a request message to the UPF. The UPF may allocate addressing information (e.g., IP address/port) for the SPF/tunnel end point. The UPF may associate the SPF/tunnel end point with the received tunnel security parameters. The SMF may provide a root or intermediate CA certificate to the UPF to verify the AF certificate.

[0312] At 6, the UPF may send a response message that may include the SPF addressing information and/or the authentication methods supported by the SPF (e.g., certificate based, shared key based, none) to the SMF. The response message may include a root CA certificate (e.g., if server-side certificate-based

authentication is supported). Security policy for the tunnel (e.g., whether traffic between the WTRU and UPF is encrypted/integrity protected) may be included in the response message.

[0313] At 7, the SMF may send a PDU session modification response message to the WTRU that may include one or more of the following: an indication of acceptance of secure tunneling, SPF addressing information, authentication methods supported by the SPF and security policy, or any SPF credentials (e.g., root CA certificate).

[0314] At 8, the WTRU may send a connection request toward the SPF. The connection request may include AF addressing information for the establishment of the tunnel leg between the UPF and the AF.

[0315] At 9, the WTRU may perform mutual authentication with the SPF. The WTRU may select an authentication method based on its own support and the authentication methods supported by the SPF. Depending on the authentication method selected, the WTRU may perform any one of the following: a password/digest based authentication method; shared key mutual authentication; or SPF server certificate based authentication.

[0316] A password/digest based authentication method may be performed by the WTRU. The WTRU may provide the UPF/SPF with a digest (e.g., MD5 hash) and tunnel end point key identifier. The hash may be generated using the tunnel end point key. The WTRU may provide the UPF/SPF with tunnel end point key identifier as a username. The UPF may verify the hash using the tunnel end point key and identifier.

[0317] Shared key mutual authentication may be performed by the WTRU. The WTRU and the SPF may use the tunnel end point key to generate a TLS shared secret, which they may use to perform mutual authentication. The WTRU may identify the tunnel key to the UPF/SPF using the tunnel end point key identifier.

[0318] SPF server certificate-based authentication may be performed by the WTRU. The WTRU may authenticate the UPF using the root CA server certificate received from SMF. This authentication may be performed in combination with WTRU authentication (e.g., a password/digest-based authentication method or with shared key mutual authentication).

[0319] At 10, security keys may be derived and used based on the selected security policy. At 10a, the UPF/SPF may connect with the AF. At 10b, the UPF/SPF may perform a mutual authentication with the AF. The UPF may perform one of the authentication methods described above (e.g., with the UPF behaving as the WTRU). The UPF may verify the AF server certificate (e.g., using the root certificate provided by SMF). At 10c, the AF may send a connection response to the UPF/SPF.

[0320] At 11, the UPF/SPF may send a connection response to the WTRU indicating successful secure tunnel establishment with the AF. At 12, the WTRU and the AF may exchange encrypted application traffic via the secure tunnel provided by the SPF/UPF.

[0321] A secure connection (e.g., a single secure connection) between UPF and AF may be established. To establish a single secure connection between the UPF and the AF, the messages at 8-9 and 11 may not be sent (e.g., because the WTRU does not need the tunnel security parameters), and the connection at 8 may not be established. The UPF may establish the secure connection at 10a/10b/10c (e.g., as depicted). At 12, the WTRU and the AF may exchange application traffic over a PDU session between WTRU and UPF, and over a secure connection (e.g., tunnel, between UPF and AF).

[0322] FIG. 8 depicts an example method initiated by an AF for establishing a secure tunnel with a UPF. The UPF may act as a secure proxy for handling encrypted application traffic between the WTRU and the AF (e.g., over the secure tunnel).

[0323] At 0, the WTRU may register with the network. The WTRU may establish an AKMA key and a PDU Session to communicate with the AF (e.g., as described herein).

[0324] At 1, the WTRU may establish an application session with the AF. The WTRU and the AF may establish an application key KAF using the AKMA key and A-KID. The WTRU and AF may exchange keying material (e.g., freshness parameters) to be used to establish a secure tunnel with the network (e.g., derive tunnel-specific keys using KAF).

[0325] At 2, the AF may send a request message to the NEF for the network to update the PDU Session associated with the WTRU. The request message may include tunnel security parameters. The AF may specify an indication or policy (e.g., whether authentication of the WTRU by the SPF and/or a secure tunnel between the WTRU and the UPF/SPF are required).

[0326] At 3, the NEF may send a response message to the AF that may include an acceptance of the secure tunneling. At 4, the PCF may initiate the policy update for the PDU Session with the SMF. The PCF may forward the tunnel security parameters to the SMF.

[0327] At 5, the SMF may verify session management subscription data (e.g., to determine if secure tunneling is authorized for the WTRU). The SMF may send tunnel security parameters in a request message to the UPF.

[0328] At 6, the UPF may send a response message that may include the SPF addressing information and/or the authentication methods supported by the SPF (e.g., certificate-based, shared key-based, none) to the SMF. The response message may include a root CA certificate (e.g., if server-side certificate-based authentication is supported).

[0329] At 7, the SMF may send a PDU Session modification message to the WTRU that may include one or more of the following: an indication of secure tunneling enablement, SPF addressing information, authentication methods supported by the SPF and security policy, or any SPF credentials (e.g., root CA certificate).

[0330] At 8, the WTRU may establish a connection with the UPF/SPF and the UPF/SPF with the AF (e.g., as described above with regard to 8-11 of FIG. 7). The WTRU may perform authentication and establishment of security based on an authentication method and a security policy (e.g., no authentication is performed with SPF if no authentication is required).

[0331] At 9, the WTRU and the AF exchange encrypted application traffic via the secure tunnel provided by the SPF/UPF.

[0332] A single secure connection may be established between the UPF and the AF. The message at 7 may not be sent (e.g., because the WTRU may not need the tunnel security parameters), and the connection at 8a may not be established. The UPF may establish the secure connection at 8b (e.g., as described with regard to FIG. 8). At 9, the WTRU and the AF may exchange application traffic over a PDU session between the WTRU and the UPF and over a secure connection (e.g., tunnel) between the UPF and the AF.

[0333] FIG. 9 depicts an example method initiated by a WTRU to establish a secure tunnel with a UPF. The UPF may act as a secure proxy for handling encrypted application traffic between the WTRU and the AF (e.g., over the secure tunnel). The SMF may act as an EAP authenticator in an EAP authentication method between the WTRU and the AF, which may act as an authentication server.

[0334] At 0, the WTRU may register with the network. At 1, the WTRU may establish a PDU Session to communicate with the AF. The WTRU may include an indication to use a network provided SPF in the PDU Session establishment request message. The WTRU may include an indication of an EAP identity in the PDU Session establishment request message. The EAP identity may include the FQDN of AF/DN-AAA. The username may correspond to AKMA key id A-KID if AKMA is used with the AF.

[0335] At 2, the SMF may verify the WTRU session management subscription data (e.g., whether secure tunneling is authorized for the WTRU). The SMF may initiate an EAP authentication for the WTRU.

[0336] At 3, the SMF may retrieve the EAP identity (e.g., if not provided at 1). At 4, the SMF may set up N4 session management with the UPF to exchange EAP messages with the AF/DN-AAA.

[0337] At 5, the SMF may send the EAP identity from the WTRU to the AF/DN-AAA. At 6, the WTRU and AF/DN-AAA may exchange EAP messages via the SMF/UPF (e.g., as many messages as required by the EAP-method supported). At 7, the SMF may receive, from the AF/DN-AAA, an EAP-success including a master key and an identifier to be used for the secure tunnel.

[0338] At 8, the SMF may configure the UPF/SPF with a tunnel end point key derived using the master key from the AF. The UPF may allocate addressing information (e.g., IP address/port) for the SPF/tunnel end point, which the UPF may associate with the received tunnel security parameters.

[0339] At 9, the SMF may send a PDU Session establishment accept message that may include an EAP-success and SPF addressing info. At 10, the WTRU may send a connection request towards the SPF. The connection request may include AF addressing information for the establishment of the tunnel leg between the UPF and the AF. The UPF/SPF may connect with the AF and may establish a secure connection using the tunnel end point key provided by SMF. At 11, the WTRU and AF may exchange application traffic via the secure tunnel provided by the SPF/UPF.

[0340] A secure connection (e.g., a single secure connection) between the UPF and the AF may be established. 10a may be omitted (e.g., since the WTRU may not need to establish a secure connection with UPF). At 11, the WTRU and the AF may exchange application traffic over a PDU session between the WTRU and the UPF and over a secure connection (e.g., tunnel) between the UPF and the AF.

[0341] Although features and elements described above are described in particular combinations, each feature or element may be used alone without the other features and elements of the preferred embodiments, or in various combinations with or without other features and elements.

[0342] Although the implementations described herein may consider 3rd Generation Partnership Project (3GPP) specific protocols, it is understood that the implementations described herein are not restricted to this scenario and may be applicable to other wireless systems. For example, although the solutions described herein consider LTE, LTE-A, New Radio (NR) or 5G specific protocols, it is understood that the solutions described herein are not restricted to this scenario and are applicable to other wireless systems as well.

[0343] The processes described above may be implemented in a computer program, software, and/or firmware incorporated in a computer-readable medium for execution by a computer and/or processor. Examples of computer-readable media include, but are not limited to, electronic signals (transmitted over wired and/or wireless connections) and/or computer-readable storage media. Examples of computer-readable storage media include, but are not limited to, a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as, but not limited to, internal hard disks and removable disks, magneto-optical media, and/or optical media such as compact disc (CD)-ROM disks, and/or digital versatile disks (DVDs). A processor in association with software may be used to implement a radio frequency transceiver for use in a WTRU, terminal, base station, RNC, and/or any host computer.

CLAIMS

What is claimed is:

1. A first network node for providing an enabler server, the first network node comprising:

a processor configured to:

receive a session request message from a second network node, wherein the session request message indicates a request for a session and comprises a protocol data unit set handling (PSH) data channel (PDC) setup information element (IE) and an indication of a Quality of Service (QoS) associated with the session;

determine a PDC should be established based on the request for the session, the PDC setup IE, and the indication of the QoS;

send a service request message to a third network node when it is determined that the PDC should be established, wherein the service request message comprises the indication of the QoS and PDC setup IE;

receive a service response message from the third network node, wherein the second message indicates the PDC has been established based on the PDC setup IE; and

send a session response message to the second network node, wherein the session response message indicates that the PDC is associated with the requested session and that the PDC has been established based on the PDC setup IE.

2. The first network node of claim 1, wherein the PDU setup IE indicates at least one of a PDU protocol, an internet protocol (IP) address for a PDC endpoint, a port for a PDC endpoint, a security parameter, an authentication method, an authentication parameter, an identity associated with a security certificate or key, or a protocol parameter, or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection parameter.

3. The first network node of any one of claims 1 to 2, wherein the PDU establishment request message indicates a request to create a session with a Quality of Service (QoS).

4. The first network node of any one of claims 1 to 3, wherein the service request message and service response message are associated with at least one of an application function, a network function (NF), a policy creation function (PCF), or a policy authorization.

5. The first network node of any one of claims 1 to 4, wherein the PDC setup IE is a first PDC setup IE, and wherein at least the service response message or the session response message further comprises a second PDC setup IE.

6. The first network node of any one of claims 1 to 5, wherein the processor is further configured to:

receive a setup request message from the second network node, wherein the request message comprises one or more candidate PDC setup IEs;

determine the PDC setup IE from the one or more candidate PDC setups IEs; and

send a setup response message to the second network node, wherein the setup response message comprises at least the PDC setup IE.

7. A method performed by a first network node, the method comprising:

receiving a session request message from a second network node, wherein the session request message indicates a request for a session and comprises a protocol data unit set handling data channel (PDC) setup information element (IE) and an indication of a Quality of Service (QoS) associated with the session;

determining a PDC should be established based on the request for the session, the PDC setup IE, and the indication of the QoS;

sending a service request message to a third network node when it is determined that the PDC should be established, wherein the service request message comprises the indication of the QoS and PDC setup IE;

receiving a service response message from the third network node, wherein the second message indicates the PDC has been established based on the PDC setup IE; and

sending a session response message to the second network node, wherein the session response message indicates that the PDC is associated with the requested session and that the PDC has been established based on the PDC setup IE.

8. The method of claim 7, wherein the PDU setup IE indicates at least one of a PDU protocol, an internet protocol (IP) address for a PDC endpoint, a port for a PDC endpoint, a security parameter, an authentication method, an authentication parameter, an identity associated with a security certificate or key, or a protocol parameter, or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection parameter.

9. The method of any one of claims 7 to 8, wherein the PDU establishment request message indicates a request to create a session with a Quality of Service (QoS).

10. The method of any one of claims 7 to 9, wherein the service message is associated with at least one of an application function, a network function (NF), a policy creation function (PCF), or a policy authorization.

11. The method of any one of claims 7 to 10, wherein the PDC setup IE is a first PDC setup IE, and wherein at least the service response message or the session response message further comprises a second PDC setup IE.

12. The method of claim of any one of claims 7 to 11, wherein the method further comprises:

- receiving a setup request message from the second network node, wherein the request message comprises one or more candidate PDC setup IEs;

- determining the PDC setup IE from the one or more candidate PDC setups IEs; and

- sending a setup response message to the second network node, wherein the setup response message comprises at least the PDC setup IE.

13. A first network node for providing an enabler application server, the first network node comprising:
a processor configured to:

- determining one or more candidate protocol data unit set handling (PSH) data channel (PDC) (PDC) setup information elements (IEs) associated with a service flow or an application;

- sending a setup request message to the second network node, wherein the setup request message comprises the one or more candidate PDC setup IEs;

- receiving a setup response message from the second network node, wherein the setup response message comprises a PDC setup IE from the one or more candidate PC setup IEs;

- sending a session request message to a second network node, wherein the session request message indicates a request for a session and comprises the PDC setup IE and an indication of a Quality of Service (QoS) associated with the session; and

receiving a session response message from the second network node, wherein the session response message indicates that the PDC is associated with the requested session and that the PDC has been established based on the PDC setup IE.

13. The first network node of claim 13, wherein the PDU setup IE indicates at least one of a PDU protocol, an internet protocol (IP) address for a PDC endpoint, a port for a PDC endpoint, a security parameter, an authentication method, an authentication parameter, an identity associated with a security certificate or key, or a protocol parameter, or a Multiplexed Application Substrate over QUIC Encryption (MASQUE) tunnel connection parameter.

14. The first network node of any one of claims 12 to 13, wherein the PDU establishment request message indicates a request to create a session with a Quality of Service (QoS).

15. The first network node of any one of claims 12 to 13, wherein the PDC setup IE is a first PDC setup IE, and wherein the session response message comprises a second PDC setup IE.

100

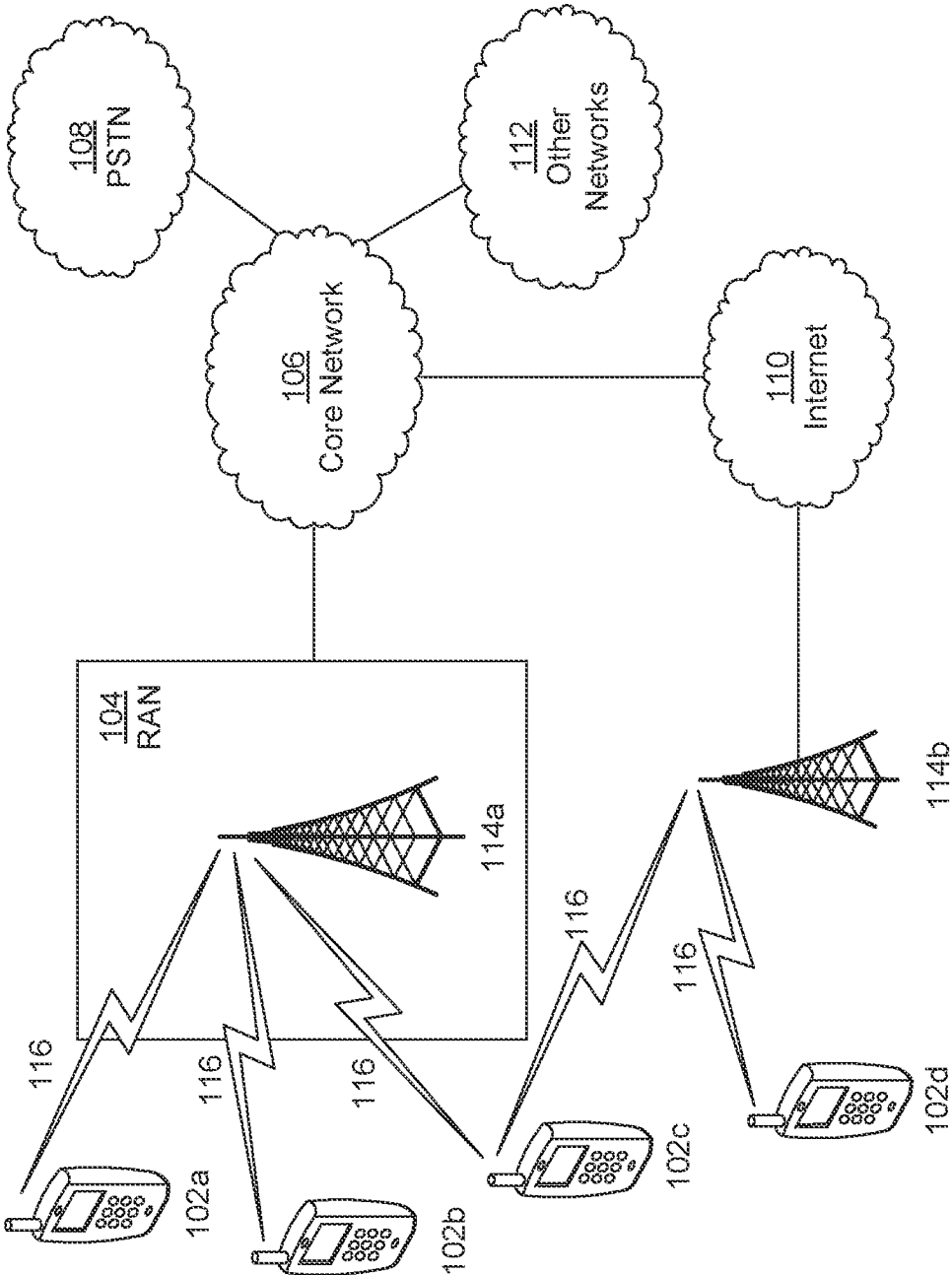
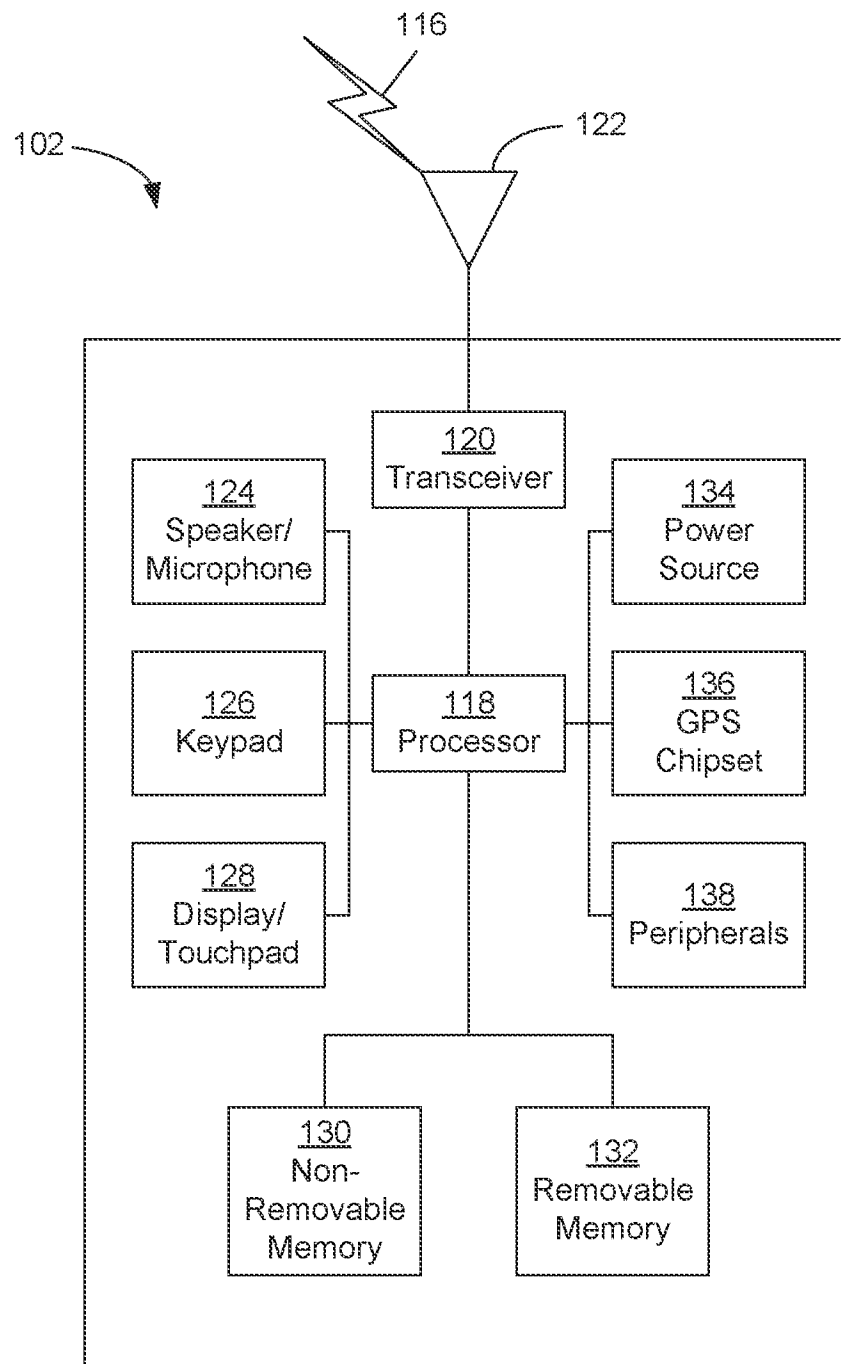


FIG. 1A

2/15

**FIG. 1B**

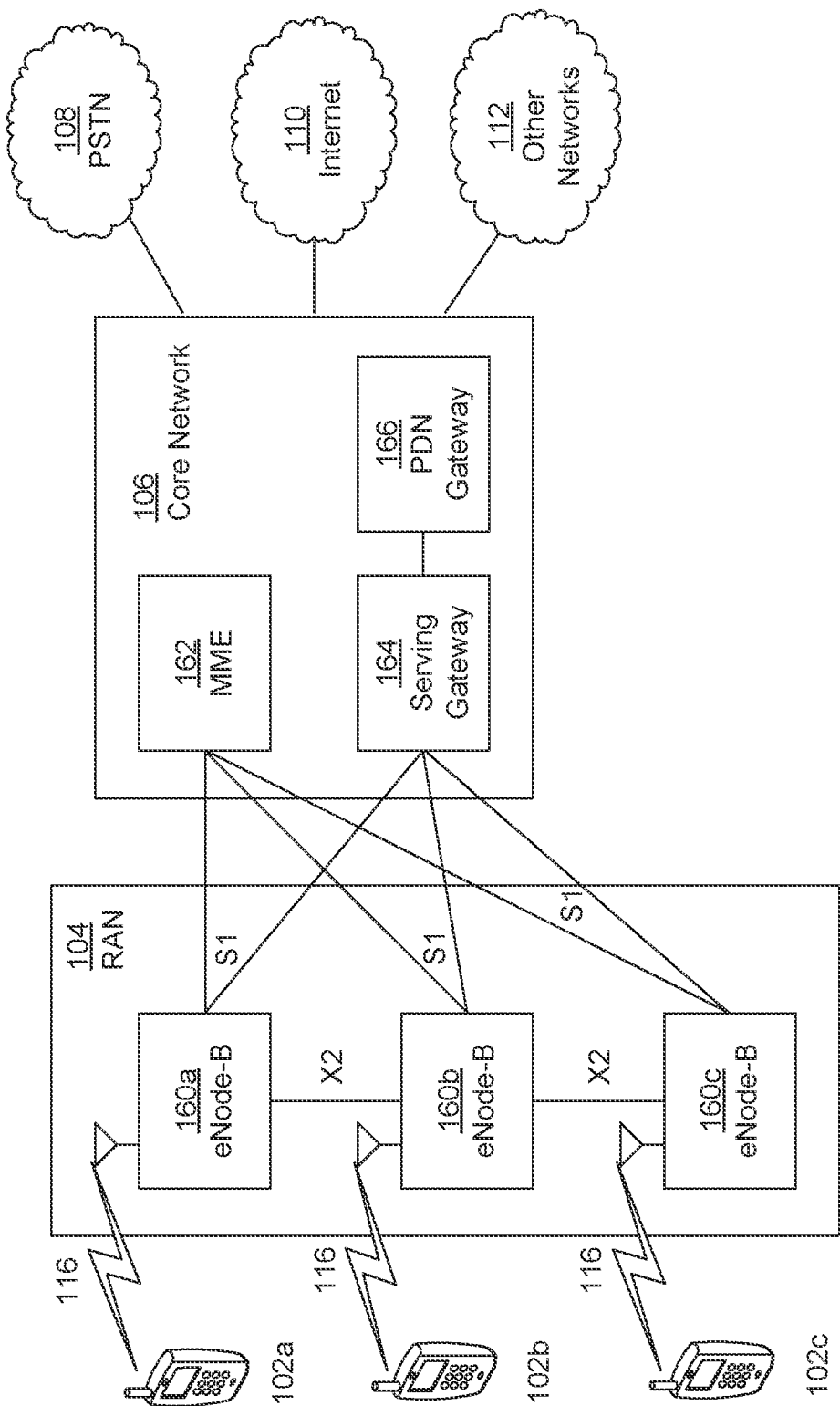


FIG. 1C

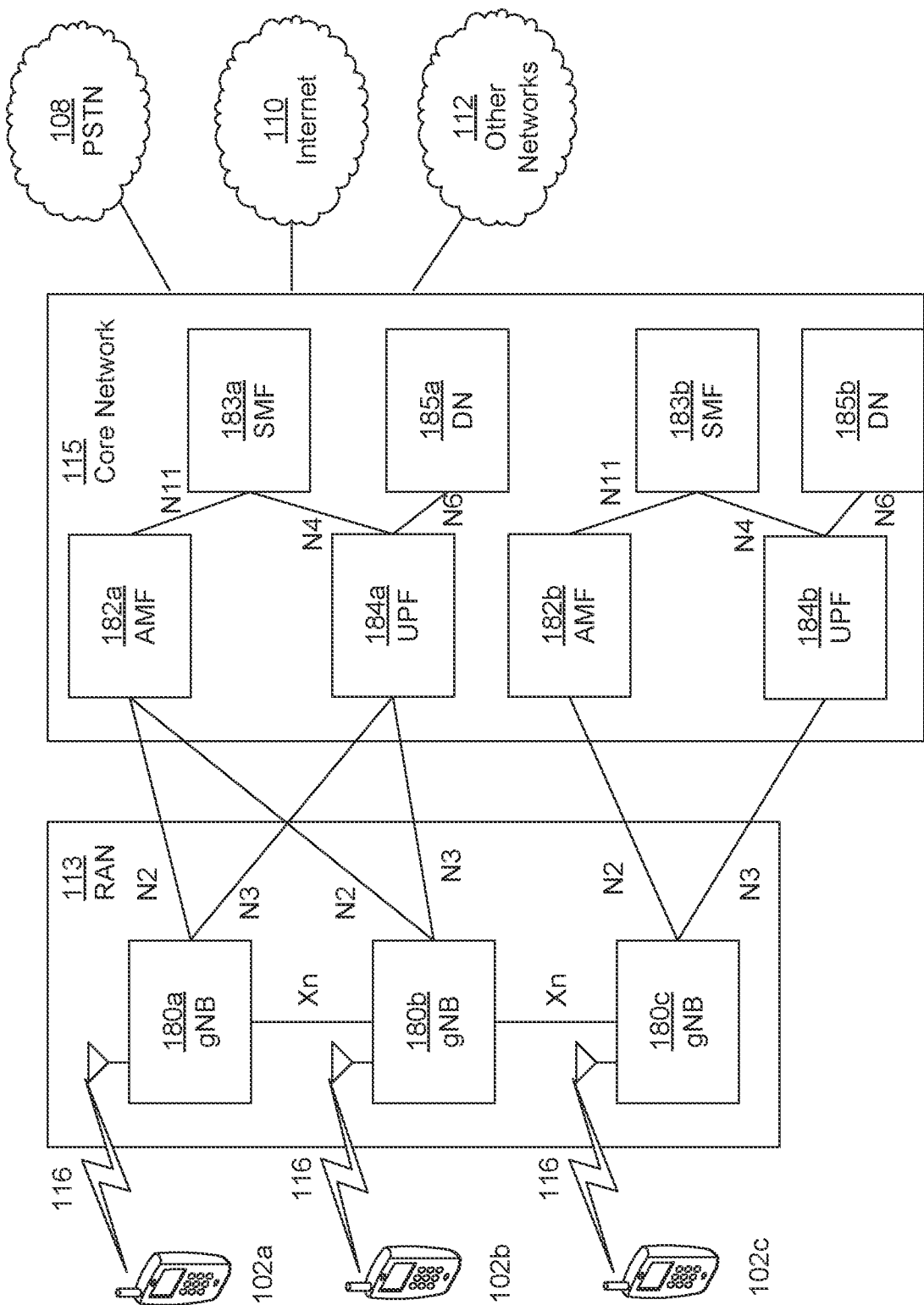


FIG. 1D

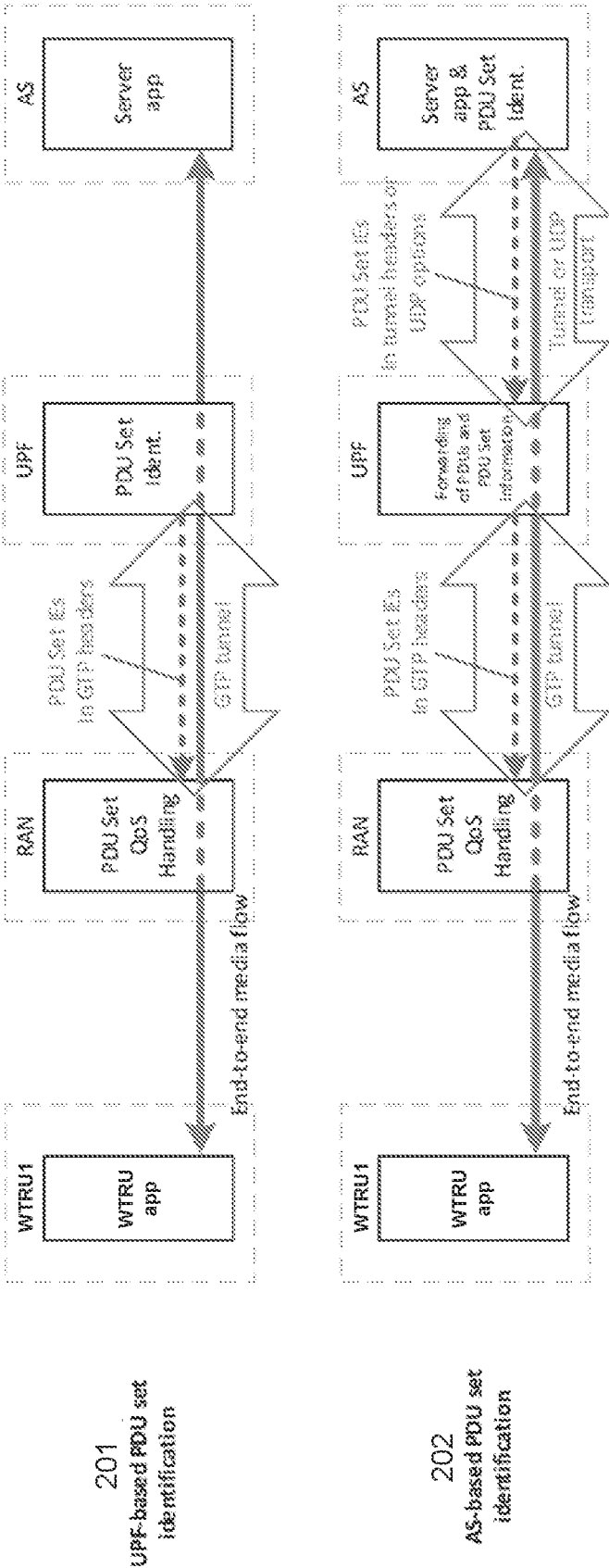
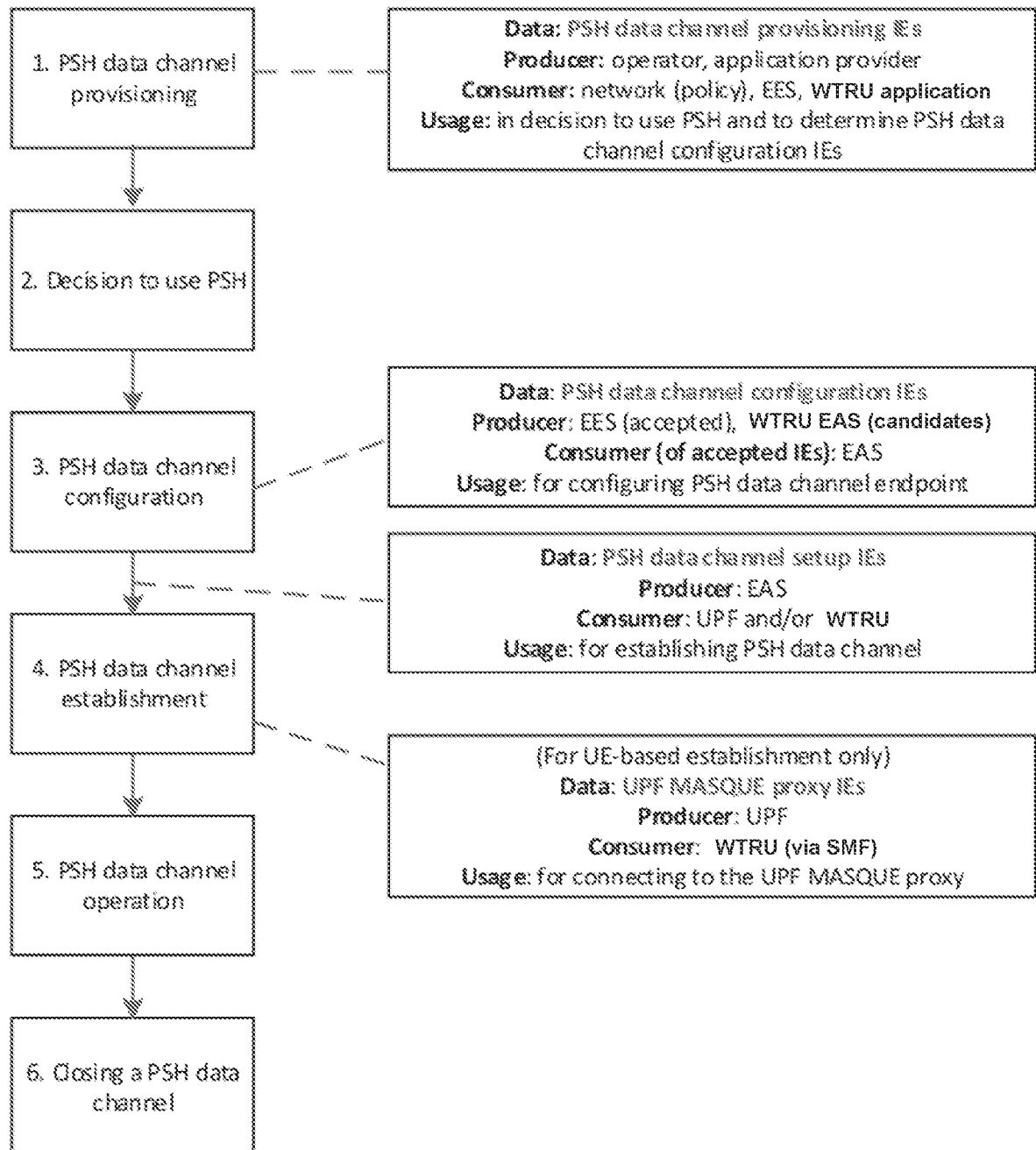


FIG. 2

6/15

**FIG. 3**

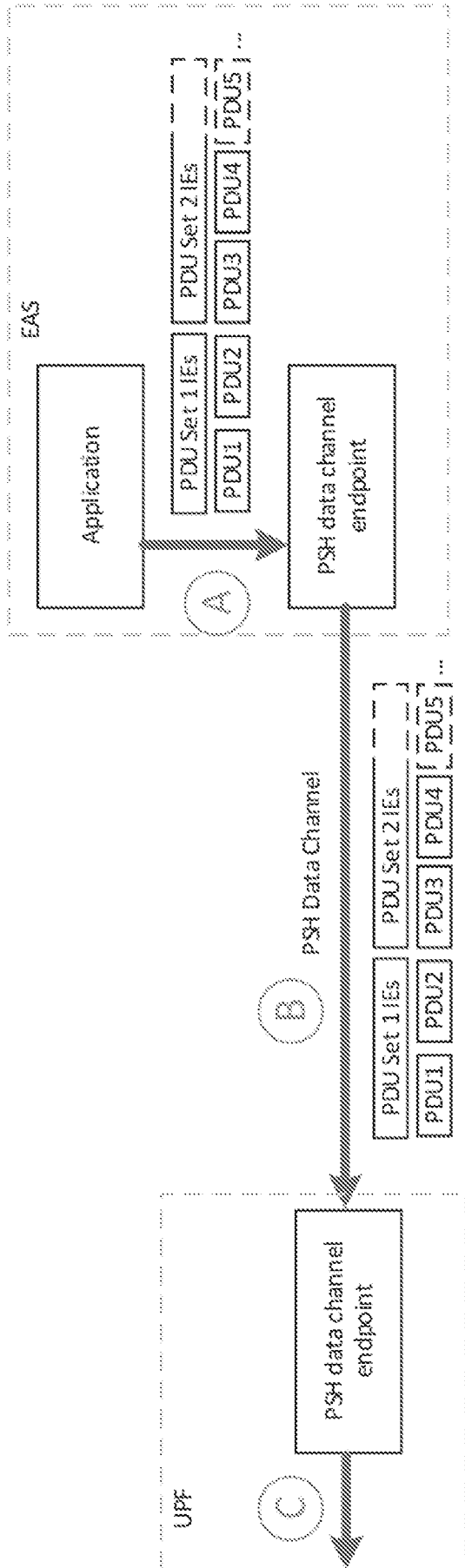


FIG. 4A

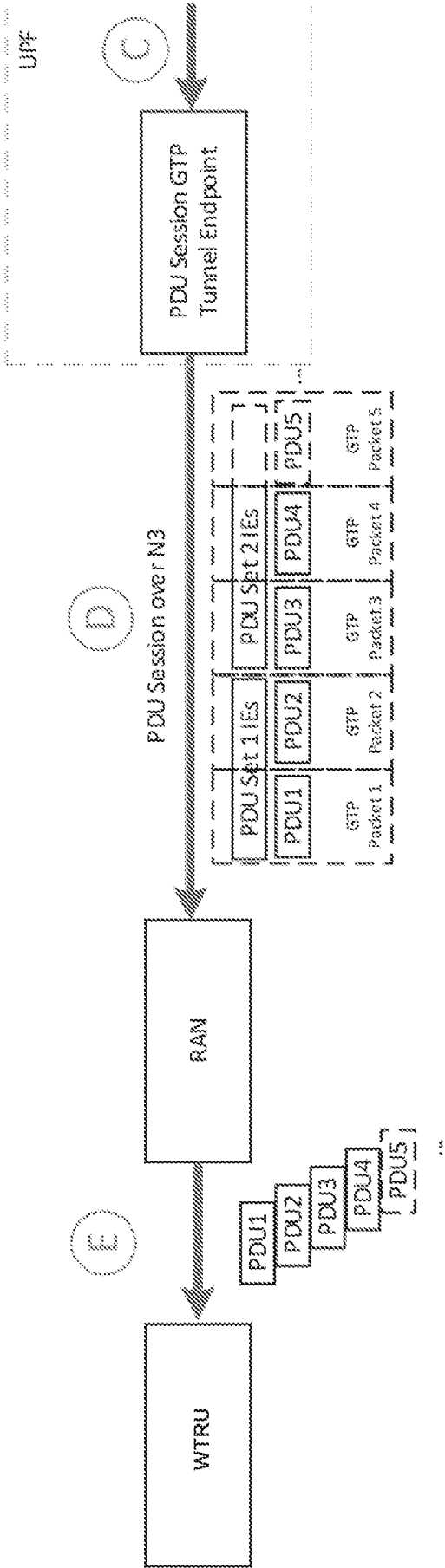


FIG. 4B

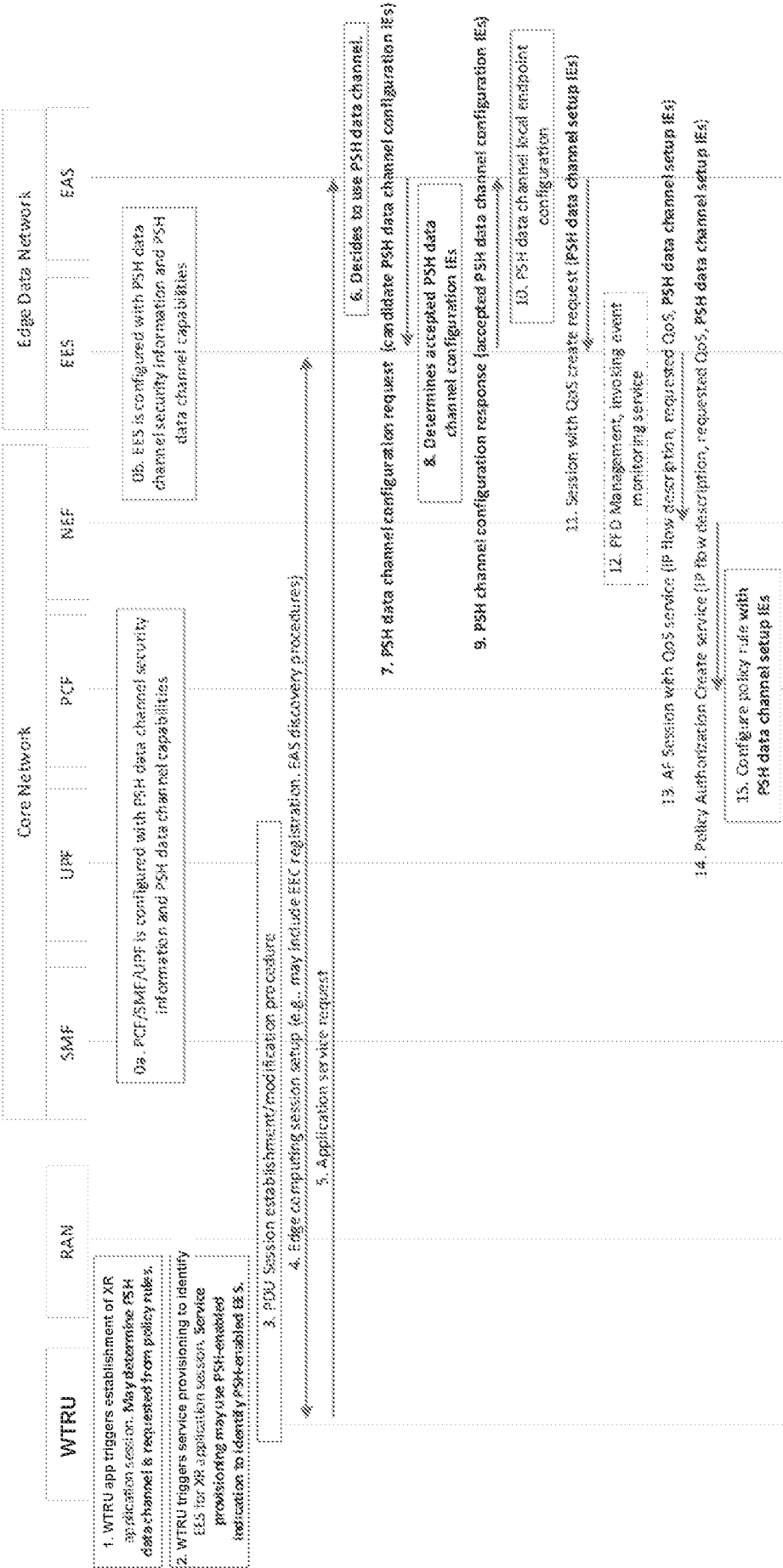


FIG. 5A

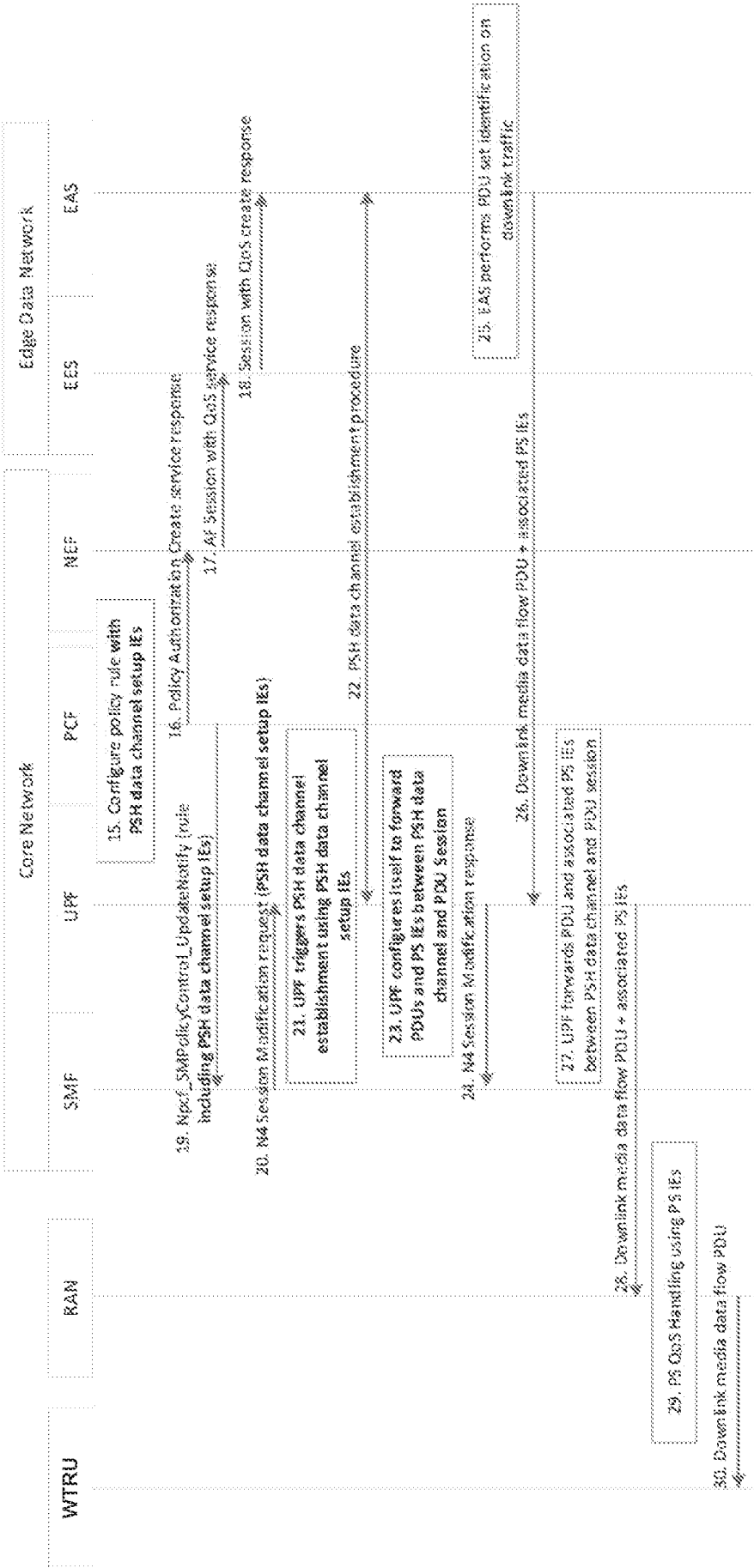


FIG. 5B

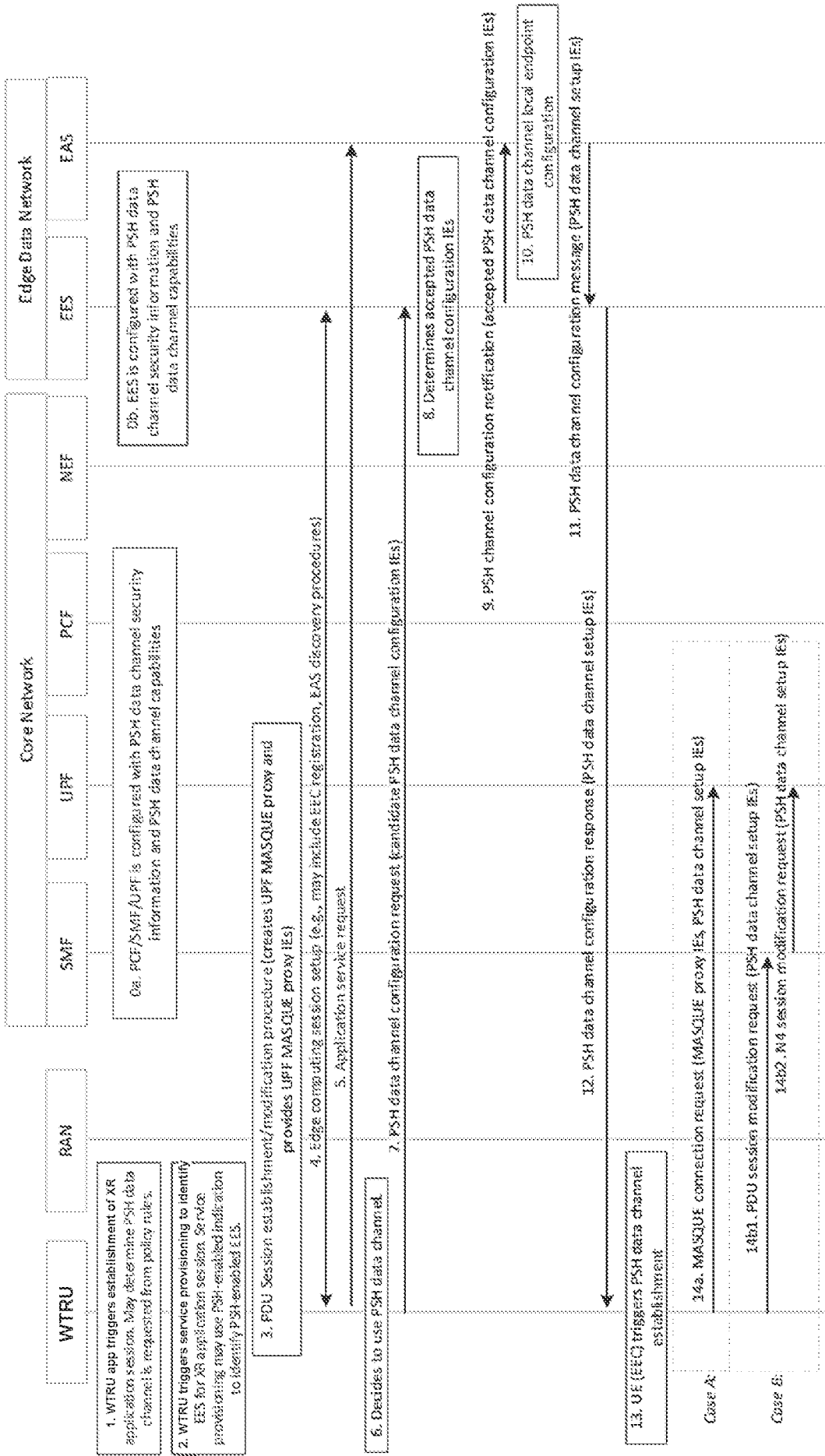


FIG. 6A

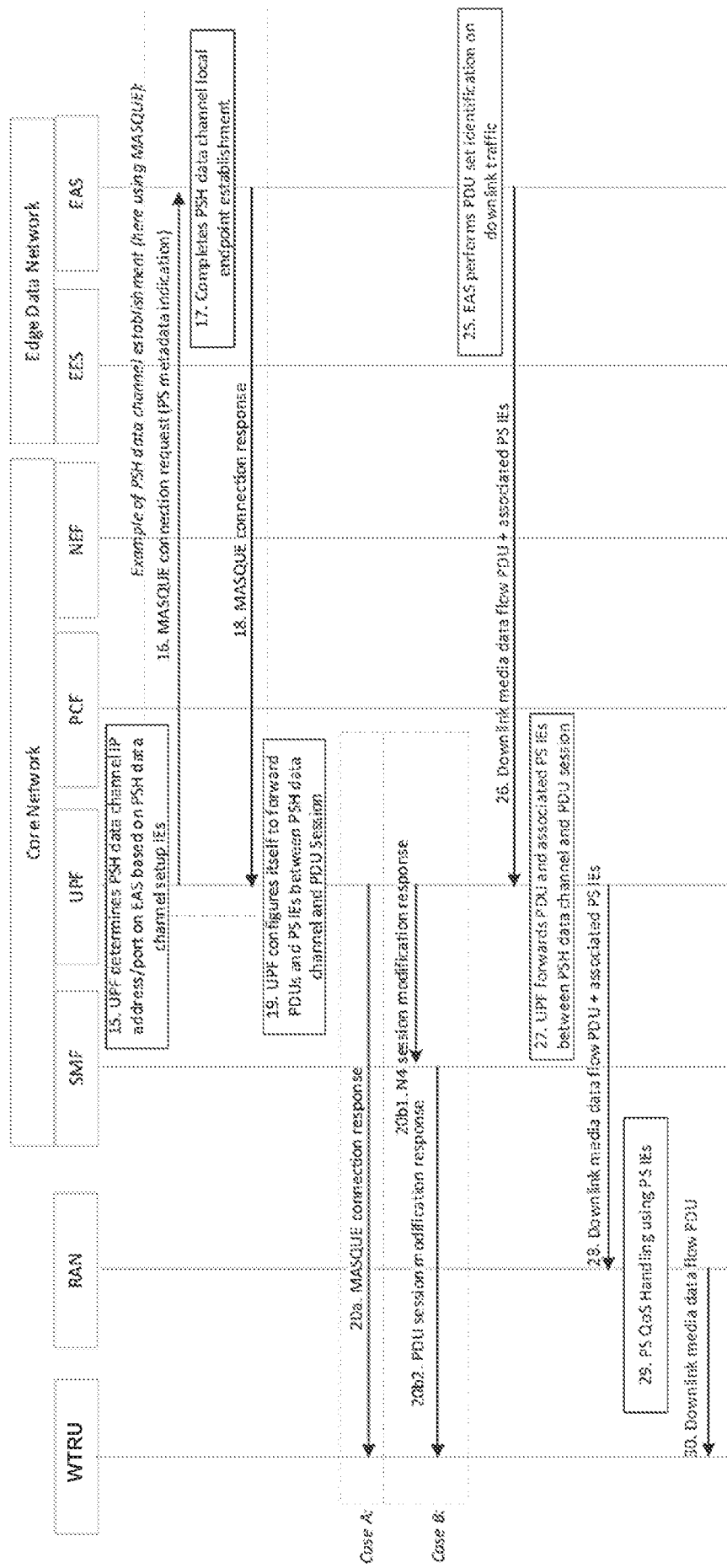
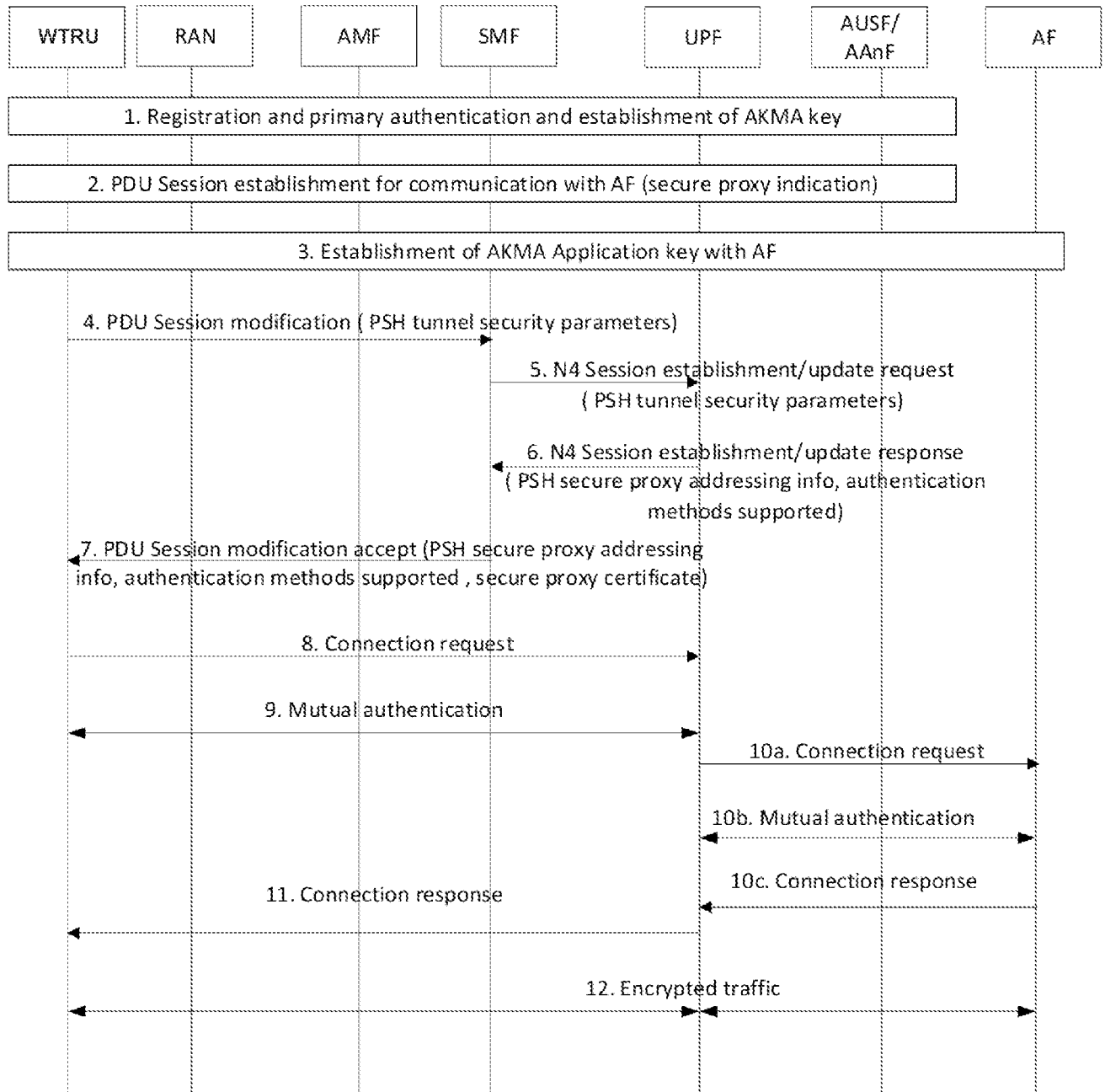


FIG. 6B

13/15

**FIG. 7**

14/15

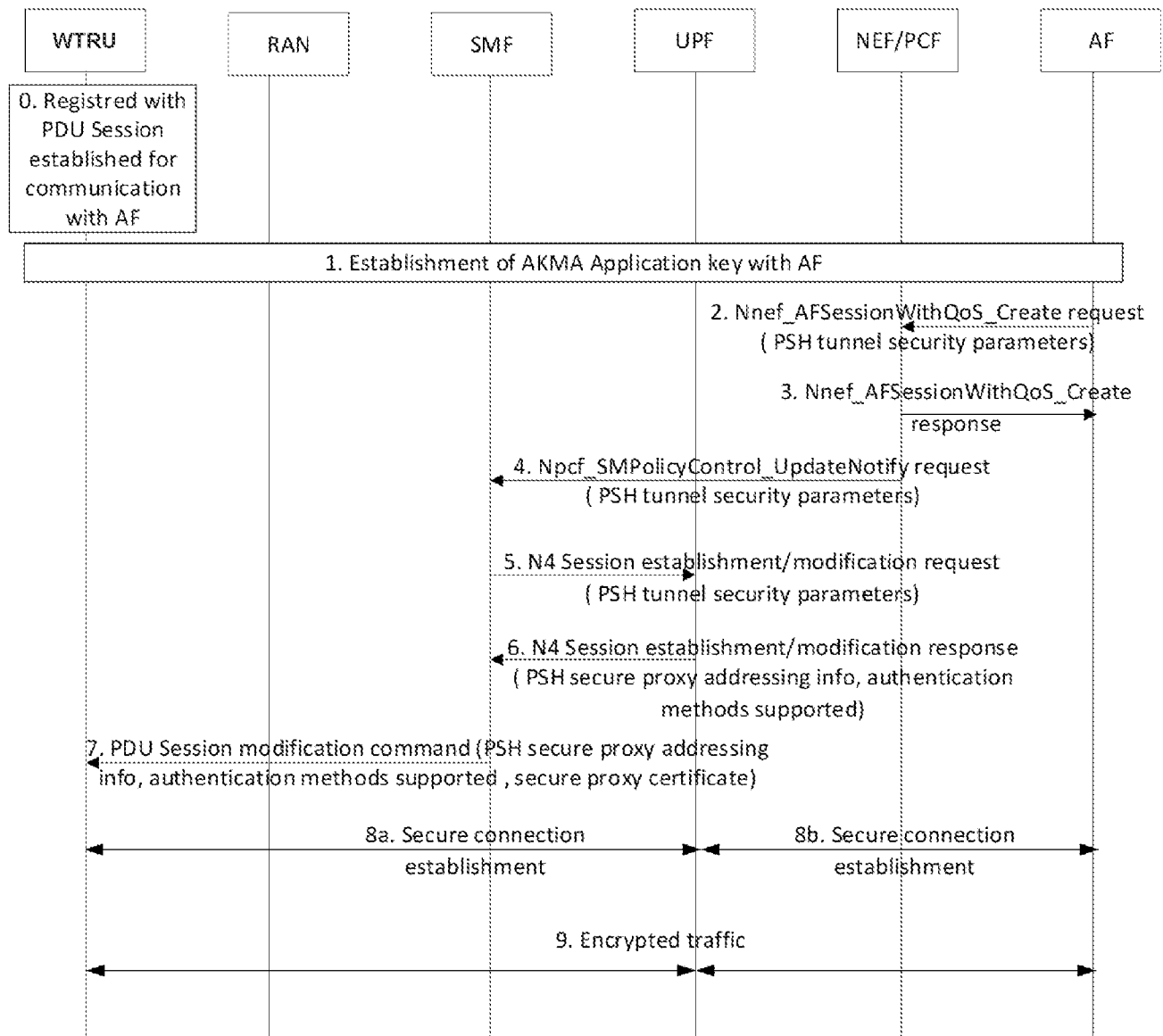


FIG. 8

15/15

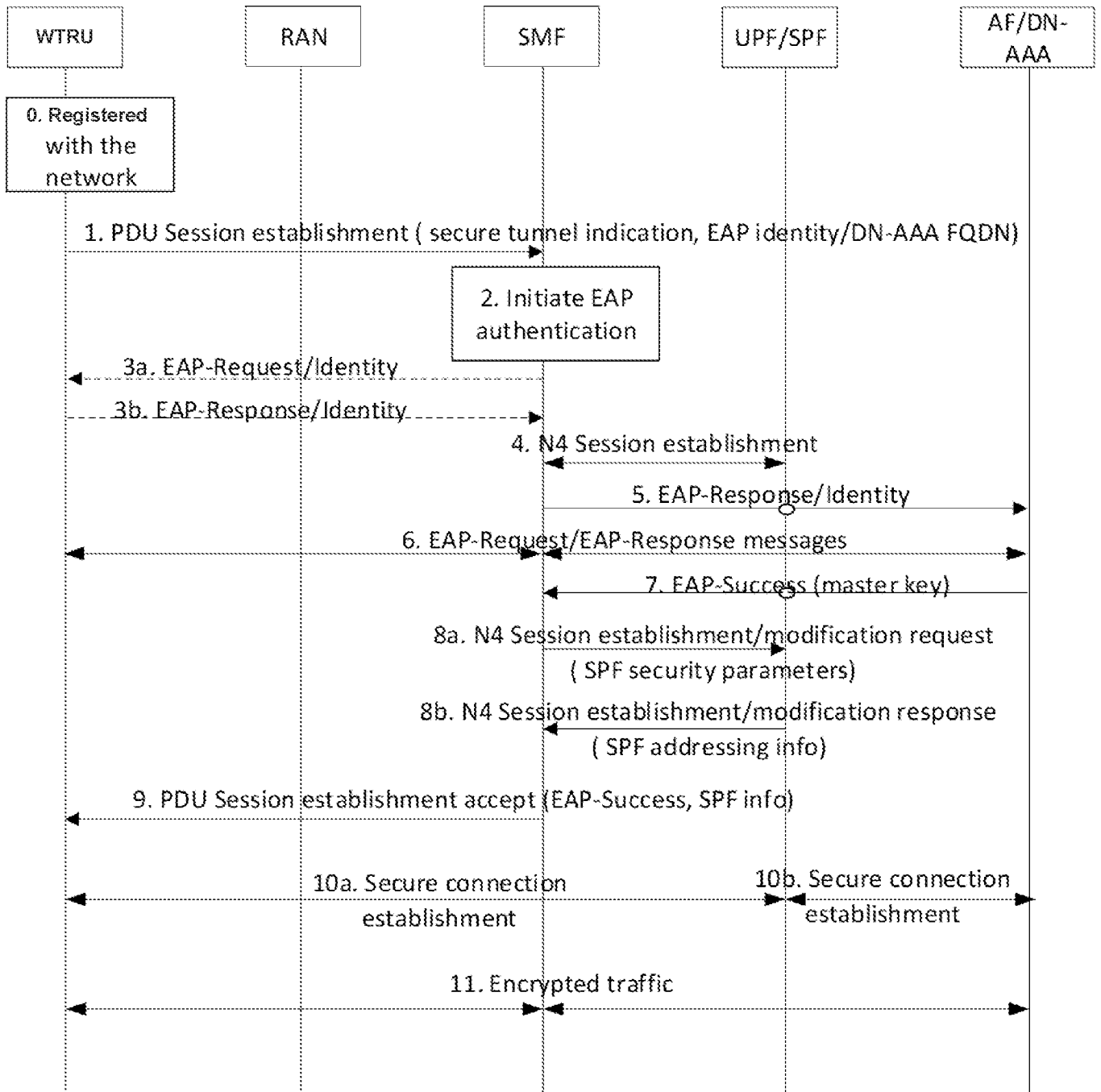


FIG. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/036804

A. CLASSIFICATION OF SUBJECT MATTER		
INV.	H04W4/50	H04L67/141 H04W28/24
ADD.	H04W12/033 H04W12/069	H04W28/02 H04L9/40
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, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KENICHI YAMAMOTO ET AL: "PDU Set information provisioning", 3GPP DRAFT; S2-2306195; TYPE CR; CR 3999; XRM, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG2, no. Online; 20230417 - 20230421 24 April 2023 (2023-04-24), XP052297497, Retrieved from the Internet: URL:https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_156E_Electronic_2023-04/Docs/S2-2306195.zip S2-2306195 was 4389r01_XRM_KI4-5_23502 PDU Set information provisioning.docx [retrieved on 2023-04-24]	7 - 12
A	section 4.15.6.6 - / - -	1 - 6,
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 9 October 2024		Date of mailing of the international search report 21/10/2024
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Ruiz Sanchez, J

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2024/036804

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	section 5.2.5.3.2 section 5.2.6.9.2 -----	13 - 16
Y	WO 2023/274366 A1 (ERICSSON TELEFON AB L M [SE]; XU WENLIANG [CN]) 5 January 2023 (2023-01-05) paragraphs [0078] - [0114] paragraphs [0157] - [0218] -----	1 - 16
Y	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on XR (Extended Reality) and media services (Release 18)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 23.700-60, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V18.0.0 21 December 2022 (2022-12-21), pages 1-266, XP052234762, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/23_series/23.700-60/23700-60-i00.zip 23700-60-i00.docx [retrieved on 2022-12-21] sections 5.4, 5.5 section 6.12.3.1 section 6.14.3.1 section 6.23.3 sections 6.24, 6.25 sections 6.52, 6.56, 6.57 -----	1 - 16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2024/036804

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2023274366 A1	05-01-2023	CN 117616784 A	27-02-2024
		EP 4364442 A1	08-05-2024
		US 2024276300 A1	15-08-2024
		WO 2023274366 A1	05-01-2023
