

(43) International Publication Date
12 September 2013 (12.09.2013)(51) International Patent Classification:
H04W 48/16 (2009.01)

(21) International Application Number:

PCT/US2013/029933

(22) International Filing Date:

8 March 2013 (08.03.2013)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/609,157 9 March 2012 (09.03.2012) US
61/703,921 21 September 2012 (21.09.2012) US

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

(72) Inventors: **LIVET, Catherine**; 5023 Rue De Brebeuf, Montreal, QC H2J 3L6 (CA). **REZNIK, Alexander**; 1212 River Road, Titusville, New Jersey 08560 (US). **PERRAS, Michelle**; 4434 Christophe-Colomb, Montreal, Quebec H2J 3G5 (CA). **TARGALI, Yousif**; 183 Delaware Ave, Cliffwood, NJ 07721 (US). **CHITRAPU, Prabhakar**; 135 Brochant Drive, Blue Bell, Pennsylvania 19422 (US). **SHAHEEN, Kamel M.**; 429 Ashton Drive, King of Prussia, Pennsylvania 19406 (US). **KARAMPATIS, Dimitrios**; 24 Shepherds Lane, Caversham, Reading RG4 7JL

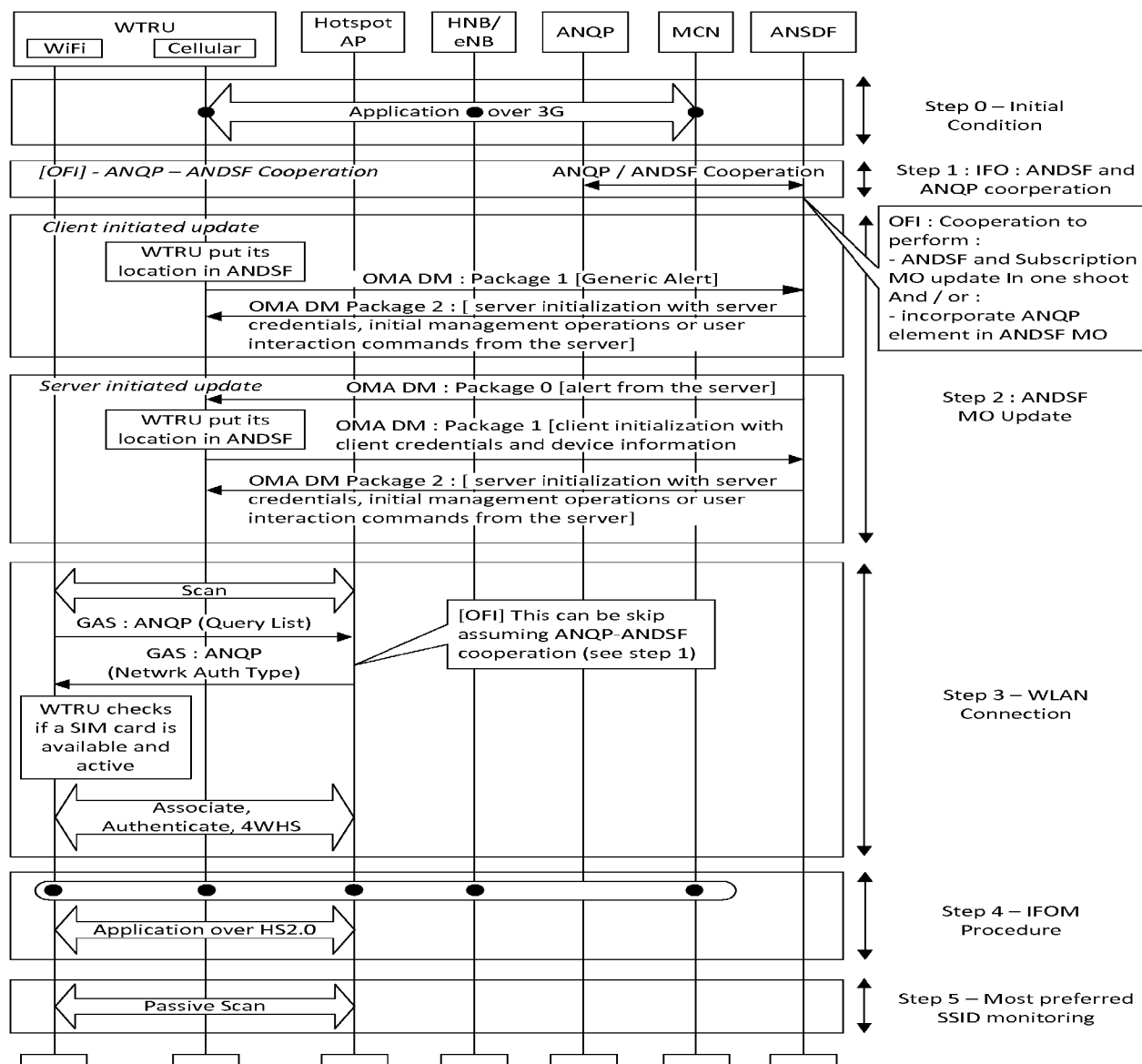


FIG. 12



(GB). **ZUNIGA, Juan, Carlos**; 955 Rue Gohier, Ville St. Laurent, Montreal, QC H4L 3J4 (CA).

(74) Agents: ROCCIA, Vincent, J. et al.; Condo Roccia LLP, One Liberty Place, Suite 2200, 1650 Market Street, Philadelphia, PA 19103 (US).

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

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(57) Abstract: Systems, methods, and instrumentalities are disclosed to assist a user equipment (UE) in accessing a wireless local area network (WLAN). A first UE may obtain information from one or more WLANs. The information may include, for example, an access network query protocol (ANQP) element associated with a WLAN. The first UE may send the information to an access network discovery and selection function (ANDSF). The ANDSF may update an ANDSF management object (MO) based on the received information. The ANDSF may receive information from a plurality of UEs relating to one or more WLANs. The ANDSF may send the updated ANDSF MO to at least one of a second UE or an access point. The updated ANDSF MO may comprise information about WLAN networks available to the second UE. The second UE may forego an ANQP query of a WLAN when the updated ANDSF MO includes information about the WLAN.

HOTSPOT EVOLUTION SUPPORT AND DISCOVERY THROUGH NON-3GPP ACCESS NETWORKS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 61/609,157, filed March 9, 2012 and U.S. Provisional Patent Application No. 61/703,921, filed September 21, 2012, the contents of which are hereby incorporated by reference herein.

BACKGROUND

[0002] Wireless (e.g., Wi-Fi) networks and wireless hotspots are becoming increasingly common in many cities. Mobile users that are communicating via a cellular communications network may encounter Wi-Fi networks and hotspots that are deployed throughout the world. However, connecting to the Wi-Fi networks and hotspots via a mobile device may be different than connecting to a cellular network. A user of a mobile device may need to select a Wi-Fi network or hotspot and provide credentials, a security key, and/or other information.

SUMMARY OF THE INVENTION

[0003] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

[0004] Systems, methods, and instrumentalities are disclosed to provide network access, for example to provide information to a user equipment (UE) to assist the UE in accessing a wireless local area network (WLAN), e.g., a wi-fi network. A first UE may obtain information from one or more WLANs (e.g., by a query/response via a WLAN access point (AP), such as a Hotspot 2.0 (HS 2.0) AP). The information may include, for example, an access network query protocol (ANQP) element associated with a WLAN. The first UE may send the information to,

and the information may be received by, a network entity such as an access network discovery and selection function (ANDSF), e.g., on an ANDSF server associated with a 3GPP network. The ANDSF may update an ANDSF management object (MO) based on the received information. The ANDSF may receive information from a plurality of UEs, relating to one or more WLANs, in a similar manner. The ANDSF may send the updated ANDSF MO to at least one of a second UE or an access point (e.g., a WLAN access point). For example, the ANDSF may send the updated ANDSF MO in response to a request from the second UE. When the ANDSF sends the updated ANDSF MO to the access point, the access point may send the updated ANDSF MO to the second UE (e.g., when receiving a request from the second UE). The updated ANDSF MO may comprise information about WLAN networks available to the second UE. The second UE may forego an ANQP query of a WLAN when the updated ANDSF MO includes information about the WLAN.

[0005] The updated ANDSF MO may be a generic ANDSF MO. For example, the generic ANDSF MO may be capable of being used by a plurality of UEs associated with a network (e.g., each of the plurality of UEs may be capable of using the ANDSF MO to choose a WLAN with which to connect). The generic ANDSF MO may not include UE-specific information. The generic ANDSF MO may include a prioritized list of WLAN networks. A UE may use the generic ANDSF MO to choose a WLAN with which to connect (e.g., without querying WLANs, querying fewer WLANs, etc.). A WLAN may receive the generic ANDSF MO from the ANDSF and provide the generic ANDSF MO to a UE connected to the WLAN, e.g., a UE looking for another WLAN with which to connect.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] A more detailed understanding may be had from the following description, given by way of example in conjunction with the accompanying drawings wherein:

[0007] FIG. 1A depicts a system diagram of an example communications system in which one or more disclosed embodiments may be implemented.

[0008] FIG. 1B depicts a system diagram of an example wireless transmit/receive unit (WTRU) that may be used within the communications system illustrated in FIG. 1A.

[0009] FIG. 1C depicts a system diagram of an example radio access network and an example core network that may be used within the communications system illustrated in FIG. 1A.

- [0010] FIG. 1D depicts a system diagram of an example radio access network and an example core network that may be used within the communications system illustrated in FIG. 1A.
- [0011] FIG. 1E depicts a system diagram of an example radio access network and an example core network that may be used within the communications system illustrated in FIG. 1A.
- [0012] FIG. 2 shows an exemplary network architecture that includes macro and/or femto cell deployment with a hotspot network;
- [0013] FIG. 3 shows an example of an Access Network Discovery and Selection Function (ANDSF) Management Object (MO);
- [0014] FIG. 4 shows an example format for 3GPP Cellular Network information;
- [0015] FIG. 5 shows an example structure for a generic container;
- [0016] FIG. 6 shows an example of a hotspot network selection for a mobile device;
- [0017] FIG. 7 shows an example of an IEEE 802.xx/Extensible Authentication Protocol (EAP) protocol stack;
- [0018] FIG. 8 shows an example call-flow diagram for EAP-SIM/AKA-based public hotspot access;
- [0019] FIG. 9 shows an example of WiFi-3GPP integration using EAP-SIM;
- [0020] FIG. 10 shows an example of AAA proxy-based Hotspot-3GPP interworking;
- [0021] FIG. 11 shows an example of Single Sign-On (SSO)-based WiFi-Cellular integration;
- [0022] FIG. 12 shows an example of seamless IP Flow Mobility (IFOM) from 3GPP to hotspot;
- [0023] FIG. 13 shows an example of an access network discovery information sub-tree;
- [0024] FIG. 14 shows an example of an ANDSF-MO-WTRU location sub-tree;
- [0025] FIG. 15 shows an example of an ANDSF MO - Policy (ISMP) information sub-tree;
- [0026] FIG. 16 is an example of an ANDSF MO - ISRP sub-tree;
- [0027] FIG. 17 shows an example of seamless IFOM mobility from a hotspot to another hotspot;
- [0028] FIG. 18 shows an example of a shared 3GPP internet connection (tethering) via Wi-Fi;
- [0029] FIG. 19 shows exemplary connection sharing;

[0030] FIG. 20 shows an exemplary enhanced ANDSF MO with elements added to enable connection sharing;

[0031] FIG. 21 shows an example of neighbor discovery via an Access Network Query Protocol (ANQP) update; and

[0032] FIG. 22 depicts an example radio access network with an Access Network Discovery and Selection Function (ANDSF) and respective interfaces between the ANDSF and one or more Access Points (APs) and/or WLAN gateways.

DETAILED DESCRIPTION

[0033] A detailed description of illustrative embodiments will now be described with reference to the various figures. Although this description provides a detailed example of possible implementations, it should be noted that the details are intended to be exemplary and in no way limit the scope of the application. The figures may illustrate call flows, which are meant to be exemplary. Other embodiments may be used. The order of the messages may be varied where appropriate. Messages may be omitted if not needed, and, additional flow steps may be added. As used herein, the term UE may relate to a WTRU.

[0034] FIG. 1A is a diagram of an example communications system 100 in which one or more disclosed embodiments may be implemented. For example, a wireless network (e.g., a wireless network comprising one or more components of the communications system 100) may be configured such that bearers that extend beyond the wireless network (e.g., beyond a walled garden associated with the wireless network) may be assigned QoS characteristics.

[0035] 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), and the like.

[0036] As shown in FIG. 1A, the communications system 100 may include at least one wireless transmit/receive unit (WTRU), such as a plurality of WTRUs, for instance WTRUs 102a, 102b, 102c, and 102d, a radio access network (RAN) 104, a core network 106, a public switched telephone network (PSTN) 108, the Internet 110, and other networks 112, though it should 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 may be configured to transmit and/or receive wireless signals and may include user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a cellular telephone, a personal digital assistant (PDA), a smartphone, a laptop, a netbook, a personal computer, a wireless sensor, consumer electronics, and the like.

[0037] The communications systems 100 may also include a base station 114a and 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 core network 106, the Internet 110, and/or the 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 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 should be appreciated that the base stations 114a, 114b may include any number of interconnected base stations and/or network elements.

[0038] The base station 114a may be part of the RAN 104, 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 within a particular geographic region, which may be referred to as a cell (not shown). 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, i.e., one for each sector of the cell. In another embodiment, the base station 114a may employ multiple-input multiple output (MIMO) technology and, therefore, may utilize multiple transceivers for each sector of the cell.

[0039] 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, infrared (IR), ultraviolet (UV), visible light, etc.). The air interface 116 may be established using any suitable radio access technology (RAT).

[0040] 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 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 116 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 Packet Access (HSDPA) and/or High-Speed Uplink Packet Access (HSUPA).

[0041] In another 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).

[0042] In other embodiments, the base station 114a and the WTRUs 102a, 102b, 102c may implement radio technologies such as 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.

[0043] 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, 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 another 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, 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 core network 106.

[0044] The RAN 104 may be in communication with the core network 106, 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. For example, the core network 106 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 should be appreciated

that the RAN 104 and/or the core network 106 may be in direct or indirect communication with other RANs that employ the same RAT as the RAN 104 or a different RAT. For example, in addition to being connected to the RAN 104, which may be utilizing an E-UTRA radio technology, the core network 106 may also be in communication with another RAN (not shown) employing a GSM radio technology.

[0045] The core network 106 may also serve as a gateway for the WTRUs 102a, 102b, 102c, 102d to access the PSTN 108, the Internet 110, and/or 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 the internet protocol (IP) in the TCP/IP internet protocol suite. The networks 112 may include wired or wireless communications networks owned and/or operated by other service providers. For example, the networks 112 may include another core network connected to one or more RANs, which may employ the same RAT as the RAN 104 or a different RAT.

[0046] Some or all of the WTRUs 102a, 102b, 102c, 102d in the communications system 100 may include multi-mode capabilities, i.e., 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.

[0047] FIG. 1B is a system diagram of 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 other peripherals 138. It should be appreciated that the WTRU 102 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment.

[0048] 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 Array (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 should be appreciated that the processor 118 and the transceiver 120 may be integrated together in an electronic package or chip.

[0049] 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 another 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 receive both RF and light signals. It should be appreciated that the transmit/receive element 122 may be configured to transmit and/or receive any combination of wireless signals.

[0050] In addition, 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.

[0051] 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 UTRA and IEEE 802.11, for example.

[0052] 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).

[0053] 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.

[0054] 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 should be appreciated that the WTRU 102 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

[0055] 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 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, and the like.

[0056] FIG. 1C is a system diagram of an embodiment of the communications system 100 that includes a RAN 104a and a core network 106a that comprise example implementations of the RAN 104 and the core network 106, respectively. As noted above, the RAN 104, for instance the RAN 104a, may employ a UTRA radio technology to communicate with the WTRUs 102a, 102b, and 102c over the air interface 116. The RAN 104a may also be in communication with the core network 106a. As shown in FIG. 1C, the RAN 104a may include Node-Bs 140a, 140b, 140c, which may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 116. The Node-Bs 140a, 140b, 140c may each be associated with a particular cell (not shown) within the RAN 104a. The RAN 104a may also include RNCs 142a, 142b. It should be appreciated that the RAN 104a may include any number of Node-Bs and RNCs while remaining consistent with an embodiment.

[0057] As shown in FIG. 1C, the Node-Bs 140a, 140b may be in communication with the RNC 142a. Additionally, the Node-B 140c may be in communication with the RNC 142b. The

Node-Bs 140a, 140b, 140c may communicate with the respective RNCs 142a, 142b via an Iub interface. The RNCs 142a, 142b may be in communication with one another via an Iur interface. Each of the RNCs 142a, 142b may be configured to control the respective Node-Bs 140a, 140b, 140c to which it is connected. In addition, each of the RNCs 142a, 142b may be configured to carry out or support other functionality, such as outer loop power control, load control, admission control, packet scheduling, handover control, macrodiversity, security functions, data encryption, and the like.

[0058] The core network 106a shown in FIG. 1C may include a media gateway (MGW) 144, a mobile switching center (MSC) 146, a serving GPRS support node (SGSN) 148, and/or a gateway GPRS support node (GGSN) 150. While each of the foregoing elements is depicted as part of the core network 106a, it should be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0059] The RNC 142a in the RAN 104a may be connected to the MSC 146 in the core network 106a via an IuCS interface. The MSC 146 may be connected to the MGW 144. The MSC 146 and the MGW 144 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.

[0060] The RNC 142a in the RAN 104a may also be connected to the SGSN 148 in the core network 106a via an IuPS interface. The SGSN 148 may be connected to the GGSN 150. The SGSN 148 and the GGSN 150 may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between and the WTRUs 102a, 102b, 102c and IP-enabled devices.

[0061] As noted above, the core network 106a may also be connected to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0062] FIG. 1D is a system diagram of an embodiment of the communications system 100 that includes a RAN 104b and a core network 106b that comprise example implementations of the RAN 104 and the core network 106, respectively. As noted above, the RAN 104, for instance the RAN 104b, may employ an E-UTRA radio technology to communicate with the WTRUs 102a, 102b, and 102c over the air interface 116. The RAN 104b may also be in communication with the core network 106b.

[0063] The RAN 104b may include eNode-Bs 140d, 140e, 140f, though it should be appreciated that the RAN 104b may include any number of eNode-Bs while remaining consistent with an embodiment. The eNode-Bs 140d, 140e, 140f 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 140d, 140e, 140f may implement MIMO technology. Thus, the eNode-B 140d, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 102a.

[0064] Each of the eNode-Bs 140d, 140e, and 140f 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 uplink and/or downlink, and the like. As shown in FIG. 1D, the eNode-Bs 140d, 140e, 140f may communicate with one another over an X2 interface.

[0065] The core network 106b shown in FIG. 1D may include a mobility management gateway (MME) 143, a serving gateway 145, and a packet data network (PDN) gateway 147. While each of the foregoing elements is depicted as part of the core network 106b, it should be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0066] The MME 143 may be connected to each of the eNode-Bs 140d, 140e, and 140f in the RAN 104b via an S1 interface and may serve as a control node. For example, the MME 143 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 143 may also provide a control plane function for switching between the RAN 104b and other RANs (not shown) that employ other radio technologies, such as GSM or WCDMA.

[0067] The serving gateway 145 may be connected to each of the eNode Bs 140d, 140e, 140f in the RAN 104b via the S1 interface. The serving gateway 145 may generally route and forward user data packets to/from the WTRUs 102a, 102b, 102c. The serving gateway 145 may also perform other functions, such as anchoring user planes during inter-eNode B handovers, triggering paging when downlink data is available for the WTRUs 102a, 102b, 102c, managing and storing contexts of the WTRUs 102a, 102b, 102c, and the like.

[0068] The serving gateway 145 may also be connected to the PDN gateway 147, 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.

[0069] The core network 106b may facilitate communications with other networks. For example, the core network 106b 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 core network 106b may include, or may communicate with, an IP gateway (e.g., an IP multimedia subsystem (IMS) server) that serves as an interface between the core network 106b and the PSTN 108. In addition, the core network 106b may provide the WTRUs 102a, 102b, 102c with access to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0070] FIG. 1E is a system diagram of an embodiment of the communications system 100 that includes a RAN 104c and a core network 106c that comprise example implementations of the RAN 104 and the core network 106, respectively. The RAN 104, for instance the RAN 104c, may be an access service network (ASN) that employs IEEE 802.16 radio technology to communicate with the WTRUs 102a, 102b, and 102c over the air interface 116. As described herein, the communication links between the different functional entities of the WTRUs 102a, 102b, 102c, the RAN 104c, and the core network 106c may be defined as reference points.

[0071] As shown in FIG. 1E, the RAN 104c may include base stations 102a, 102b, 102c, and an ASN gateway 141, though it should be appreciated that the RAN 104c may include any number of base stations and ASN gateways while remaining consistent with an embodiment. The base stations 102a, 102b, 102c may each be associated with a particular cell (not shown) in the RAN 104c and may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 116. In one embodiment, the base stations 140g, 140h, 140i may implement MIMO technology. Thus, the base station 140g, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 102a. The base stations 140g, 140h, 140i may also provide mobility management functions, such as handoff triggering, tunnel establishment, radio resource management, traffic classification, quality of service (QoS) policy enforcement, and the like. The ASN Gateway 141 may serve as a traffic aggregation point and may be responsible for paging, caching of subscriber profiles, routing to the core network 106c, and the like.

[0072] The air interface 116 between the WTRUs 102a, 102b, 102c and the RAN 104c may be defined as an R1 reference point that implements the IEEE 802.16 specification. In addition, each of the WTRUs 102a, 102b, and 102c may establish a logical interface (not shown) with the core network 106c. The logical interface between the WTRUs 102a, 102b, 102c and the core network 106c may be defined as an R2 reference point, which may be used for authentication, authorization, IP host configuration management, and/or mobility management.

[0073] The communication link between each of the base stations 140g, 140h, 140i may be defined as an R8 reference point that includes protocols for facilitating WTRU handovers and

the transfer of data between base stations. The communication link between the base stations 140g, 140h, 140i and the ASN gateway 141 may be defined as an R6 reference point. The R6 reference point may include protocols for facilitating mobility management based on mobility events associated with each of the WTRUs 102a, 102b, 102c.

[0074] As shown in FIG. 1E, the RAN 104c may be connected to the core network 106c. The communication link between the RAN 104c and the core network 106c may be defined as an R3 reference point that includes protocols for facilitating data transfer and mobility management capabilities, for example. The core network 106c may include a mobile IP home agent (MIP-HA) 144, an authentication, authorization, accounting (AAA) server 156, and a gateway 158. While each of the foregoing elements is depicted as part of the core network 106c, it should be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0075] The MIP-HA may be responsible for IP address management, and may enable the WTRUs 102a, 102b, and 102c to roam between different ASNs and/or different core networks. The MIP-HA 154 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 AAA server 156 may be responsible for user authentication and for supporting user services. The gateway 158 may facilitate interworking with other networks. For example, the gateway 158 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 landline communications devices. In addition, the gateway 158 may provide the WTRUs 102a, 102b, 102c with access to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0076] Although not shown in FIG. 1E, it should be appreciated that the RAN 104c may be connected to other ASNs and the core network 106c may be connected to other core networks. The communication link between the RAN 104c and the other ASNs may be defined as an R4 reference point, which may include protocols for coordinating the mobility of the WTRUs 102a, 102b, 102c between the RAN 104c and the other ASNs. The communication link between the core network 106c and the other core networks may be defined as an R5 reference point, which may include protocols for facilitating interworking between home core networks and visited core networks.

[0077] FIG. 2 shows an exemplary network architecture that may include macro and/or femto cell deployment with a hotspot network. The WTRU may have one or more of the

following. The WTRU may be a simultaneous dual (3GPP / Wi-Fi) RAT WTRU capable of providing IP flow mobility (IFOM) over both technologies. One or more Wi-Fi cards may be ON simultaneously. Hotspot technology or other evolved hotspot technology may be enabled. The WTRU may support access network query protocol (ANQP). The WTRU may support hotspot protocols or other communication methods. The WTRU may use hotspot security requirements (e.g., with or without SIM credentials). The WTRU may support on-line sign up, which may include subscription management object (MO) provisioning. Mobility features may be supported. The WTRU may include an embedded connection sharing client.

[0078] The network (for example, a 3GPP network) may include one or more hotspot features. For hotspot inter-working, the security features of hotspot networks may enable these networks to be considered as trusted non-3GPP access networks. Hotspot networks may be able to interwork with 3GPP networks for trusted non-3GPP access.

[0079] The Wi-Fi network may be a trusted network. Untrusted WiFi access (e.g., IPsec tunnels and SSO) may be provided. The network may be hotspot enabled. The hotspot Wi-Fi network may offer an online sign-up and hotspot architecture, e.g., with an AAA server, on-line sign-up (OSU) server, etc. and may include an advertisement server (for example, an ANQP server). The hotspot network may support related provisioning (e.g., subscription provision and management, the policy provisioning that depends on the credential that the mobile device has, etc.), for example username/password, certificate, SIM, etc. The hotspot network may support a logical entity such as an advertisement server. An advertisement server may communicate over-the-air information to a WTRU using a generic advertisement server (GAS).

[0080] An access network discovery and selection function (ANDSF) may be part of the mobile operator's network. It may be a standalone policy function providing WTRU policies on how to discover and/or use various non-3GPP access networks in conjunction with 3GPP access networks. It may be connected with the various functions of the policy and charging control (PCC) subsystem, and, may coordinate policies that may control various network elements (e.g., via the PCC) and the WTRU (e.g., via the ANDSF). An ANDSF MO may be used by the ANDSF and the WTRU, e.g., according to 3GPP specifications.

[0081] FIG. 3 shows an example of an access network discovery and selection function (ANDSF) management object (MO). The ANDSF MO may include inter-system mobility policy (ISMP) (which may be referred to as "Policy"), which may provide prioritized access networks. The ANDSF MO may include inter-system routing policy (ISRP), which may indicate how to distribute traffic among available accesses when the WTRU is capable of connecting through multiple accesses for one or more of IFOM, MAPCON, non-seamless WLAN offload, etc. The

ANDSF MO may include access network discovery information, e.g., available networks in the WTRU's vicinity. The ANDSF MO may provide these based on the WTRU location, which the ANDSF may be able to read from the ANDSF MO.

[0082] Hotspot implementations may include one or more of discovery, registration, and access. For discovery, the mobile device may scan for networks with which to associate and for related information for network selection. The mobile device may not be associated with the Wi-Fi access networks that the mobile device is scanning. The mobile device may use operator policy and user preferences in the network selection process. Development may include registration, whereby the mobile device may be in the process of setting up a new account with a SP or hotspot provider. If the mobile device already has valid credentials for a given Wi-Fi access network, registration may not need to be performed. For provisioning, the Wi-Fi infrastructure may establish credential information. The Wi-Fi infrastructure may provide policy information to the mobile device. For hotspot implementation, policy may refer to Wi-Fi access network selection policy. If the mobile device already has valid credentials for a given Wi-Fi access network, provisioning may not be performed. For access, the mobile device may associate and authenticate with the Wi-Fi access network and may access services, e.g., for which the user has subscribed.

[0083] Hotspot network selection and discovery may be described herein. IEEE 802.11u may provide for the discovery of networks through the advertisement of access network type [e.g., private network, free public network, for-fee public network], roaming consortium, and/or venue information. For example, one or more of the following may apply. A generic advertisement service (GAS) may be used. IEEE 802.11u may provide a Layer 2 transport of an advertisement protocol's frames between a mobile device and a server in the network prior to authentication, e.g., to provide the availability of information related to the network services, for example, information about local services available. GAS may use a generic container to advertise network services information over 802.11. Network selection and discovery may include access network query protocol (ANQP), which may be a query and response protocol used by a mobile device to discover a range of information, including one or more of: a hotspot operator's domain name (e.g., a globally unique, machine searchable data element); roaming partners accessible via the hotspot along with their credential type and EAP method supported for authentication; IP address type availability (for example, IPv4 or IPv6); or other metadata useful in a mobile device's network selection process. Hotspots may support a customized ANQP, e.g., based on IEEE 802.11u ANQP elements and additional elements introduced by hotspot evolution. One or more of the following IEEE 802.11u ANQP elements may be

supported (e.g., as defined in IEEE 802.11u): venue name information; network authentication type information; roaming consortium list; IP address type availability information; NAI realm list; domain name list; or 3GPP cellular network information,.

[0084] 3GPP cellular network information may include cellular information such as network advertisement information, for example, network codes and country codes, e.g., to assist a 3GPP non-AP STA in selecting an AP to access 3GPP networks. FIG. 4 shows an example format for 3GPP cellular network information. The Info ID field may be equal to 264 (e.g., according to the ANQP information ID). The Length field may be a 2-octet field and may be equal to the length of the Payload field. The Payload field may be a generic container. FIG. 5 shows an example structure for a generic container. As shown in FIG. 5, GUD may be generic container user data, UDHL may be user data header length, and IEI may be an information element identity, which may comprise a PLMN list (e.g., MCC/MNC Code).

[0085] ANQP elements may be added, for example one or more of the following: a hotspot operator friendly name; hotspot WAN metrics; hotspot connection capability; NAI home realm query; hotspot online sign-up providers list; or anonymous NAI. QoS map distribution may be used. This may provide a mapping between the IP's differentiated services code point (DSCP) to over-the-air Layer 2 priority on a per-device basis, which may facilitate end-to-end QoS.

[0086] The information required to select a network and authenticate to it may be delivered by ANQP (e.g., using a number of formats). For example, a management object may be used with ANQP.

[0087] FIG. 6 shows an example of hotspot network selection, e.g., for a mobile device. The exemplary hotspot network selection may be performed by a WTRU, and, may be illustrated for example with reference to a hotspot Wi-Fi connection manager (CM). The CM may be an entity within the mobile phone that may control one or more of the following: which modems (e.g., 3G and WiFi) modems are used for particular communications, which IP addresses are "bound" to which modems, which data is sent where, etc. The CM may be an entity that implements policies, e.g., ANDSF policies.

[0088] The CM may initiate a network selection process, e.g., with an active or passive scan for Wi-Fi access networks. The CM may compare discovered networks (e.g., a list of discovered networks) with a list of user-preferred networks (e.g., previously configured by the user on the WTRU). The CM may cause the mobile device to associate with the Wi-Fi access network having a highest user preference (e.g., if a match is found). If no user-preferred network is found, the listed discovered networks, e.g., from 1, may be filtered for hotspot networks (for

example, non-hotspot networks may be deleted from the list). For hotspot networks not having a cached profile, ANQP queries may be performed, e.g., as needed, which may include NAI realm list and/or 3GPP cellular information. The query protocol for access network information retrieval may be transported by generic advertisement service (GAS) public action frames. ANQP may support information retrieval from an advertisement server. ANQP may be a L2 protocol between a WTRU and a server. ANQP may be a query and response protocol used by a WTRU to discover information, which may include a hotspot operator's domain name, roaming partners accessible via the hotspot along with their credential type and EAP supported for authenticating IP address type availability (for example, IPv4 or IPv6). If a handover is performed from a hotspot to 3GPP network, in a location in which the 3GPP network wants to be the preferred network, the ANQP information related to the 3GPP cellular network may be set accordingly.

[0089] Still referring to FIG. 6, the discovered network list may be filtered based on implementation dependent criteria, e.g., minimum RSSI level, protocols/ports blocked by hotspot firewall, PLMNs, and the like. This may include adding criteria such as IFOM preferences, application preferred network, and the like. The discovered network list may be filtered for realms matching the user's credentials. Wi-Fi access networks whose NAI realm list or 3GPP cellular information do not match user credentials, which may include credential types, may be filtered. If the user has more than one Wi-Fi subscription, the remaining Wi-Fi access networks in the list may be sorted by subscription preference, e.g., that the user has previously configured. The Wi-Fi access networks in the list may go through a 2nd-level sort (for example, a nested sort) in which the networks may be ordered by subscription preference and/or by operator preference. The sorted list may be filtered for blacklisted networks. If the filtered and sorted list of networks has one or more remaining networks, the following may be performed. The CM may cause the WTRU to associate to the first entry (e.g., highest sorted network) in the list. The CM may request the user to decide whether to associate with a Wi-Fi access network. An OSU Server serversubscriptionmobile device may confirm that the OSU Server owns the fully qualified domain name (FQDN) stated in the URI. The mobile device may use an identity and/or handshaking protocol to initiate the sign-up. The mobile device may analyze information carried by ANQP such as, for example, an OMA DM MO. If a policy exists, the mobile device may initiate downloading of the policy using the protocol as specified.

[0090] Hotspot security architecture may be disclosed herein. IETF's extensible authentication protocol (EAP) may be used for an authentication framework at the link layer. There may be three entities in the framework: supplicant (client), authenticator (access point),

and authentication server (AAA server). FIG. 7 shows an example of an IEEE 802.xx/extensible authentication protocol (EAP) protocol stack.

[0091] The authenticator (AP) may transfer EAP messages, which may be EAPOL-encapsulated on the wireless side and RADIUS-encapsulated on the wired side, e.g., between the supplicant and the server. The client may be allowed network access and traffic may be sent over the radio link in an encrypted form, e.g., as a result of successful authentication. EAP authentication may enhance WLAN security by providing mutual authentication between client and network, secure transfer of authentication credentials, and/or generation of keying material for session encryption keys.

[0092] There may be one or more EAP authentication methods used in Wi-Fi networks. Hotspot protocols may mandate supporting one or more of the following: EAP-TLS, EAP-TTLS, EAP-SIM, or EAP-AKA. EAP-AKA' may be included in the list of hotspot-supported EAPs. 3GPP operators may use EAP-SIM/AKA/AKA' for WiFi Hotspot access, e.g., this may enable 3GPP operators to leverage their existing authentication infrastructure that is xSIM based (e.g., SIM for GSM, USIM for UMTS/LTE, and ISIM for IMS).

[0093] FIG. 8 shows an example call-flow for EAP-SIM/AKA-based public hotspot access. An example may comprise one or more of the following. An authenticator (e.g., AP) may issue an EAP Request asking for WTRU Identity. The WTRU may return an international mobile subscriber identity (e.g., IMSI with its realm), for example, '0'(ASCII 0x30) or '1' (ASCII 0x31) may be pre-pending to the IMSI. '0' may be used to indicate EAP-AKA and '1' may be used for EAP-SIM authentication. The AP may send EAP ID to AAA server using access request. The AAA server may request authentication vector(s) from HLR/HSS. The AAA server may use a MAP interface towards the HLR or Diameter interface to the HSS. The AAA server may send an EAP-request/challenge message. The AP may receive from the AAA server a challenge and a message authentication code (MAC) and may send it to the WTRU, e.g., using EAP-request message. The WTRU may compute its MAC value and compare it with the received MAC value. If the MAC values do not match, the WTRU may silently discard the EAP packet. If the MAC values do match, the WTRU may send the challenge to the UICC, which may run a SIM/AKA authentication algorithm to generate the SRES. The WTRU may return an SRES in EAP-Response to the AP. The AP may forward an EAP-response in a RADIUS message to the AAA server. If the checks are successful, the AAA Server may send an access accept message, which may include an EAP success and the key material, to the AP. The key material may include the MSK generated during the authentication process. The EAP success

message may be forwarded to the WTRU. The WTRU status may become authorized on the AP. The WTRU may obtain an IP address using DHCP and may access the Internet.

[0094] Hotspot evolution may require hotspot access points to support one or more of the following: WPA2 (EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS), IEEE 802.11u, or 802.11v. Legacy hotspot APs that do not support these features may not be capable of being used and may need to be replaced with compliant APs. FIG. 9 shows an example of WiFi-3GPP integration using EAP-SIM. Hotspot technology may require a hotspot AAA server to support EAP-SIM/AKA. This may require an IP-based AAA server to support a SS7/Diameter interface towards MNO HLR/HSS, e.g., as shown in FIG. 9.

[0095] Some hotspot AAA servers may not support such an interface. Such hotspot AAA servers may need to be replaced or additional gateways, such as MAP proxy GWs, may be needed, e.g., to mediate the communication between a hotspot AAA server and MNO HLR/HSS. By allowing access to an MNO subscriber master database (e.g., HSS/HLR) for many hotspots, vulnerabilities to the MNO networks may be introduced and different types of attacks may be launched (for example, DoS or DDoS attacks on the HSS/HLR, MNO AAA servers, etc.).

[0096] Hotspot deployment may require additional network elements to be deployed into the hotspot, e.g., to support network discovery (for example, ANQP servers), online registration and/or sign-up servers.

[0097] Hotspot deployments may require changing hotspot architecture to mimic enterprise-WiFi architecture, e.g., in order to be able to use 802.1X/EAP-based WiFi access. Existing hotspot deployments may not be compatible with the enterprise-WiFi architecture and may not support EAP. Such legacy deployments may not be capable of being leveraged, e.g., there may not be a smooth migration path from legacy hotspots towards evolved hotspots. A cost may be incurred as a result of deploying compliant equipment.

[0098] HS 2.0 may create performance issues, e.g., as a result of network discovery, registration, association, and/or authentication implementations. Poor end user experience for real time applications (for example, VoIP) may occur. Cellular-WiFi handoff may become non-seamless to the end user. Access to UICC functionality (for example, for PIN entry) as part of the EAP-SIM/AKA procedure may result in “locking” user SIM card, e.g., as a result of multiple failed attempts.

[0099] AAA-proxy based secure WiFi-cellular integration may be used. FIG. 10 shows an example of AAA proxy-based hotspot-3GPP interworking. Use of a AAA-proxy may have one or more of the following: in the case of no roaming relationship between the Wi-Fi network and the home network holding SIM/USIM credentials, the AAA proxy may not work; setting up

a hotspot AAA server as a proxy towards MNO AAA server may require provisioning and configuration parameters on both networks (for example, shared secret, IP addresses, ports, realms, etc.); interfacing hotspot AAA proxy with a pre-Release 8 MNO AAA server may require a RADIUS-RADIUS interworking function to align RADIUS attributes between the two networks; or interfacing a hotspot AAA proxy with post-Release 8 MNO AAA server may require a RADIUS-Diameter interworking function to convert RADIUS attributes to Diameter attributes between the two networks.

[0100] FIG. 11 shows an example of single sign-on (SSO)-based WiFi-cellular integration. The SSO-based WiFi-cellular integration shown in FIG. 11 may be aligned with the WFA hotspot program. The SSO based WiFi-cellular integration may leverage a previously established security association between a WTRU and a network (for example, the cellular network), e.g., to enable authentication and secure link setup on another network (for example, a WLAN network), for example, in an on-demand and seamless fashion. In the SSO-based WiFi-cellular integration, a reverse bootstrap of application-layer credentials on one network may be used to generate credentials used in a follow-on access-layer authentication procedure in another network. In the SSO-based WiFi-cellular integration, SSO protocols such as OpenID or GBA may be used, e.g., to enable the WTRU to discover and access previously unknown networks such as WLAN networks. There may be no need to pre-provision credentials at the follow-on network, e.g., since these may be bootstrapped from the already running application service security on the cellular network.

[0101] Implementations for SSO-based WLAN-cellular integration may be limited to needing a software upgrade to a hotspot or MNO AAA server to include SSO and enhanced ANDSF (eANDSF) server functionalities. The SSO-based WiFi-cellular integration may support APs including legacy UAM-based and 802.1x/EAP-based hotspots. The SSO-based WiFi-cellular integration may simplify provisioning for users entering the hotspot and support mobility between cellular and WiFi hotspots.

[0102] FIG. 12 shows an example of seamless mobility and IFOM with 3GPP and a hotspot, which may include interworking between 3GPP ANDSF and hotspot ANQP approaches. The WTRU may perform an initial connection procedure. The WTRU may be connected to a 3GPP network and may camp on a 3GPP cell. WiFi may be off, e.g., for battery saving. The IP traffic may go through the 3GPP network. The WTRU may be provisioned with one or more of the following. The WTRU may include a list of user preferred networks for WiFi (e.g., hotspot or private), which may have been previously configured by the user on the mobile device. The WTRU may include a PLMN selection input, stored in (U)SIM, which may include

a home PLMN (HPLMN) selector with access technology, a user-controlled PLMN selector with access technology (e.g., in priority order), and/or an operator-controlled PLMN selector with access technology (e.g., in priority order). The WTRU may include a pre-loaded ANDSF MO. This may include, for example, at least a list of prioritized access network (e.g., part of the Policy/ISMP sub-tree). The WTRU may include security related information, e.g., stored in a (U)SIM.

[0103] ANDSF and ANQP cooperation may be disclosed. There may be some coordination between an ANDSF server and ANQP. For example, an ANDSF MO may be expanded to include some ANQP related information. An interface between ANDSF and ANQP servers may be added.

[0104] The ANDSF server and ANQP server may know each other's information, e.g., via initial provisioning by the operators. The ANQP may aid the ANDSF server discovery through interaction with the domain name service function or the DHCP server function. ANDSF server discovery may be performed through an added DHCPv4 and DHCPv6 options code, which may be referred to as the ANDSF IP address options.

[0105] The following hotspot ANQP elements may be added to the ANDSF MO. The added hotspot ANQP elements may speed-up hotspot association (for example, as defined in IEEE 802.11u). These elements may bring hotspot knowledge to legacy APs. These elements may include one or more of the following: venue name information; network authentication type information; roaming consortium list; IP address type availability information; NAI realm list; 3GPP cellular network information; domain name list; hotspot operator friendly name; hotspot WAN metrics; hotspot connection capability; NAI home realm query; hotspot online sign-up providers list; or anonymous NAI. There may be an interface between an ANDSF server and a hotspot subscription server, e.g., to communicate such element(s).

[0106] FIG. 13 shows an example of an access network discovery information (ANDSF MO) sub-tree. An ANDSF MO update may be performed. The WTRU may want to update its internal access network discovery information (for example, ANDSF MO). Based on OMA DM, this may be initiated by the WTRU using OMA DM "Generic Alert" message (for example, pull model) or initiated by an ANDSF server (for example, push mechanism).

[0107] The WTRU may report (e.g., initially) back its location to the ANDSF server. This may help to receive location-based information. The WTRU may fill its internal ANDSF MO / location data with its current location (e.g., PLMN, Cell ID, registered PLMN (RPLMN), and the like). If geo location is available (for example, the WTRU has an embedded GPS), it may provide geo_location information. FIG. 14 shows an example of an ANDSF-MO-WTRU

location sub-tree. Location information may include, for example, the leaves identified as PLMN, TAC, LAC, GERAN_CI, UTRAN_CI, EUTRA_CI, AnchorLongitude, AnchorLatitude, and/or RPLMN.

[0108] In case of a WTRU-initiated update, the WTRU may initiate an OMA DM “Generic Alert”, with the “LocURI” element of the OMA DM generic alert message set to “urn:oma:mo:ext-3gpp-andsf:1.0:...:UE_Location.” The ANDSF server may perform a “get” on the ANDSF MO <X>/UE_Location/ to read the WTRU location. Based on the WTRU location, the ANDSF server may provide an update of a different sub-tree of the UE’s ANDSF MO. The policy (ISMP) part may provide a preferred access technology. If WiFi is setup as higher priority than 3GPP, the WTRU may keep searching for a WiFi network.

[0109] FIG. 15 shows an example of an ANDSF MO - policy (ISMP) information sub-tree. The discovery information may provide information on available access networks. The WTRU may use the information as an aid in discovering other access networks. The ANDSF server may provide a list of SSIDs of WLAN networks available around the WTRU. The WLAN networks may be identified by SSID_A, SSID_B and SSID_C, e.g., in the order of preference. Assuming that one or more of the previous has occurred, ANQP elements added to ANDSF may be received by the WTRU. The ISRP part may provide an indication on traffic distribution for WTRUs that are configured for IFOM, MAPCON, or non-seamless WLAN offload. The ANDSF server may fill the related part for the WTRU to perform IFOM. This may be shown in FIG. 16, which is an example of an ANDSF MO - ISRP sub-tree.

[0110] Hotspot WLAN connection may be performed. The WTRU may decide to check whether Wi-Fi is available, e.g., to switch over to Wi-Fi. This may be performed because, based on ISRP, the application is requested to be sent over Wi-Fi or because, based on policy (ISMP)/DiscoveryInformation, the WLAN has a higher priority than 3GPP. If Wi-Fi is turned on, and if the WLAN driver is hotspot capable, it may perform one or more of the following. Discovery may be performed, whereby the WTRU may perform discovery message exchange (for example, ANQP) to obtain network information, e.g., prior to association. ANQP (L2-HRP Query) may be skipped if ANQP elements have been received through ANDSF. Registration may be performed, whereby the mobile device may be in the process of setting up an account (e.g., new account) with a SP or hotspot provider. If the mobile device has valid credentials for a given Wi-Fi access network, registration may not be performed. If no pre-configured subscription information is available (for example, via a hotspot MO), the mobile device may check whether a SIM card is available and active. In this case, the mobile device may try to authenticate using SIM based authentication. Association and authentication may be performed.

[0111] IFOM may be performed. The IP flow that is running over 3GPP may be moved to WLAN.

[0112] Monitoring for a most preferred SSID may be performed. Assuming that the SSID that the WTRU is connected to is not the most preferred in the ANDSF MO (e.g., policy (ISMP) sub-tree), the WTRU may check (e.g., periodically) whether a more preferred SSID is available to handover to it.

[0113] FIG. 17 shows an example of seamless IFOM mobility from a hotspot to another hotspot. In the initial condition, the WTRU may be in an area where there is no 3GPP coverage. The WTRU may be connected to a mobile core network through a Wi-Fi hotspot network operated by a SP (Service Provider #1) (Home SP or roaming partner) and it may perform IFOM to a second Wi-Fi Hotspot network operated by SP#2.

[0114] The WTRU may be connected to a hotspot operated by SP#1 (e.g., HS2.0 #1). This connection may be an initial condition, e.g., from an initial connection procedure. The network selection procedure used may be the hotspot network selection as described above, e.g., when SP#1 is the home SP or a roaming partner. The information may be provided using OMA DM Management Objects, etc.

[0115] An ANDSF MO update may be performed as described herein. A Wi-Fi connection may be established with HS#2. For example, the WTRU may be connected to HS#1 and HS#1 is congested or SP#2, with a higher priority, has been detected. The WTRU may wish to perform IFOM from SP#1 to SP#2. Using one Wi-Fi card, a hotspot network selection may occur (e.g., scan / GAS / Association / Authentication) to SP#2, but the application connection may be disconnected. For IFOM, the WTRU may keep the application running over HS#1 and turn on Wi-Fi card #2. The network selection for Wi-Fi card #2 may not follow the hotspot network selection procedure as described above. If so, it may try to connect to HS#1 as Wi-Fi card 1 network selection. The Dual Wi-Fi cards and their network selection may need to consider the state of Wi-Fi card #1.

[0116] In some cases an ANDSF update, for example to get an ANDSF MO (e.g., new or updated), may be necessary when connecting to a hotspot (e.g., new hotspot). Access to this ANDSF MO may be through the hotspot, and, may not otherwise be accessible. In this case, the subscription information carried by ANQP may be used to provide the ANDSF MO. The hotspot may request the MO on behalf of the WTRU at connect time. The hotspot may run the ANDSF function itself, e.g., as a mirror of the master ANDSF function in the core network, and may be able to generate the MO upon request. The mirror function may have limited capabilities related to the hotspot and its geographical location, and, the resulting MOs may be

limited. For example, they may be limited to including some of the information that the master ANDSF would have been able to provide.

[0117] Information provided may be limited to the name and IP address of the ANDSF server. In this case, the hotspot may provide a limited IP-based address, e.g., to allow the WTRU to obtain the ANDSF MO from the ANDSF server. This may be implemented by the hotspot restricting access to the destination IP address of the ANDSF server; such access may be granted to a WTRU for a limited period of time after the initial access of the hotspot by the WTRU.

[0118] Still referring to Fig. 17, IFOM may be performed, e.g., as described herein. A most preferred SSID monitoring may be performed. Assuming that the SSID the WTRU is connected to is not the most preferred in the ANDSF MO (e.g., Policy (ISMP) sub-tree), the WTRU may check (e.g., regularly) whether a more preferred SSID is available, e.g., to eventually reconnect to it. This may be performed through WiFi card #2 passive scanning.

[0119] Interaction between application-specific policies (e.g., ANDSF) and eHotspot-specific context policies (e.g., ANQP) may be disclosed. This may illustrate the coordination between the application specific policies as defined in ANDSF and the hotspot policies as defined with ANQP. For example, a connection sharing client through Wi-Fi (e.g., "Wi-Fi tethering") may be used. Based on user profiles, ANDSF may not allow tethering, except if one or more of the following are met: tethering runs over Wi-Fi; or the HS policy (e.g., as advertised by ANQP) allows it. This example may illustrate how this is established, checked, and, when verified to be correct, tethering is established.

[0120] Wi-Fi tethering may mean that a user may share his mobile phone's 3GPP internet connection with external non-3GPP devices such as laptops over Wi-Fi. The mobile phone may act as a Wi-Fi relay. The laptop and the mobile phone may communicate over Wi-Fi and the mobile-phone may be connected to 3GPP network. FIG. 18 shows an example of a shared 3GPP internet connection (e.g., tethering) via Wi-Fi.

[0121] The mobile phone (e.g., the serving WTRU) may provide the tethering capability. This may be done, for example, in standalone (e.g., the serving WTRU may be seen as an hotspot device by the served WTRU and no other AP may be required) or through direct link setup (DLS), e.g., as defined by IEEE 802.11, where the AP may be involved for the setup. In the above, the serving WTRU may require an embedded tethering SW which may provide the Wi-Fi connection setup, then provide the data relay between the 3GPP connection and the Wi-Fi connection. 3GPP carriers may provide some "hotspot-capable smart phones," wherein the

embedded tethering SW may be provided and setup by the carriers, which may provide in parallel some specific tether data plan.

[0122] FIG. 19 shows exemplary connection sharing. The exemplary connection sharing may include one or more of the following: an initial condition, an ANDSF update, a (T)DLS setup, a hotspot enabled UE-link setup, or a served and/or serving UE data transmission. As an initial condition, the serving WTRU may have an IP connection through 3GPP. An ANDSF MO update may be performed. The serving WTRU may receive an ANDSF MO update, which may provide the WTRU with onnection sharing policies (e.g., new connection sharing policies). The WTRU may request an update when it receives a connection request over one of its radio access networks (e.g., wifi, Bluetooth, etc.).

[0123] FIG. 20 shows an exemplary enhanced ANDSF MO with elements added, e.g., to enable connection sharing. For an authorized WTRU, the non-3GPP served client may have been connected to some Wi-Fi hotspot in the vicinity of the serving WTRU. The served WTRU may have been lost (for example, loss of Wi-Fi coverage). The network may push the ID of this WTRU to other WTRUs, e.g., belonging to the same operators, for example so that the hotspot-enabled WTRUs may share their 3GPP connection with the out-of-coverage non-3GPP served WTRU. In this way, operators may launch the connection sharing client transparently to the serving user. In FIG. 20, the ConnectionSharing branch and related features may be added.

[0124] IEEE 802.11 specifies the direct link setup (DLS) protocol which may enable direct communication between a pair of stations within the same basic service set (BSS). This may eliminate anunnecessary triangular traffic route through an access point and may increase the overall effective throughput within the BSS. The setup may be performed with a 2-way handshake (e.g., DLS Setup Req / DLS Setup Resp) going through the AP. IEEE 802.11z provides an extension to DLS mechanisms that may allow IEEE 802.11 to set up a direct link between client devices while remaining associated with the access point (AP). Tunneled direct-link setup (TDLS) may be characterized by the use of signaling frames that are encapsulated in data frames so that the signaling frames may be transmitted through an AP transparently. A TDLS direct link may be set up (e.g., automatically), without need for user intervention, while the connection with the AP is maintained.

[0125] The direct client-to-client communication may provide one or more benefits. Potential benefits may include one or more of the following: IEEE 802.11z may reduce the number of times a packet gets transmitted over the air from 2 to 1; shorter transmission times on TDLS direct links may provide power savings; if client devices capable of operating at data rates or in frequency bands not supported by the access point, they may do so; TDLS direct links,

bypassing the access point, may eliminate one of the transmissions and the client-to-client transmissions may often occur at much higher data rates, both of which may result in shorter transmission times and client device power savings; there may be no need to upgrade APs to support TDLS direct links, as TDLS may be a client (e.g., client only) feature; or TDLS may be designed to enhance the communication between clients, e.g., mobile handheld devices, with limited battery capacity. The TDL setup may be performed with a 3-way handshake (e.g., DLS Setup Req / DLS Setup Resp / DLS Setup Confirm) going through the AP.

[0126] This may also include performing Wi-Fi connection setup with the served WTRU. On the serving WTRU, the WTRU may launch the connection sharing client. The serving WTRU may act as a legacy AP that may be seen as such by the served WTRU. The latter may perform a Wi-Fi legacy request to have an IP connection. The connection sharing client may consider ANDSF MO elements (e.g., new ANDSF MO elements) to accept or reject the connection. Network sharing may be performed. The serving WTRU may share the packet access with the served WTRU. The connection sharing client may consider the policies to share the data.

[0127] Neighbor discovery may be implemented via ANQP updates. This may improve network discovery by providing ANDSF with some ANQP related information. FIG. 21 shows an example of neighbor discovery via an ANQP update. WLAN passive scanning may be performed. The WTRU may or may not be connected to a network. The WTRU may periodically scan actively (e.g., if not already connected to a WLAN AP) or passively (e.g., if already connected) to determine whether there are available networks in the vicinity, and, may prioritize these in terms of signal strength. The WTRU may use existing ANDSF information to narrow down the list of SSIDs for which ANQP query is needed, e.g., in order to avoid a large number of potential ANQP queries. If no relevant ANDSF info is present, this may be skipped. If ANQP information for some SSIDs is present via enhanced ANDSF MO (e.g., as in some of the examples provided herein), ANQP queries of these networks may be avoided.

[0128] A lifetime may be associated to the ANQP neighbor information kept in the ANDSF server. This may be useful if the information changes at some point. This may prevent the information from being out-of-sync. The probability of having this information change on the ANQP server may be taken into account for setting the lifetime value (for example, very probable=short lifetime, very improbable=long lifetime). An expired lifetime may force the WTRU to query the ANQP server and update the ANDSF server with the latest information. If a WTRU is connected to a network, it may obtain information regarding neighbor congestion, QoS

supported, service available at the neighbor, and the like; this may be a non-ANQP exchange, e.g., since association may be assumed.

[0129] An ANQP query for a hotspot enabled AP may be performed. The WTRU may obtain information regarding congestion (e.g., QoS, Service availability, and the like) loading of networks through the ANQP query. This information may be combined with signal strength in prioritizing potential candidate networks for mobility. The ANQP MO for neighbors may be obtained as part of ANQP exchanged, which may include the enhanced congestion and other information described herein.

[0130] The mobile device may perform a discovery message exchange (for example, ANQP Procedures) to obtain network information, e.g., prior to association. The retrieved elements may include one or more of the following: venue name information; network authentication type information; roaming consortium list; IP address type availability information; NAI realm list; 3GPP cellular network information; domain name list; hotspot operator friendly name; hotspot WAN metrics; hotspot connection capability; NAI home realm query; hotspot online sign-up providers list; or anonymous NAI.

[0131] An ANDSF update (for example, hotspot capable WTRU to ANDSF server) may be performed. Assuming that the ANDSF MO is enhanced to include some ANQP elements, the WTRU may use an OMA DM mechanism (e.g., Generic Alert) to inform the network about its updated ANQP information it has stored in the ANDSF MO. An ANDSF update (for example, ANDSF server to non-hotspot capable WTRU) may be performed. An ANDSF update may be used to further downselect target networks; it may result in the need to repeat one or more of the implementations described herein. If a non-hotspot-capable WTRU requests an ANDSF MO update, the server may provide it with ANQP enhanced information. If a target network is selected, access may be attempted using the normal procedures.

[0132] ANQP and or WiFi HotSpot subscription server and ANDSF server content consistency may be resolved. A mechanism between ANQP/HS and ANDSF (e.g., such as a direct link through the WTRU's reporting) may need to be defined so that a coherent provisioning is done between both. The WTRU may include WiFi MO (e.g., associated with ANQP, GAS, or other discovery/subscription service in the WiFi network) and ANDSF MO and their respective content may be coherent or at least some priority between them may be established. An enhanced ANQP or GAS protocol may be used. As described herein, ANQP or GAS may provide, through Wi-Fi layer 2 connection, some limited 3GPP information. The protocol may be extended to expand the 3GPP information sent to the WTRU and may add information such as, for example, ANDSF server availability and IP address, or eventually some

ANDSF MO update over hotspot Layer 2. Media independent service discovery may also be performed. With IEEE 802.11u, service discovery may be enabled through 802.11 advertisement services, providing interchange of data between the STA (e.g., mobile) and the AP, without need for the STA to be associated. This may be extended to other technologies, e.g., service discovery may occur prior to association.

[0133] A wireless communications device, such as a UE, may enter (e.g., may be powered on in) an area in which an operator associated with the UE does not provide wireless network coverage (e.g., 3GPP RF coverage). The UE may not be provisioned with a list of one or more preferred Wireless Local Area Network (WLAN) networks available in the area. A UE may enter an area where established wireless network coverage does not support IP access (e.g., a GSM-only coverage area) and the UE may not be provisioned with a list of preferred WLAN networks available in this area.

[0134] The area, for example the area in either of the above scenarios, may have one or more established WLAN networks with which the operator associated with the UE may or may not have respective roaming agreements. A wireless communications network in the area may rely on an Access Network Discovery and Selection Function (ANDSF) to guide UEs entering the wireless communication system to respective WLAN networks. For example, the operator associated with the UE may prefer to guide UEs associated with the operator to a specific WLAN network via provisioning ANDSF policies.

[0135] In order to access ANDSF based provisioning, e.g., to obtain roaming policies and/or a list of preferred WLANs in the area, the UE may have to associate and/or authenticate with at least one WLAN network in the area. The UE may discover, after associating with the WLAN, that the WLAN is not in the preferred list and may subsequently perform one or more re-selection procedures. The user may undesirably be charged for such accesses and/or for user plane data, for example if a service provider of the at least one WLAN does not participate in a roaming agreement with the operator associated with the UE. A user of the UE may select a WLAN service provider that is not a preferred provider of the operator associated with the UE.

[0136] An interface may be established between an ANDSF and one or more Access Points (APs) and/or WLAN gateways. The ANDSF may be configured to provide respective ANDSF Management Objects (ANDSF MOs) to the one or more APs and/or WLAN gateways. The ANDSF MOs may be received at a UE and may guide the UE to one or more select WLAN networks that may be preferred WLAN networks of an operator associated with the UE.

[0137] An Access Network Discovery and Selection Function (ANDSF) may function as a framework for providing respective policies to one or more UEs and may be designed to

manage inter-RAT access selections and/or mobility of one or more UEs (e.g., on a per-flow basis). An ANDSF may be used, for example, in discovery of non-3GPP wireless communication systems, for example WiFi networks, WiMAX networks, etc.

[0138] ANDSF provisioning may include one or more of the following. A UE connected to a wireless network may have an IP address. The UE may contact an ANDSF. The UE may provide information about itself, such as an identity of the UE, a location of the UE, information pertaining to one or more types of policies (e.g., ISRP, ISMP, etc.) that may be requested by the UE, or the like. An ANDSF may respond with an ANDSF Management Object (ANDSF MO) that may be composed for the UE, for example specifically for the UE.

[0139] Access to ANDSF MO information may be enabled for one or more UEs that may not yet be connected to a cellular network with which the ANDSF is associated, for example one or more UEs that may not have an IP address and/or may not be able to use an S14 interface supported by the ANDSF. For example, ANDSF MO information may be made available to one or more Access Points (APs) (e.g., WLAN APs) and/or WLAN gateways. A WLAN gateway may, for example, include a service controller, a service router, or the like. The WLAN APs and/or gateways may pass the ANDSF MO information (e.g., information pertaining to an ability of one or more WLAN APs and/or gateways to provide UEs with respective ANDSF MOs) to one or more UEs, for example using access network query protocol (ANQP) and/or other suitable techniques (e.g., WLAN specific techniques).

[0140] An ANDSF MO may include information sufficient to enable one or more UEs to access a cellular network and/or an ANDSF located in the cellular network (e.g., via WLAN access available to the UE). An ANDSF MO may be limited to such information, for example connection related information such as that disclosed herein, etc. Once a UE has established a connection with an ANDSF, the UE may be provisioned, for instance via a full ANDSF MO. If a more desirable WLAN access network is available for use by the UE, the UE may be provisioned using the more desirable WLAN access.

[0141] An ANDSF MO may include information that is common to UEs associated with a select operator, for instance in accordance with a location of a UE and/or a time. For example, an ANDSF MO may include information pertaining to a location of a respective ANDSF and/or information pertaining to one or more WLAN networks that are associated with a select operator in the location (e.g., a list of WLAN networks). A WLAN network may be provisioned with a common ANDSF MO that may reflect a location, but may not reflect UE-specific information.

[0142] Respective interfaces may be established between an ANDSF and one or more APs and/or WLAN gateways. For example, FIG. 22 depicts an example cellular network with

respective S14a interfaces established between an ANDSF and a pair of APs and/or WLAN gateways. The respective interfaces, such as the S14a interfaces, may be configured to function similarly to an S14 interface established between an ANDSF and a UE, for example in a 3GPP access network. Respective interfaces between an ANDSF and one or more APs and/or WLAN gateways may be established, for example, when a corresponding cellular network becomes active and may be maintained as long as the cellular network remains active. An interface between an ANDSF and an AP and/or WLAN gateway (e.g., an S14a interface) may be configured in accordance with characteristics of an internal 3GPP interface, such that the AP and/or WLAN gateway may be a trusted entity for the purposes of establishing the S14a interface.

[0143] An AP and/or WLAN gateway may be pre-provisioned with a location of a corresponding ANDSF (e.g., an IP address of the ANDSF, a Fully Qualified Domain Name (FQDN) of the ANDSF, or the like), or the AP and/or WLAN gateway may otherwise obtain information pertaining to the location of the corresponding ANDSF, for example dynamically in accordance with discovery procedures that may be used by a UE to discover an ANDSF location.

[0144] An AP and/or WLAN gateway may request a "location-default" ANDSF MO from a corresponding ANDSF. The location-default ANDSF MO may include location information sufficient to allow a UE to access the ANDSF, for example using resources of the AP and/or WLAN gateway. The ANDSF MO request may include a network identity of the AP and/or WLAN gateway, location information pertaining to the AP and/or WLAN gateway, and/or other suitable information. The location-default ANDSF MO may be location specific to one or more WLAN networks associated with a core network in which a corresponding ANDSF is located.

[0145] The AP and/or WLAN gateway may request the location-default ANDSF MO during establishment of an S14a interface and/or at a later time. The ANDSF may respond to the request by providing an ANDSF MO that may be shared with UEs associated with the corresponding cellular network. The ANDSF MO may include a list of WLAN networks that may be used by a UE to access the UE operator's network in a location. Contents of the location-default ANDSF MO may differ, for example depending on whether a WLAN network has a trusted communication link to the operator's core network (e.g., to a SGW located in the operator's core network) and/or whether the WLAN network is an untrusted network that may have no direct communication link to the operator's core network, for example such that a UE may establish a trusted connection to an evolved packet data gateway (ePDG) associated with the operator. The location-default ANDSF MO may include parameters such as an ePDG address,

internet protocol security (IPsec) configuration parameters, etc. These parameters and/or a type of relationship between the WLAN network and the ANDSF operator may be advertised by the WLAN network.

[0146] If an AP and/or WLAN gateway belongs to one or more WLAN networks having multiple roaming agreements, there may be one or more ANDSF instances serving different operators, respectively. In such a scenario, an AP and/or WLAN gateway may perform multiple ANDSF MO requests, for example one ANDSF MO request directed to each operator, so as to cache a location default ANDSF MO for each operator. When the AP and/or WLAN gateway receives an ANDSF MO request from a UE, the AP and/or WLAN gateway may provide a location default ANDSF MO response that corresponds to an operator of the UE, for example based on an operator ID and/or a public land mobile network (PLMN) identifier received from the UE.

[0147] A WLAN network (e.g., including one or more APs and/or WLAN gateways) may request provisioning from an ANDSF responsive to a UE request for ANDSF provisioning (e.g., an ANDSF MO request). The WLAN network may be pre-provisioned, for example before UE requests for ANDSF provisioning are received and/or accepted.

[0148] A protocol may be established for requesting and/or receiving location-specific ANDSF MOs by a WLAN network. The protocol may be implemented with a pull model for provisioning that may operate similarly to a pull model for provisioning a UE with ANDSF, for example, with the WLAN network acting in the role of the UE. Other suitable IP-based protocols may be used for requesting and/or receiving location-specific ANDSF MOs, such as media independent handover (MIH), hypertext transfer protocol (HTTP), constrained application protocol (CoAP), dynamic host configuration protocol (DHCP), Diameter, etc.

[0149] An ANDSF may periodically push updated location-default ANDSF MOs to respective WLAN networks, for example over one or more corresponding S14a interfaces. For interaction with a UE, transport mechanisms such as SMS may be used for transport in a push model. For interactions with a WLAN network, transport mechanisms such as extensible messaging and presence protocol (XMPP), CoAP, and/or any other suitable transport mechanism, may be used, for example to push one or more updated location-default ANDSF MOs to respective WLAN networks.

[0150] When provisioned with one or more location-default ANDSF MOs, a WLAN network may advertise that discovery information for one or more operators is available at the WLAN network. Discovery may be performed, for example, by advertising an operator's PLMN identity and/or other suitable identifier that may be recognized by a UE. For example,

advertising information may be included in a beacon and/or may be a part of a response to a query (e.g., an ANQP query).

[0151] A UE that is configured to request ANDSF provisioning from an operator may follow one or more of the following. The UE may discover that the WLAN network may be used to provision the UE with at least some ANDSF information. The UE may request ANDSF provisioning from the WLAN network. Upon being provisioned with a location-default ANDSF MO, the UE may use information in the location-default MO to select an access network and/or to sign-in to the operator's network. Once the UE is signed-in to the operator's network, it may establish a connection with ANDSF, e.g., over an S14 interface, and may request an additional ANDSF MO, such as a full ANDSF MO. Upon being re-provisioned, the UE may select a different access network or may remain on the originally chosen access network, for example depending upon a policy included in the full ANDSF MO.

[0152] Although features and elements are described above in particular combinations, one of ordinary skill in the art will appreciate that each feature or element may be used alone or in any combination with the other features and elements. In addition, the methods described herein may be implemented in a computer program, software, or firmware incorporated in a computer-readable medium for execution by a computer or processor. Examples of computer-readable media include electronic signals (transmitted over wired or wireless connections) and 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 internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs). A processor in association with software may be used to implement a radio frequency transceiver for use in a WTRU, WTRU, terminal, base station, RNC, or any host computer. Features and/or elements described herein in accordance with one or more example embodiments may be used in combination with features and/or elements described herein in accordance with one or more other example embodiments.

CLAIMS

What is claimed:

1. A method for network access, the method comprising:
receiving, from a first user equipment (UE), information relating to a wireless local area network (WLAN), wherein the information comprises an access network query protocol (ANQP) element associated with the WLAN;
updating an access network discovery and selection function (ANDSF) management object (MO) based on the received information; and
sending the updated ANDSF MO to at least one of a second UE or an access point.
2. The method of claim 1, wherein the updated ANDSF MO is a generic ANDSF MO.
3. The method of claim 2, wherein the generic ANDSF MO is capable of being used by a plurality of UEs associated with a network.
4. The method of claim 2, wherein the generic ANDSF MO does not include UE-specific information.
5. The method of claim 2, wherein the generic ANDSF MO comprises a prioritized list of WLAN networks.
6. The method of claim 1, wherein the second UE is a legacy UE.
7. The method of claim 6, further comprising receiving a request from the second UE for an ANDSF MO.
8. The method of claim 1, wherein the WLAN is a wi-fi network.
9. A network entity, comprising:
a processor configured to:
receive, from a first user equipment (UE), information relating to a wireless local area network (WLAN), wherein the information comprises an access network query protocol (ANQP) element associated with the WLAN;

update an access network discovery and selection function (ANDSF) management object (MO) based on the received information; and
send the updated ANDSF MO to at least one of a second UE or an access point.

10. The network entity of claim 9, wherein the updated ANDSF MO is a generic ANDSF MO.

11. The network entity of claim 10, wherein the generic ANDSF MO is capable of being used by a plurality of UEs associated with a network.

12. The network entity of claim 10, wherein the generic ANDSF MO does not include UE-specific information.

13. The network entity of claim 10, wherein the generic ANDSF MO comprises a prioritized list of WLAN networks.

14. The network entity of claim 9, wherein the second UE is a legacy UE.

15. The network entity of claim 14, wherein the processor is further configured to receive a request from the second UE for an ANDSF MO.

16. The network entity of claim 9, wherein the WLAN is a wi-fi network.

1/23

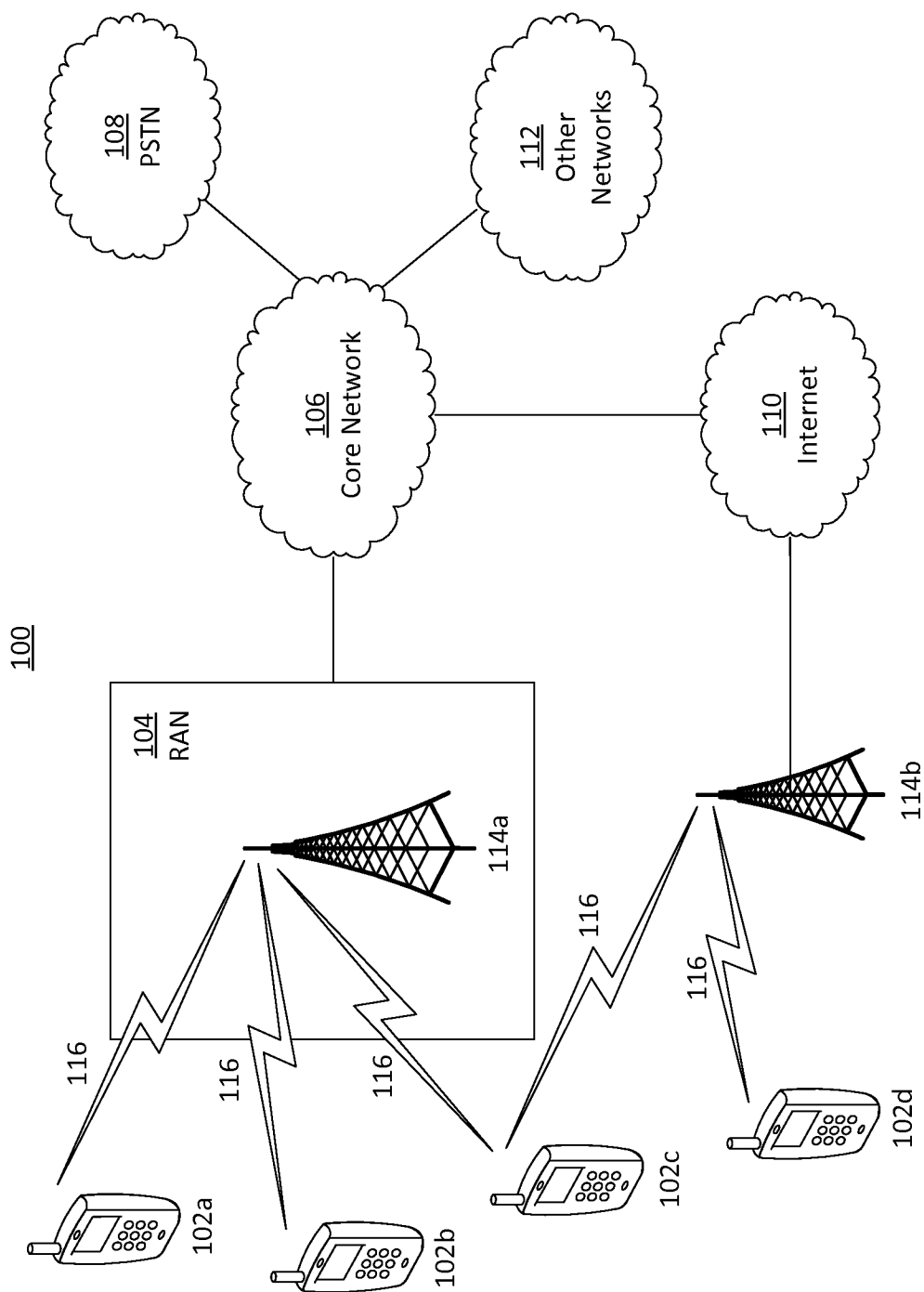


FIG. 1A

2/23

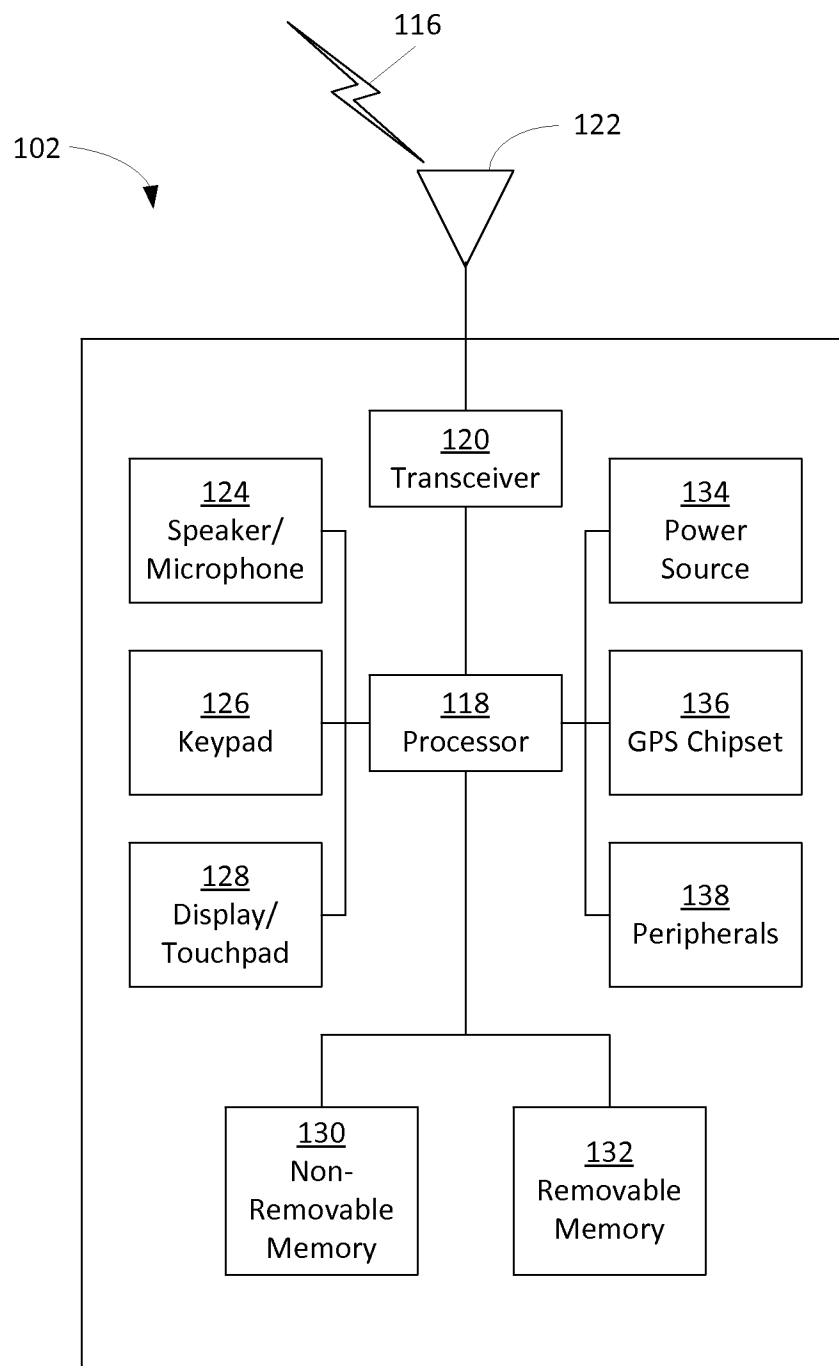


FIG. 1B

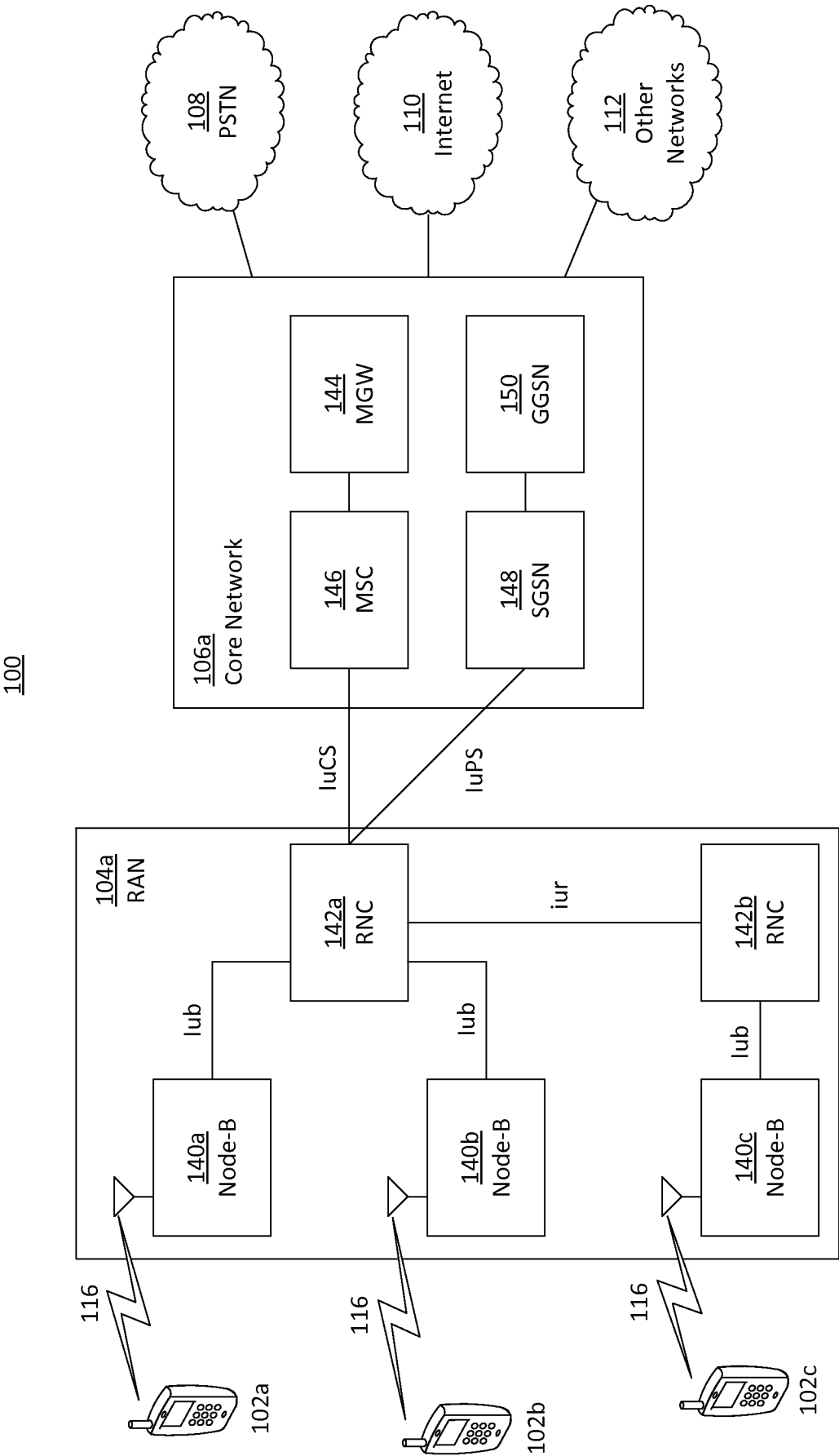


FIG. 1C

4/23

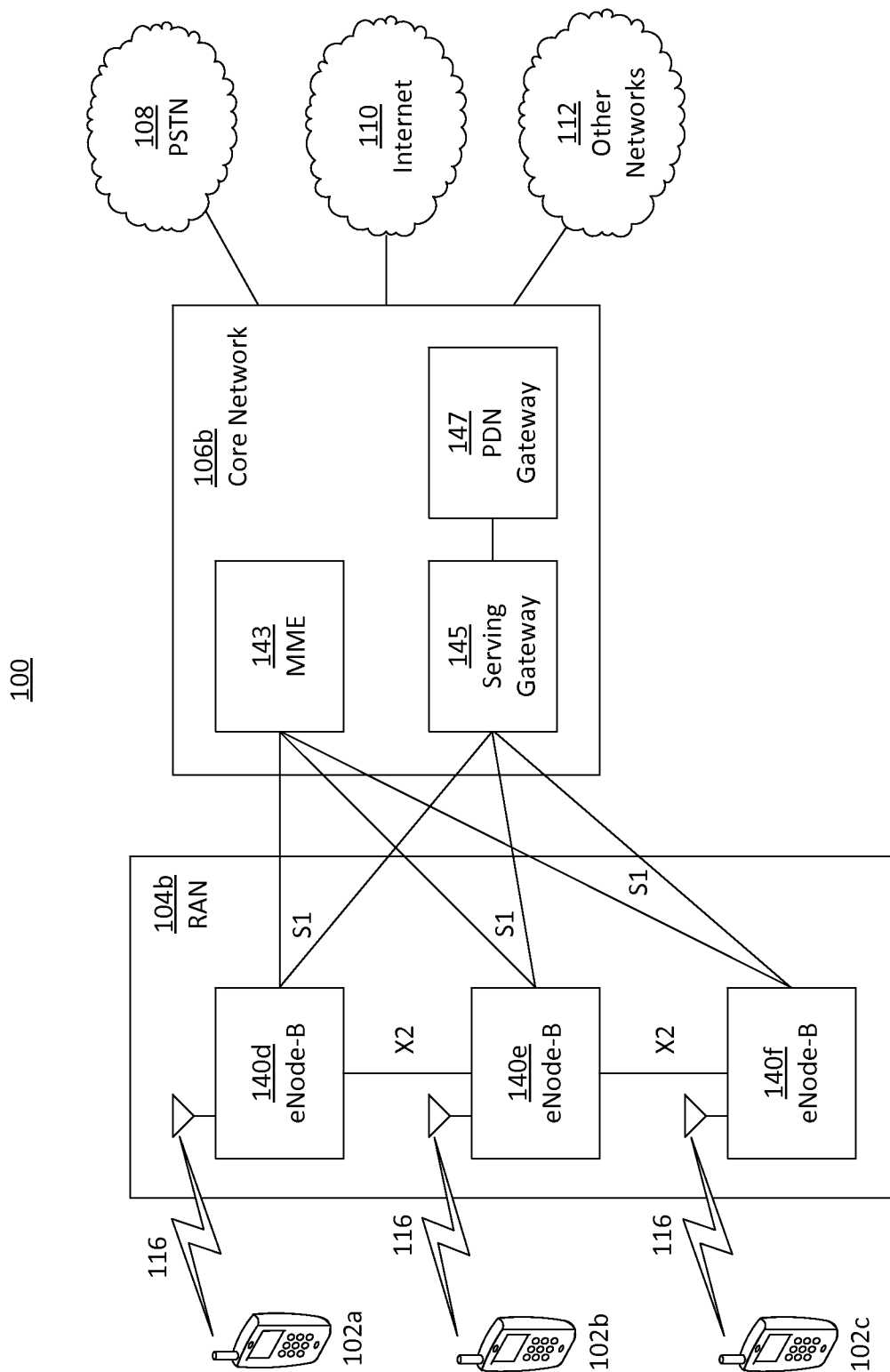


FIG. 1D

5/23

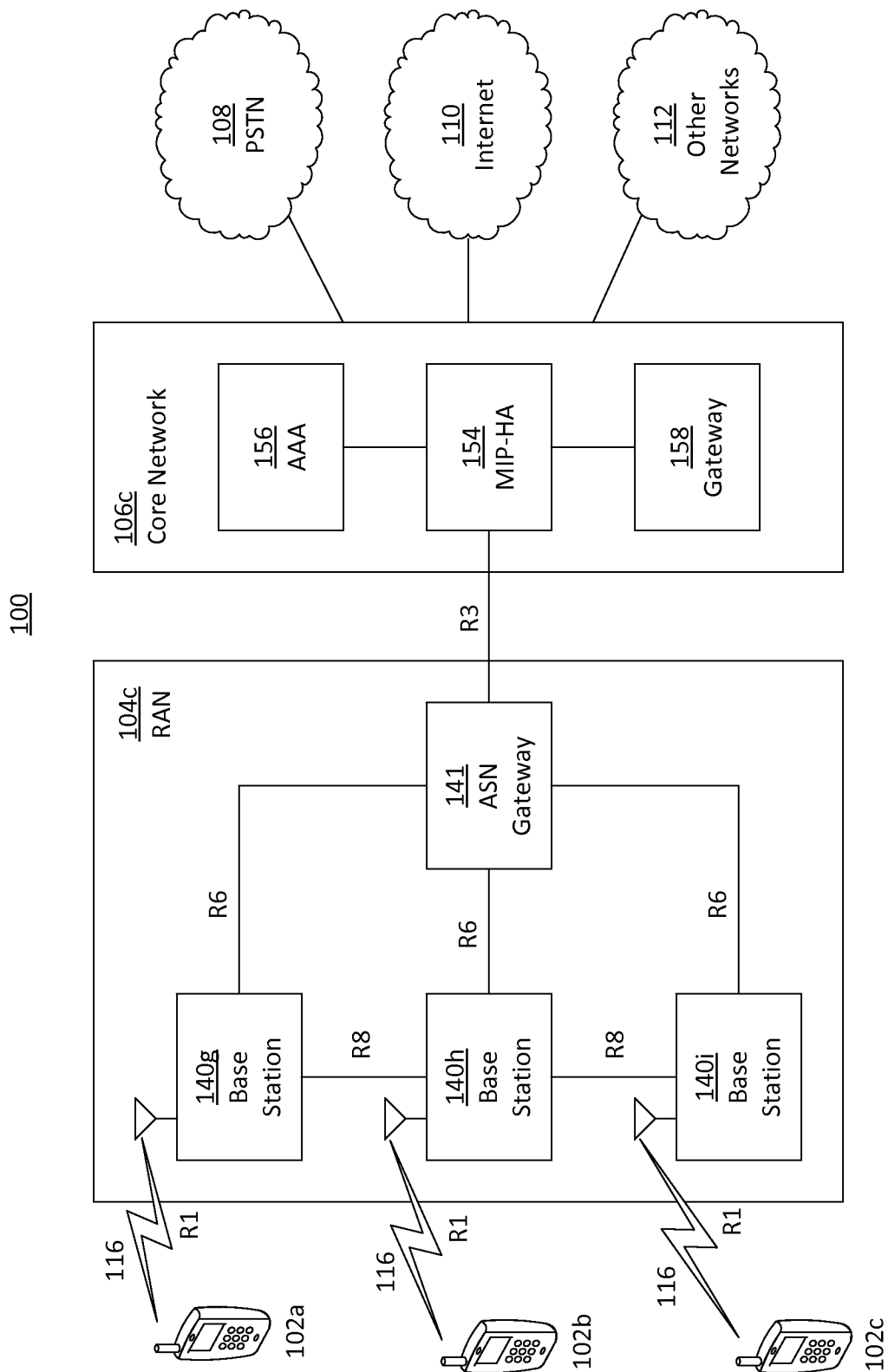


FIG. 1E

6/23

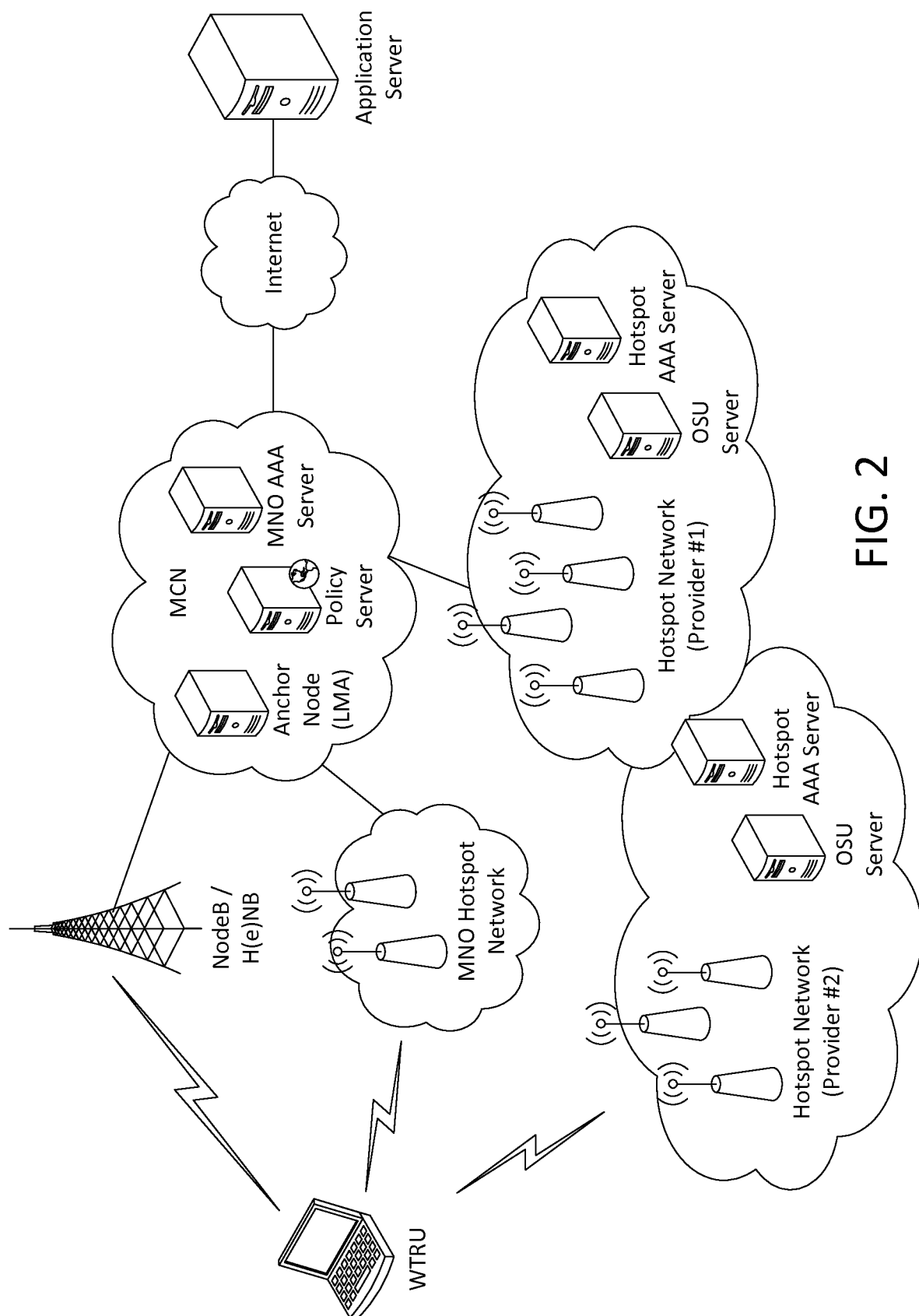


FIG. 2

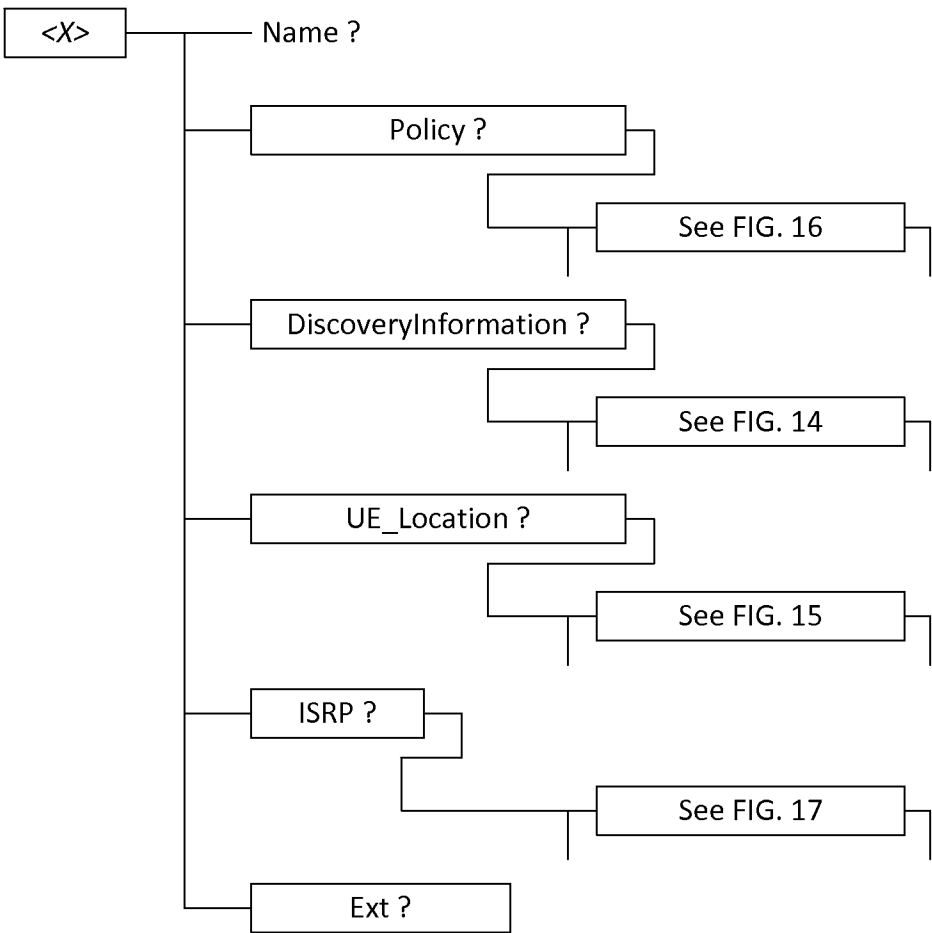


FIG. 3

	Info ID	Length	Payload
Octets:	2	2	variable

FIG. 4

GUD	UDHL	IEI1		IEIn
-----	------	------	--	------

FIG. 5

8/23

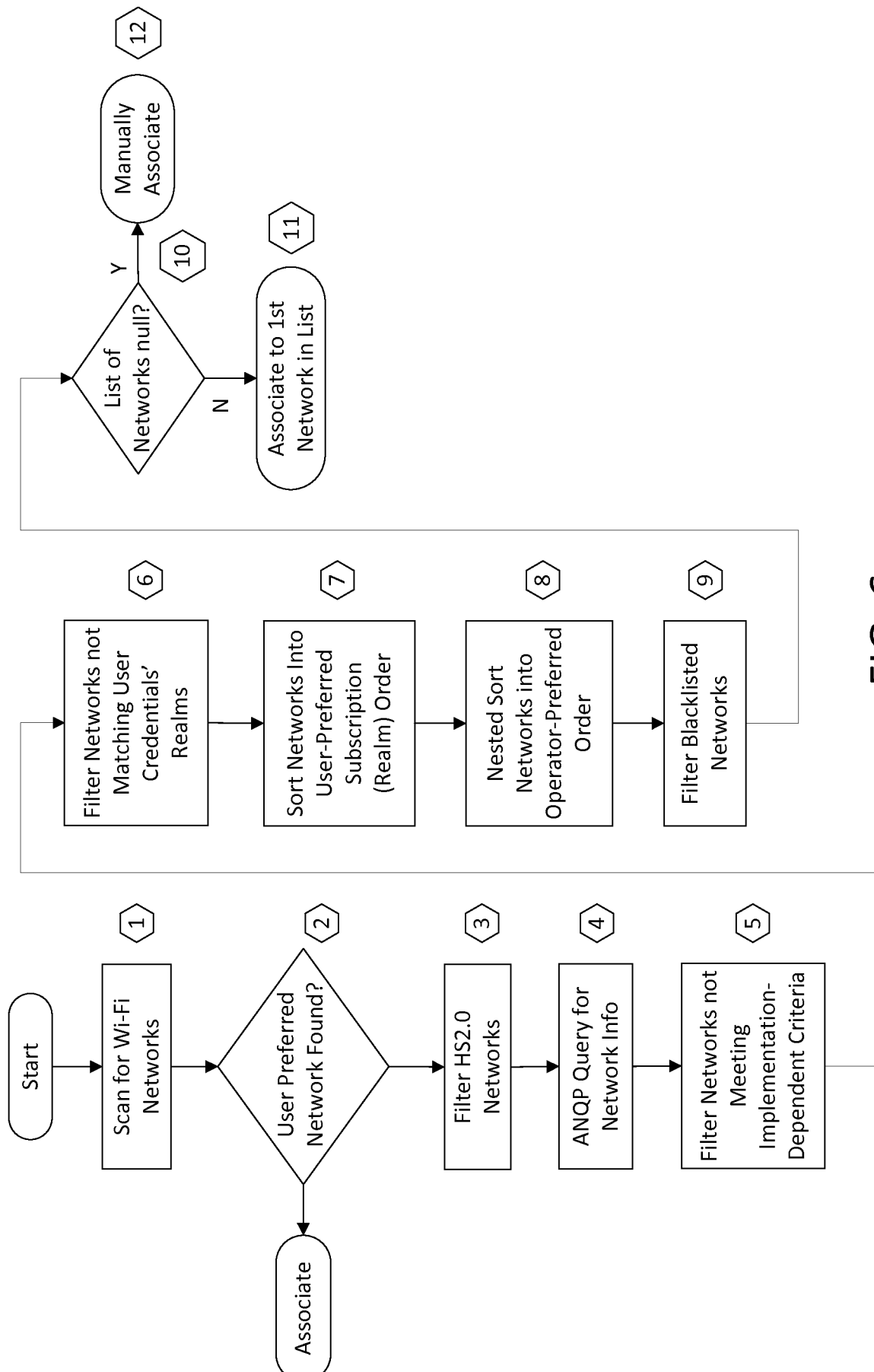


FIG. 6

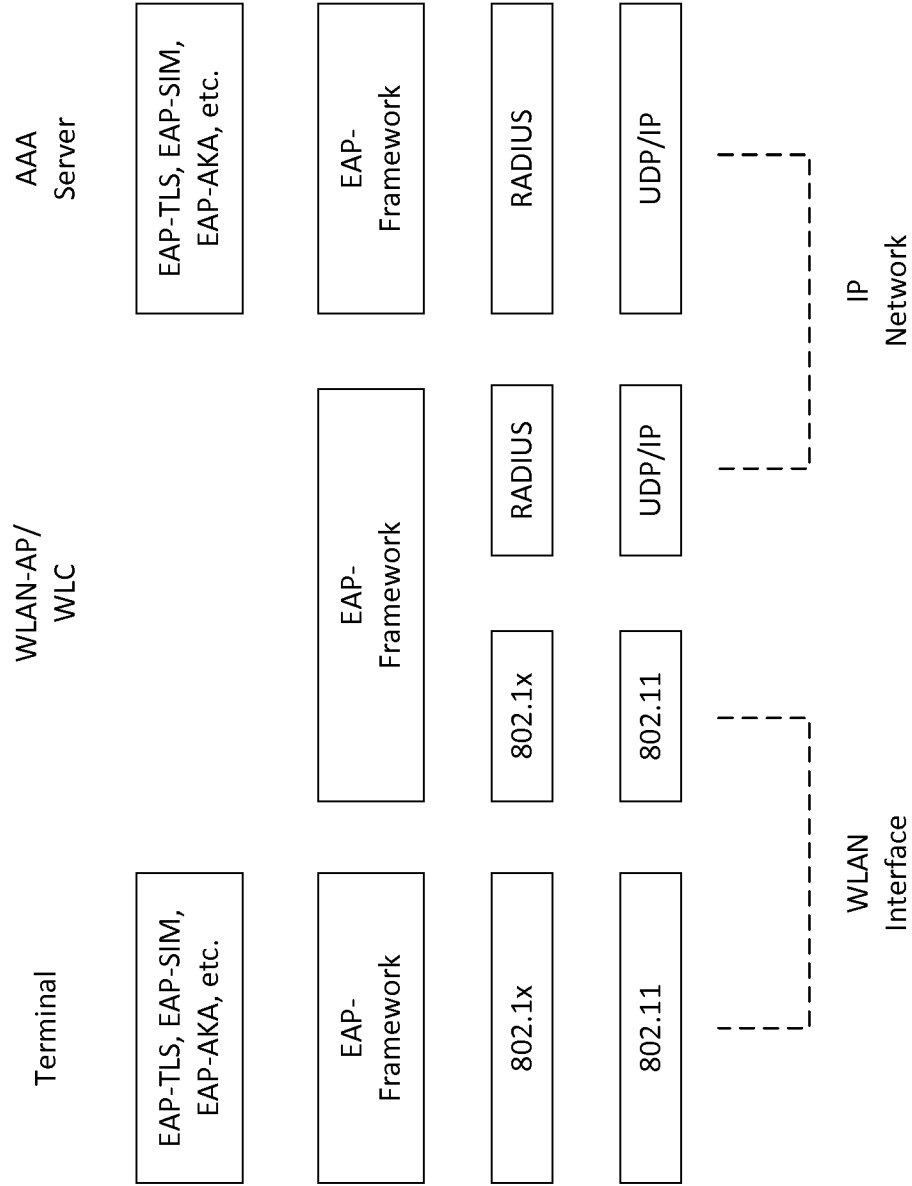


FIG. 7

10/23

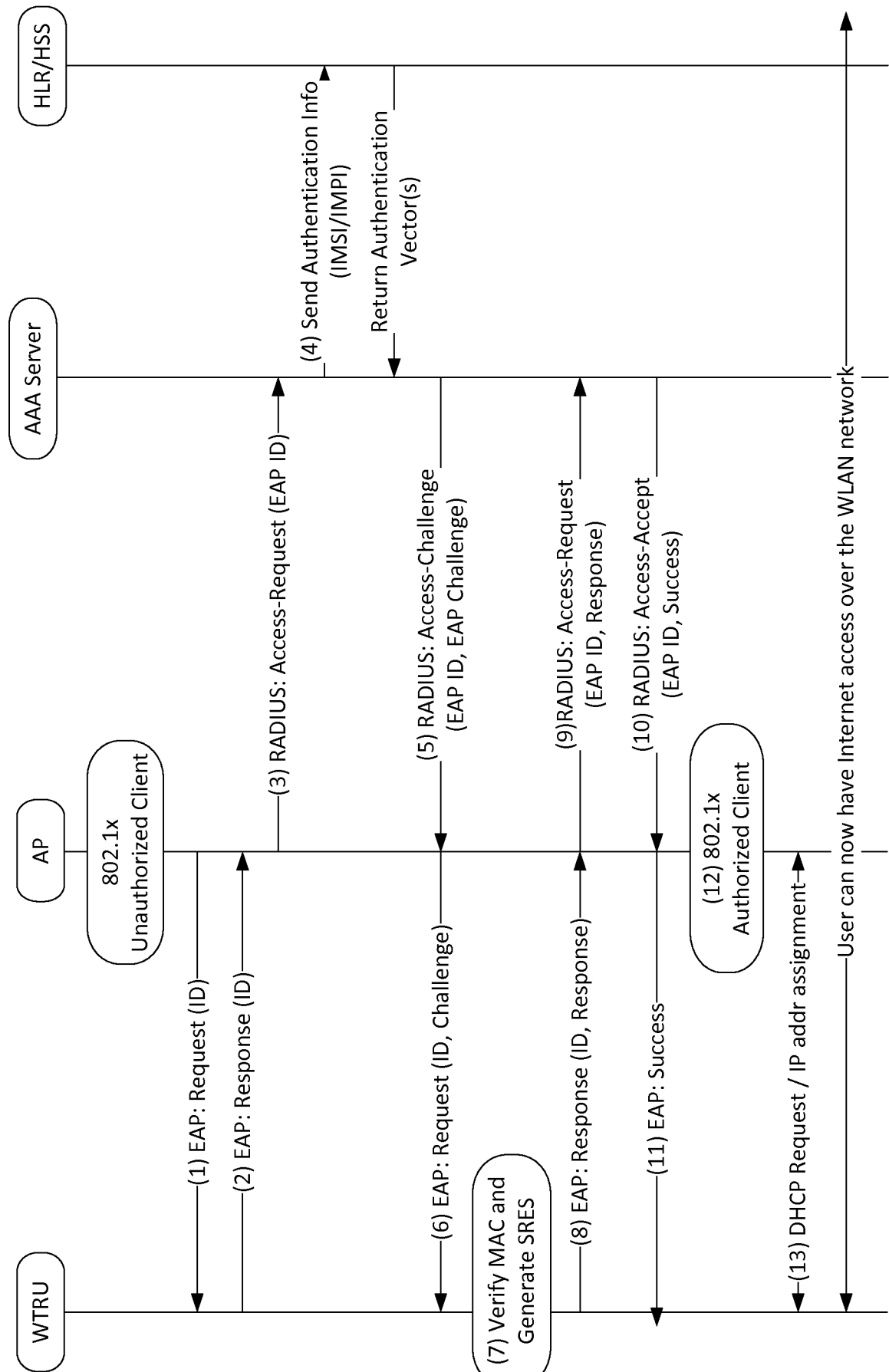


FIG. 8

11/23

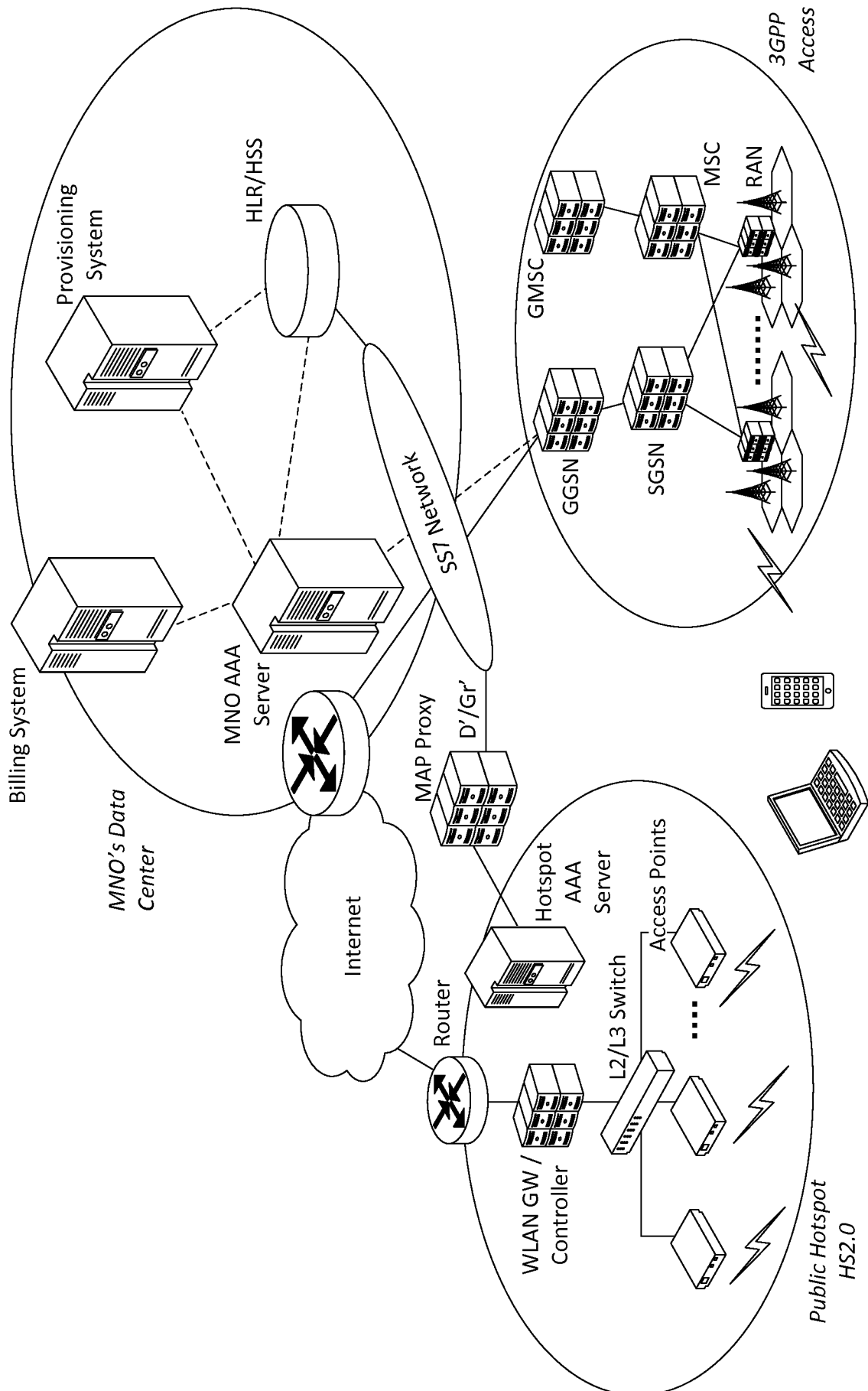


FIG. 9

12/23

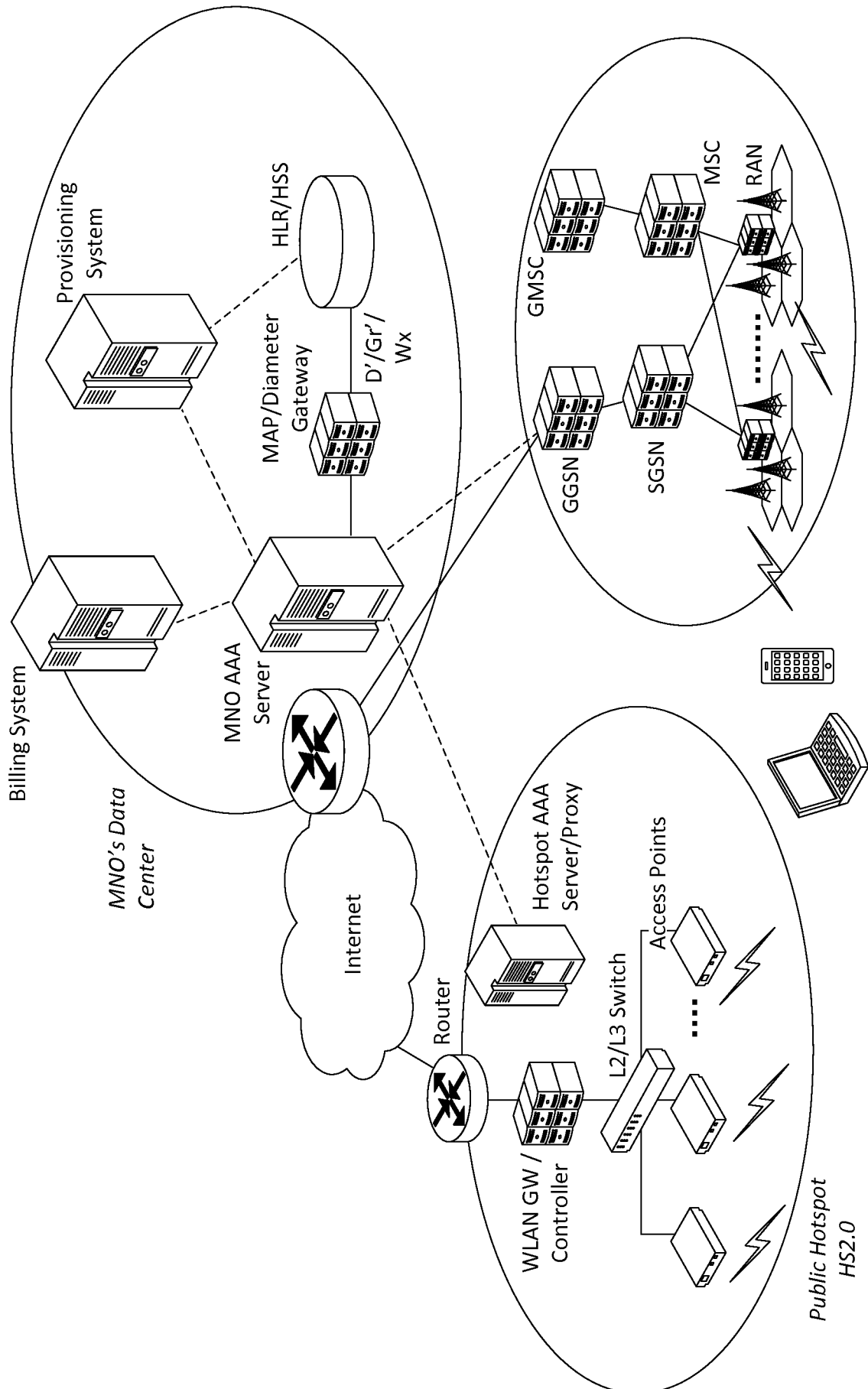


FIG. 10

13/23

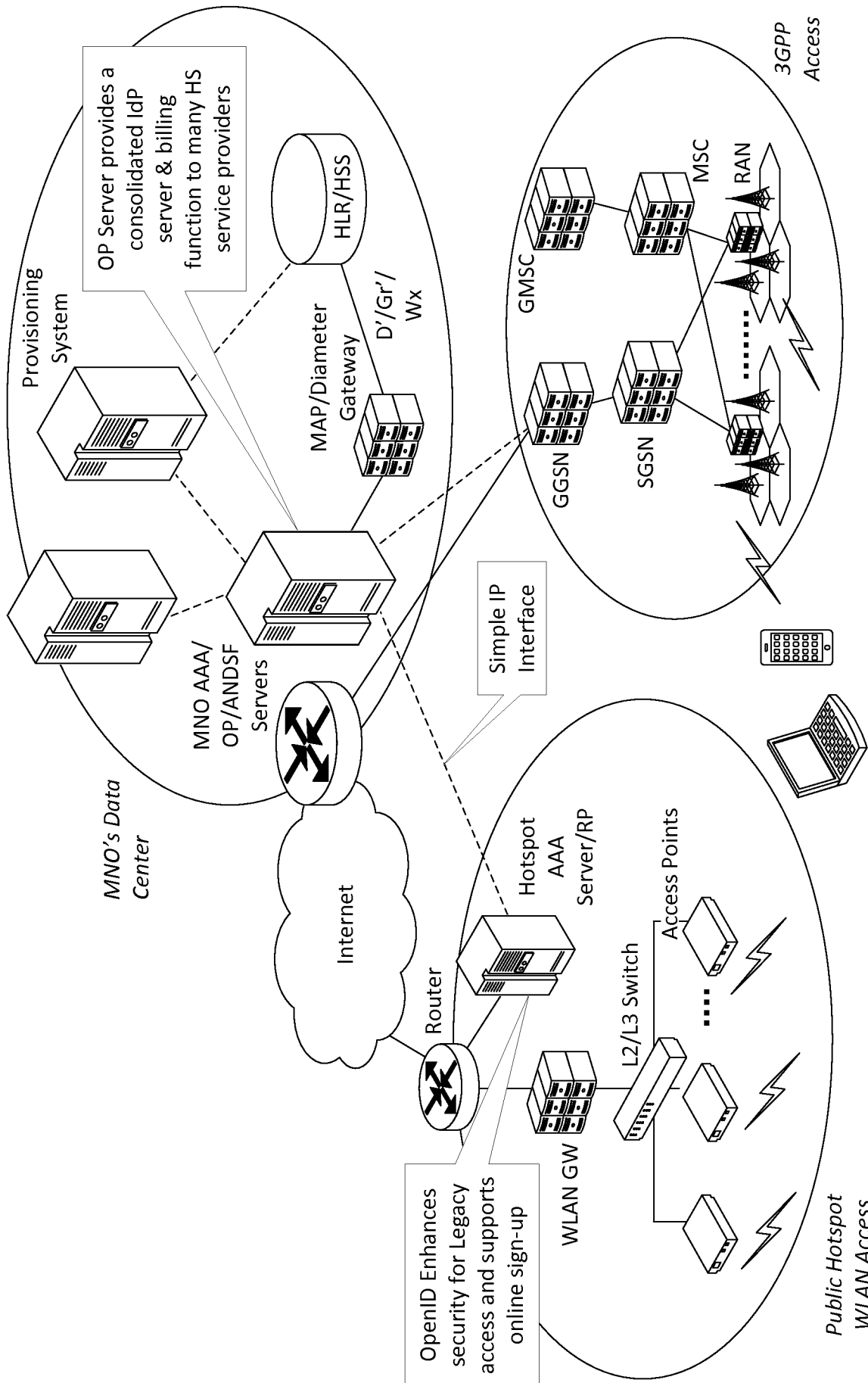


FIG. 11

14/23

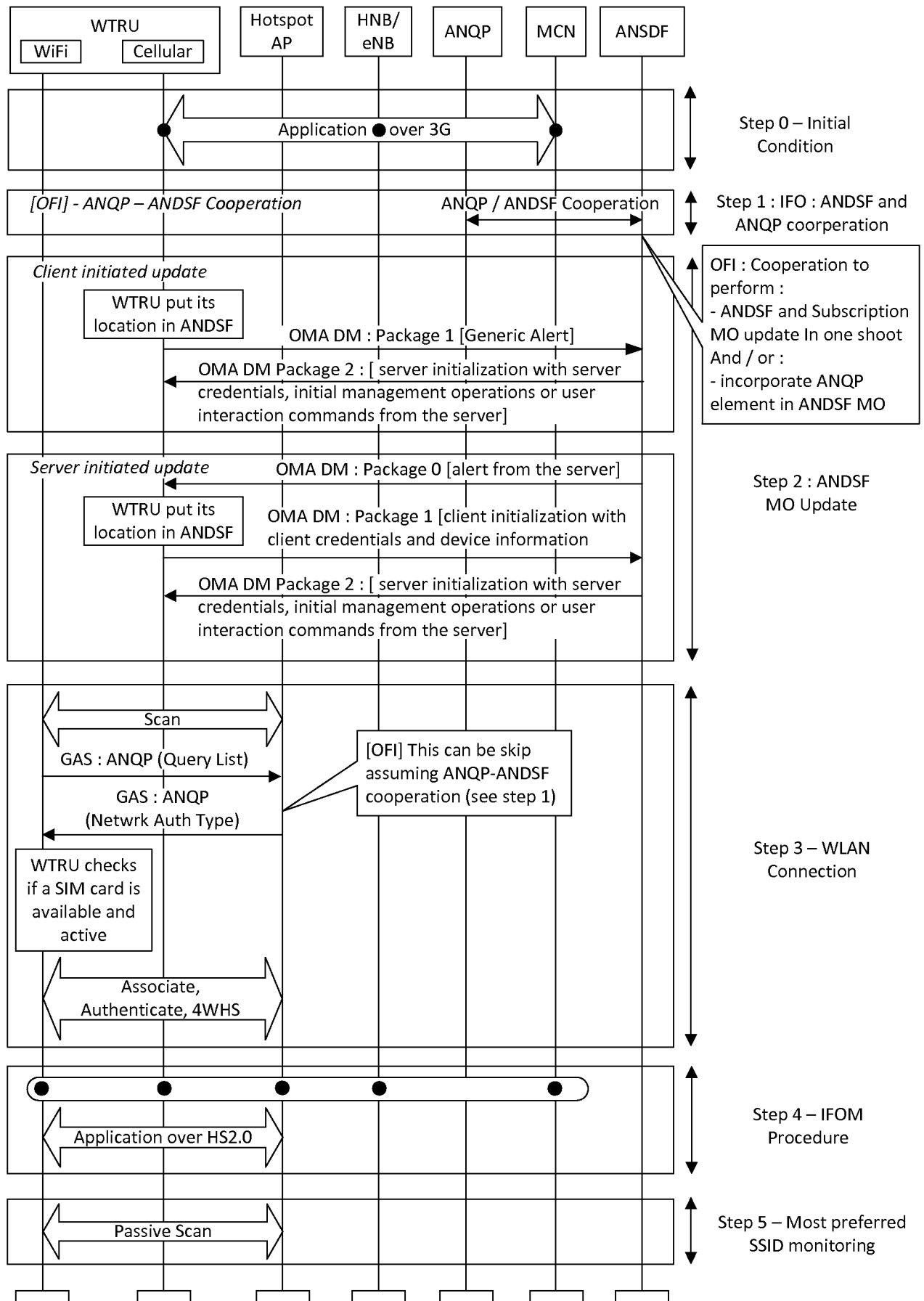


FIG. 12

SUBSTITUTE SHEET (RULE 26)

15/23

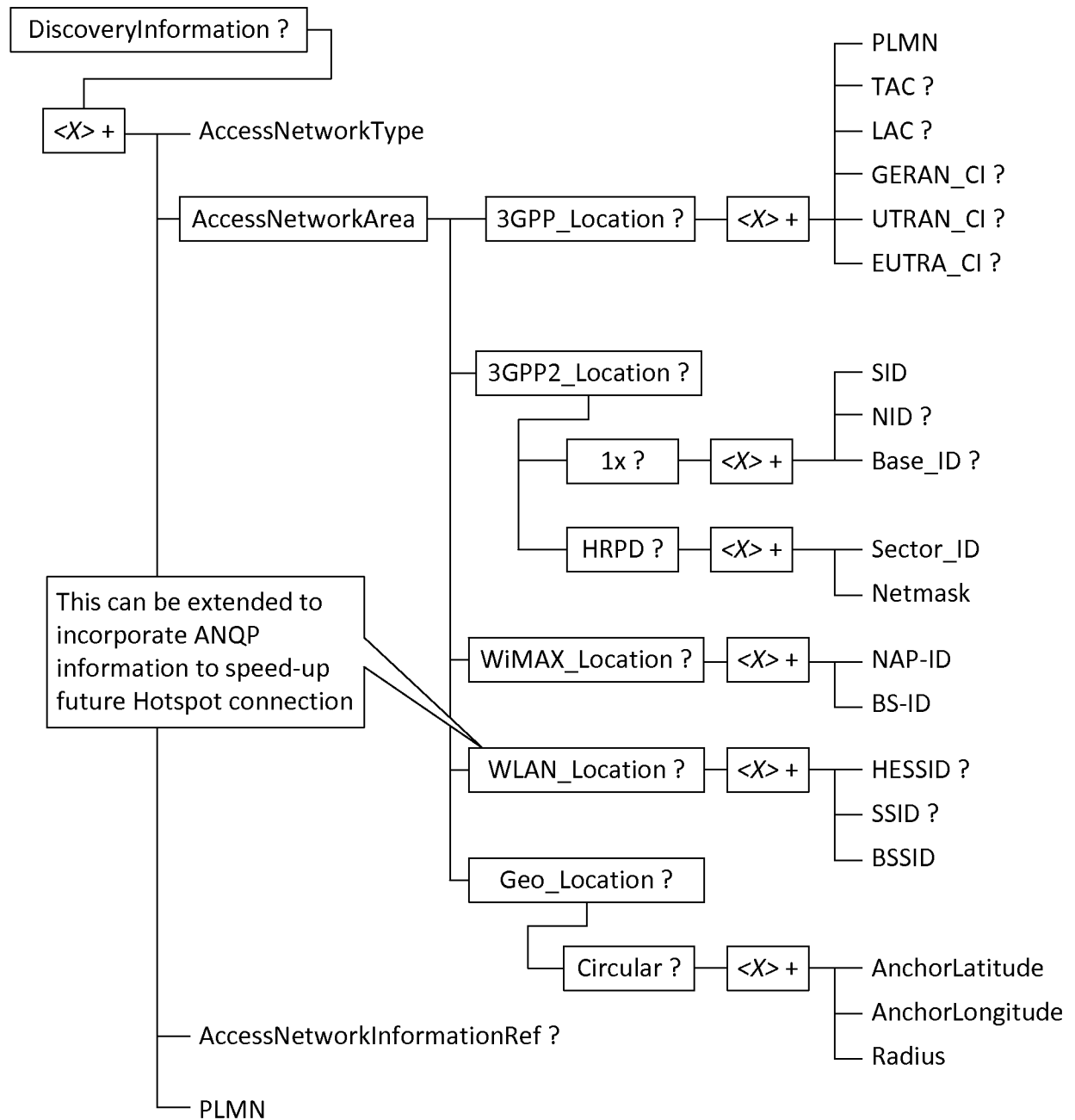


FIG. 13

16/23

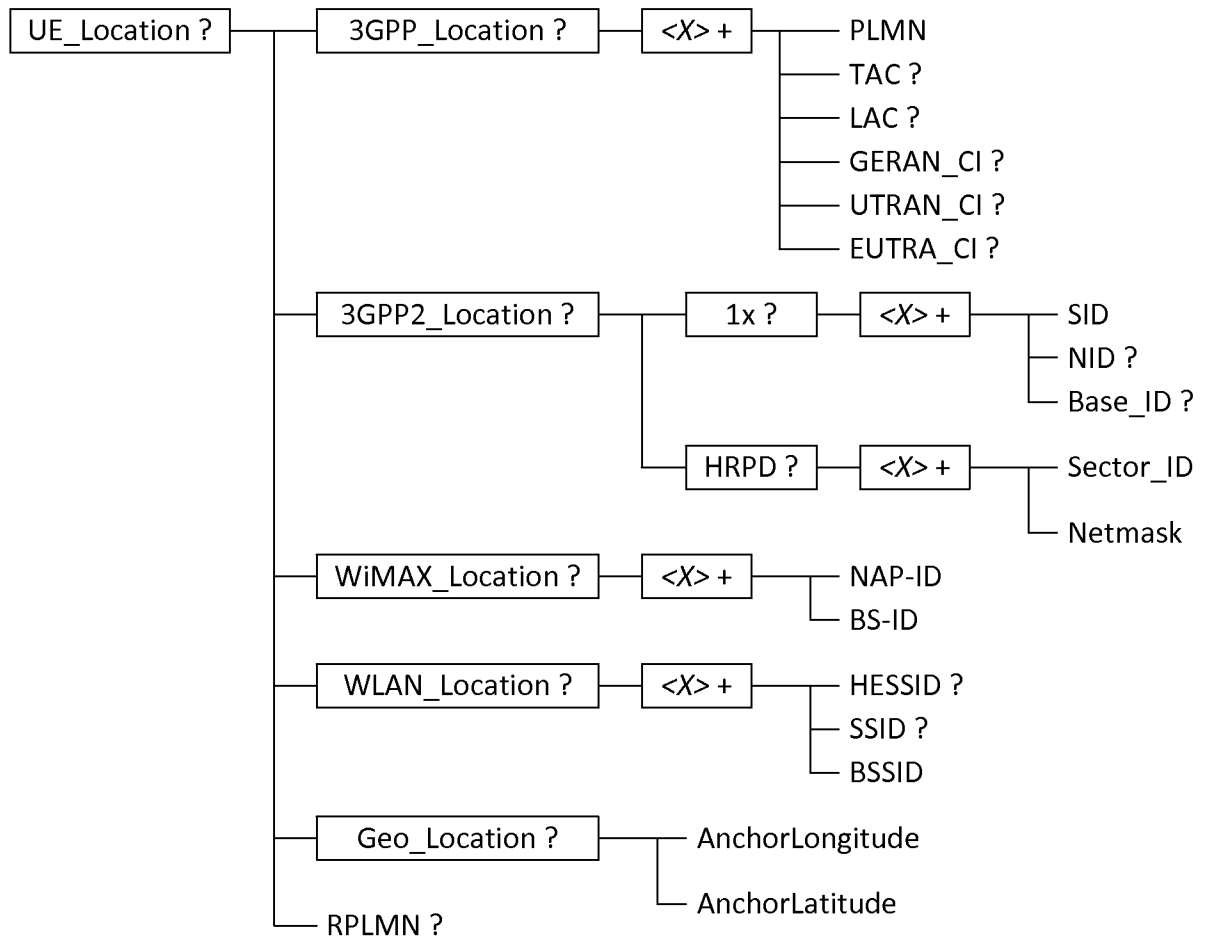


FIG. 14

17/23

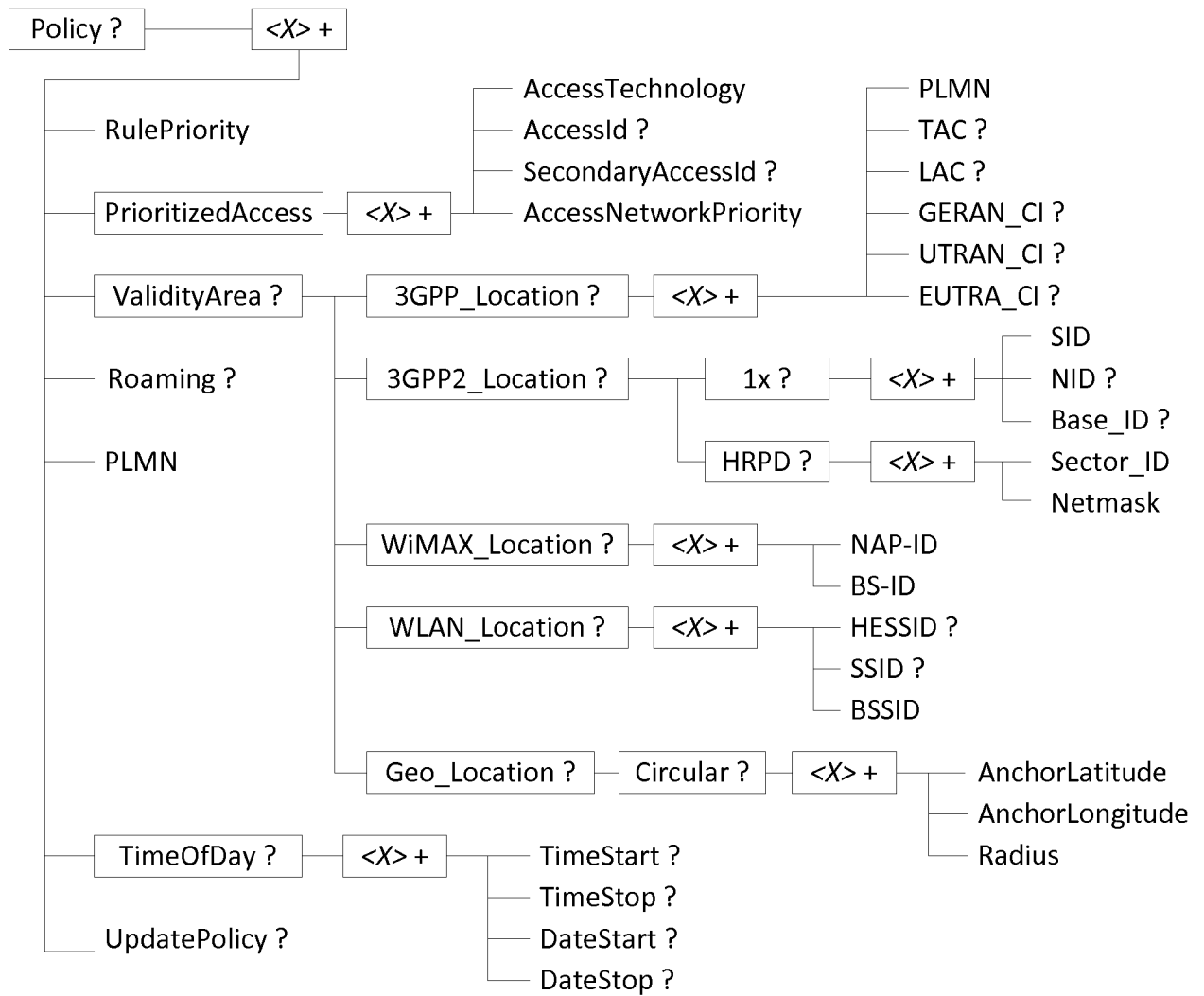


FIG. 15

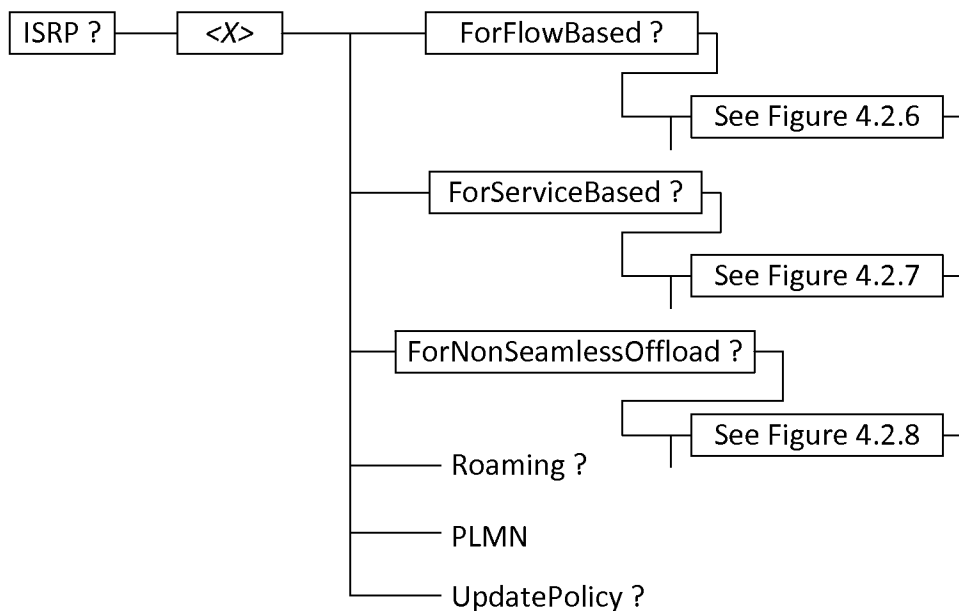


FIG. 16

18/23

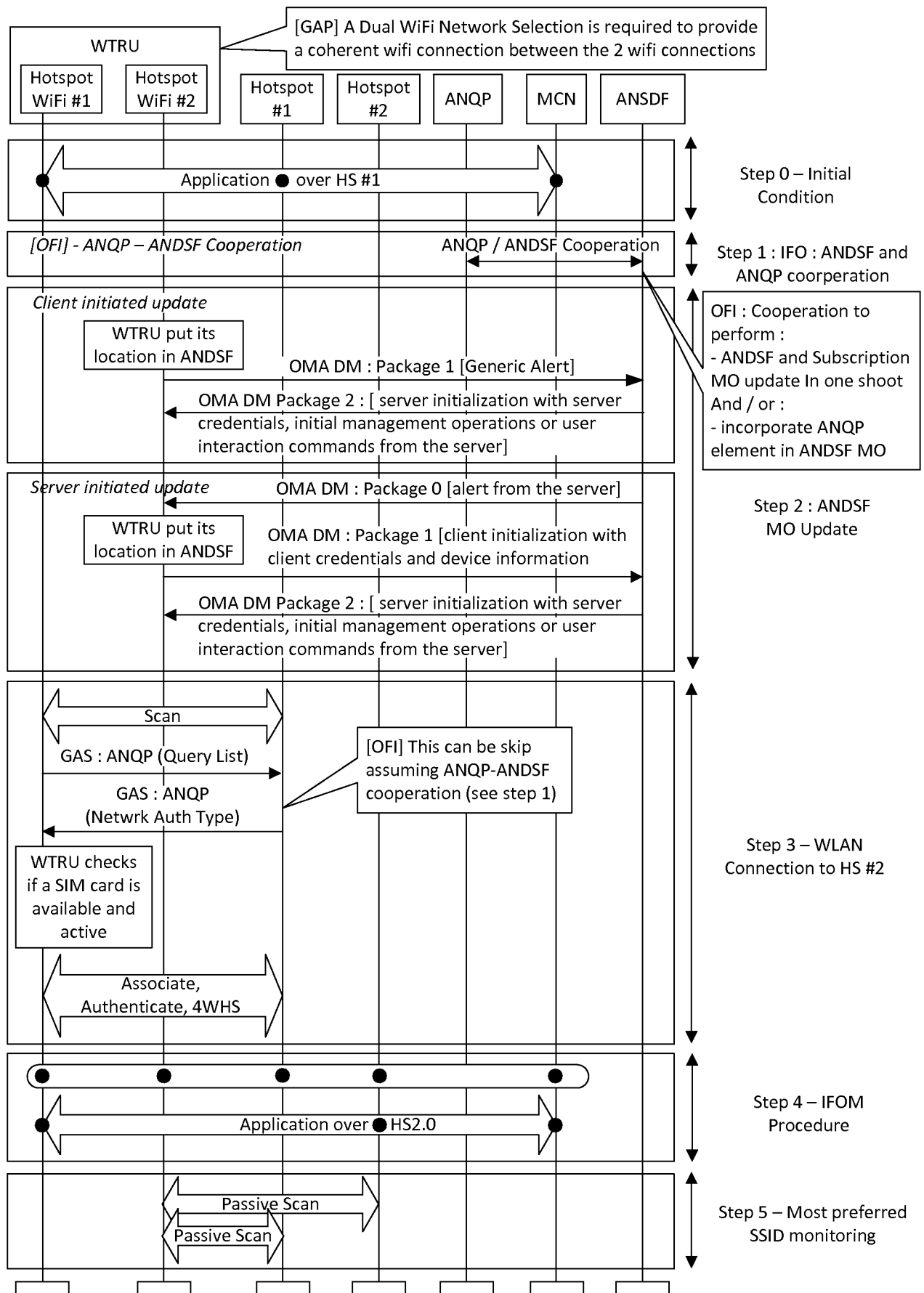


FIG. 17
SUBSTITUTE SHEET (RULE 26)

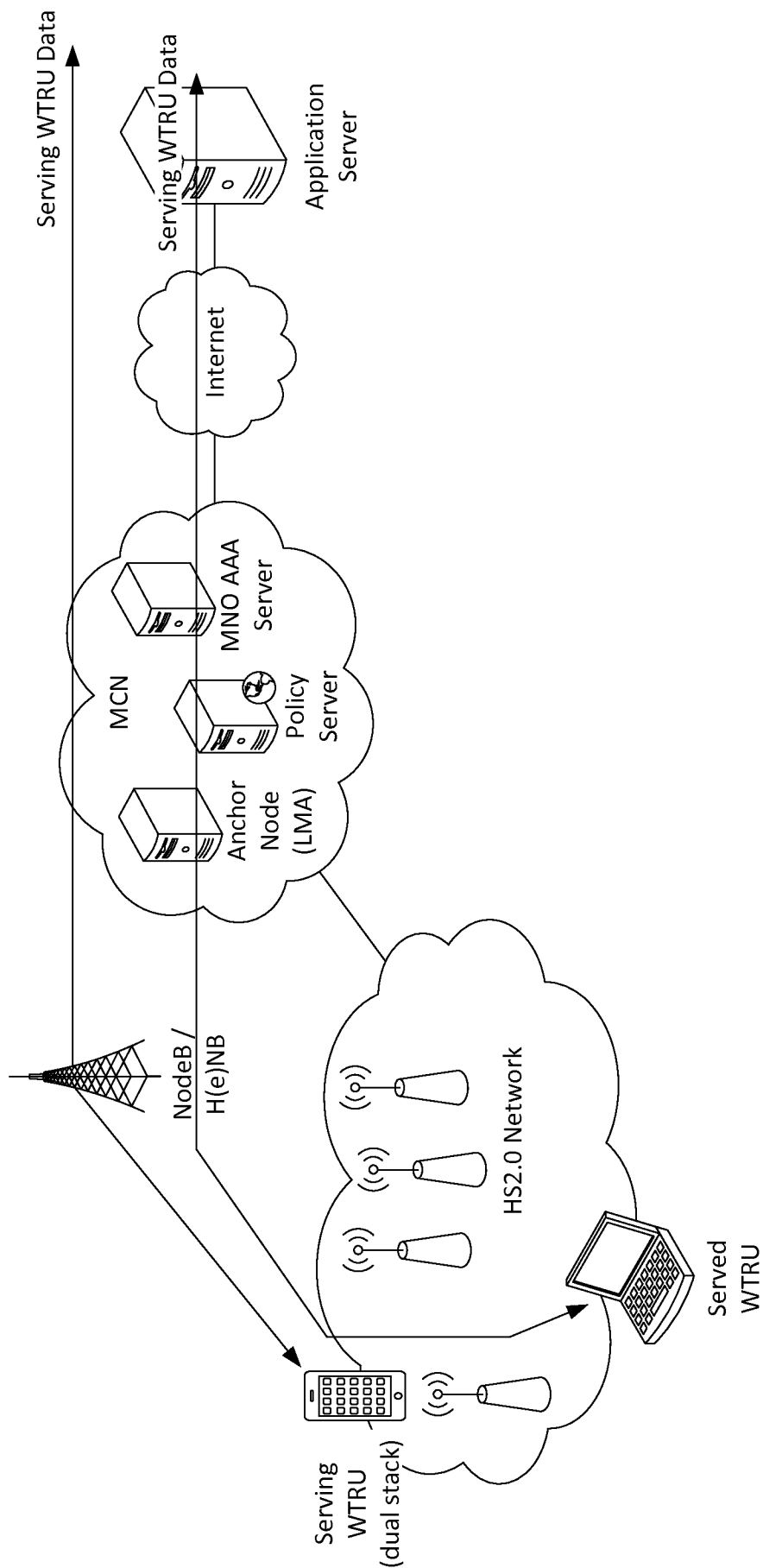


FIG. 18

20/23

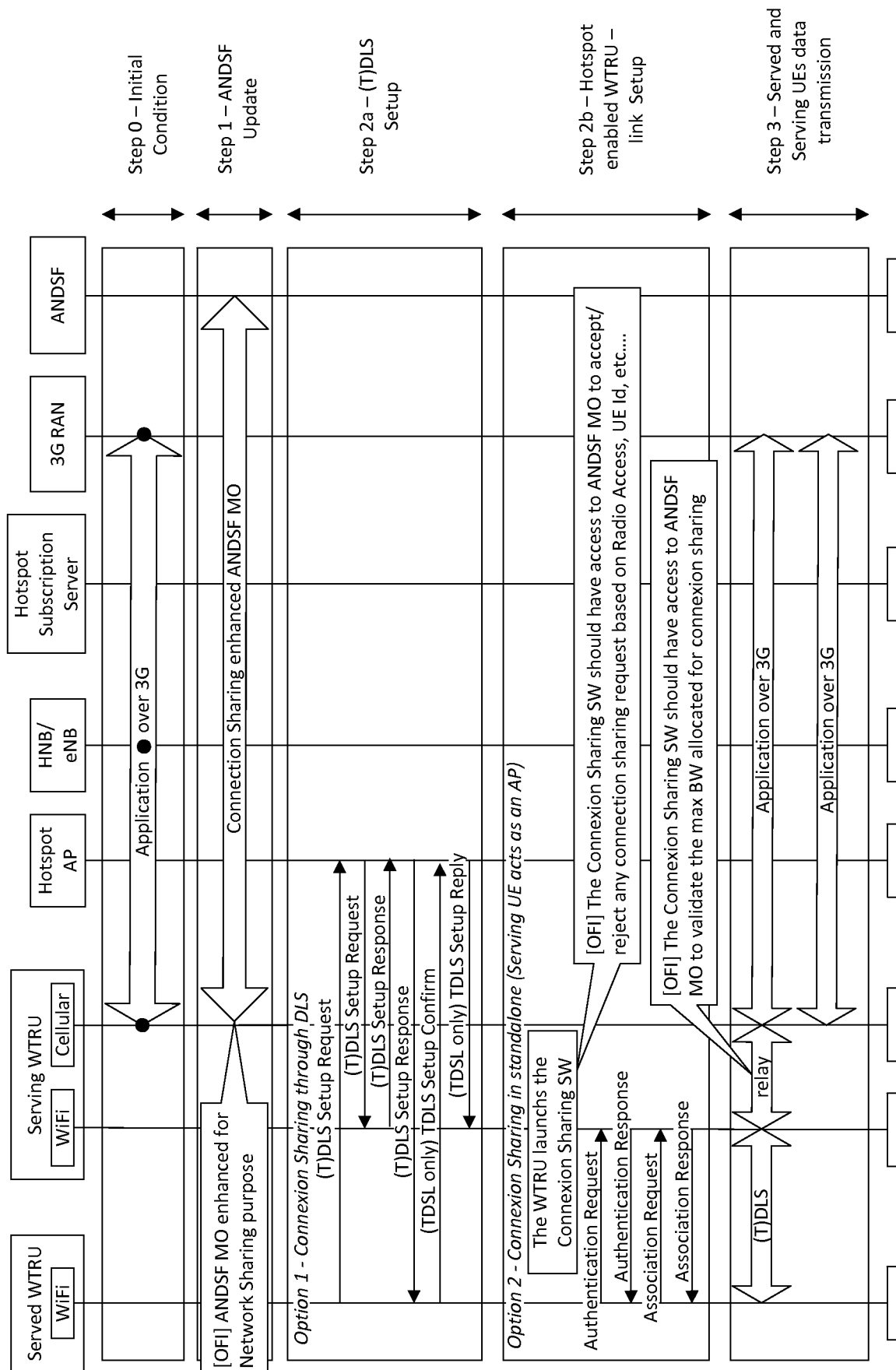


FIG. 19

21/23

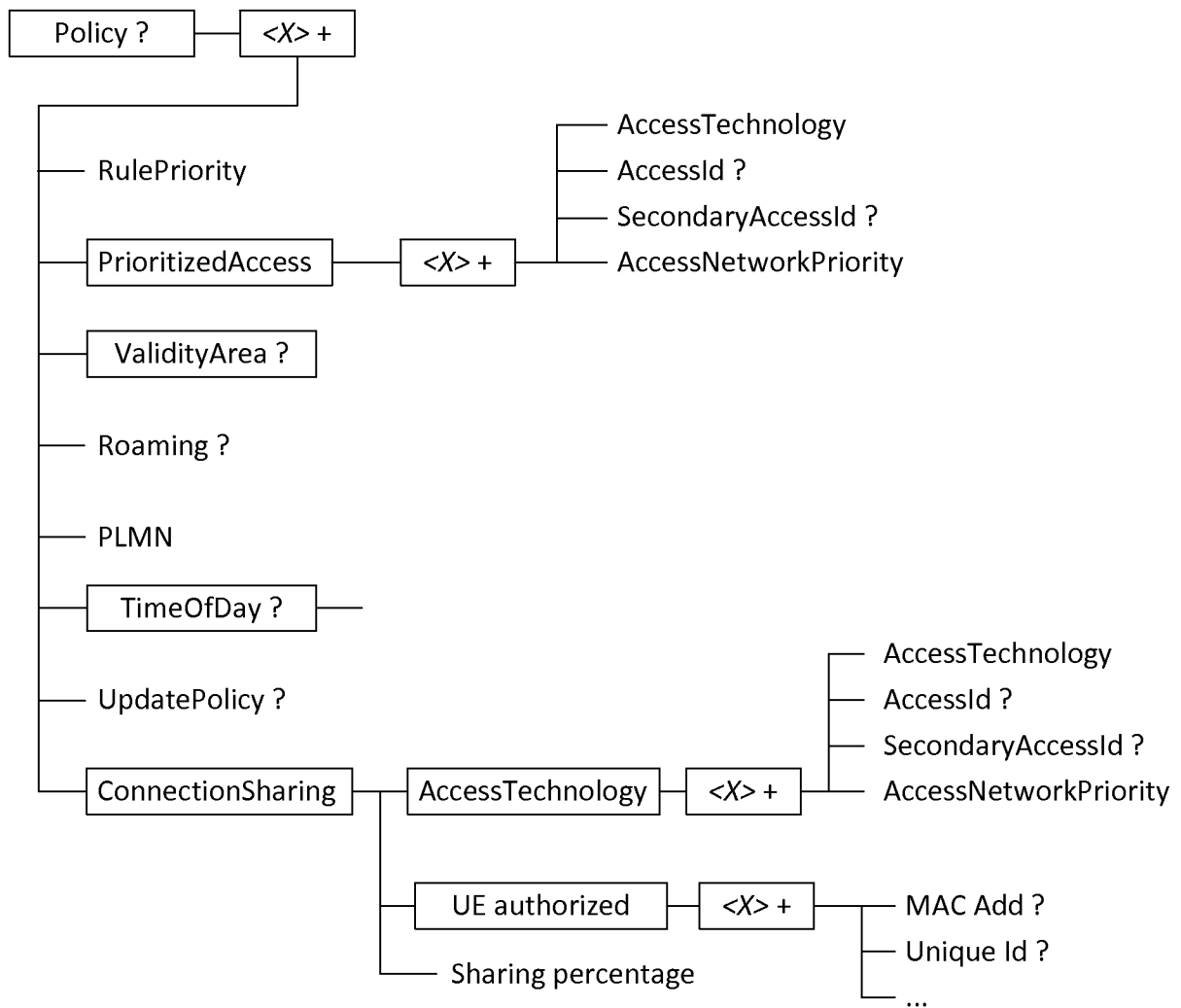


FIG. 20

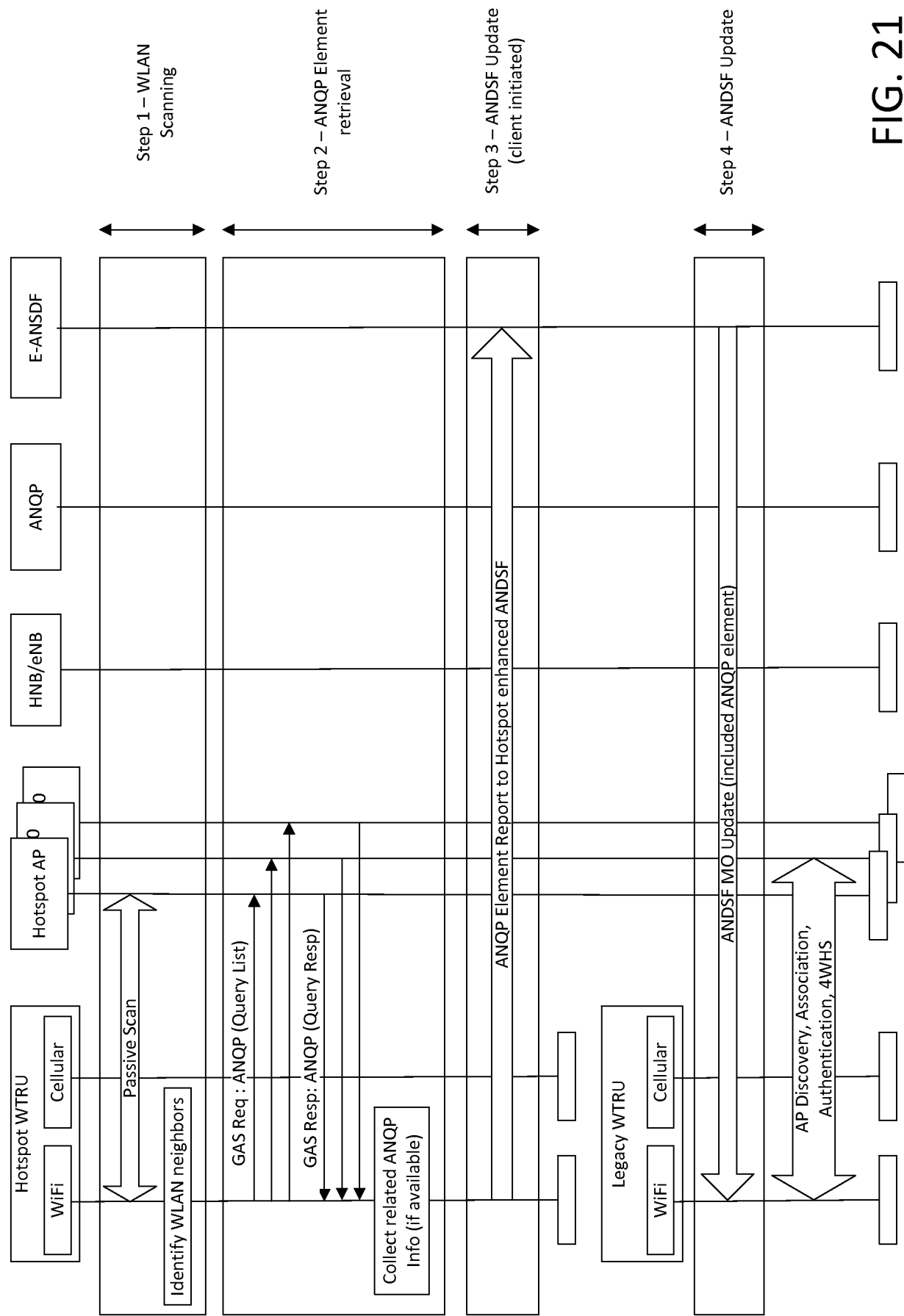


FIG. 21

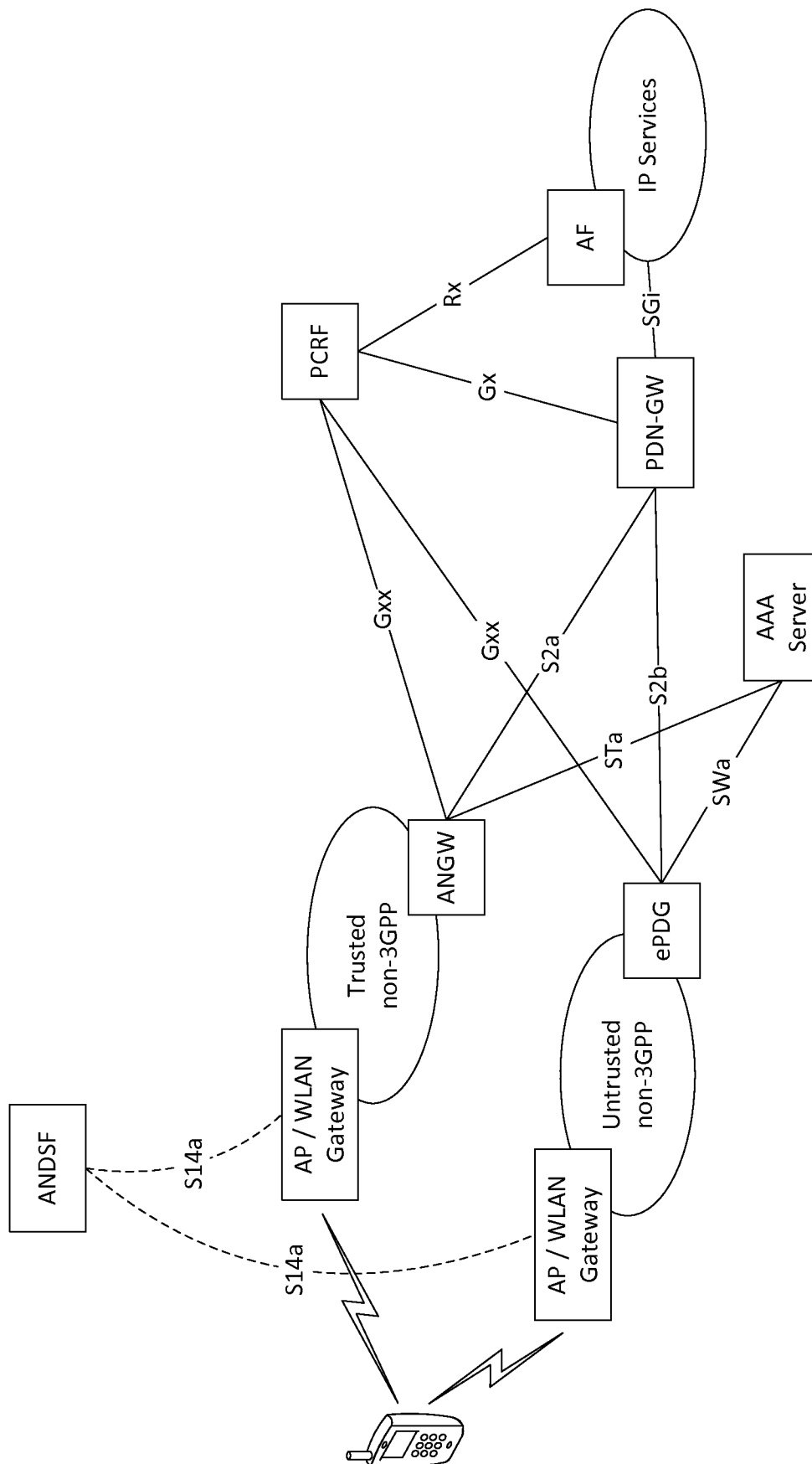


FIG. 22

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/029933

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W48/16
ADD.

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

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, COMPENDEX, INSPEC, 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	US 2010/003980 A1 (RUNE JOHAN [SE] ET AL) 7 January 2010 (2010-01-07) paragraph [0007] - paragraph [0011] paragraph [0044] - paragraph [0087] paragraph [0122] - paragraph [0199] -----	1-16
A	GB 2 457 656 A (IPWIRELESS INC [US] IPWIRELESS INC [US]; IPWIRELESS INC [US]; SONY COR) 26 August 2009 (2009-08-26) the whole document -----	1-16
A	US 2011/264780 A1 (REUNAMAEMI JUKKA PEKKA [FI] ET AL) 27 October 2011 (2011-10-27) the whole document -----	1-16



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

5 June 2013

Date of mailing of the international search report

18/06/2013

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

Frantzeskakis, D

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2013/029933

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010003980	A1	07-01-2010	EP 2324666 A1 25-05-2011
			JP 2011527136 A 20-10-2011
			NZ 589061 A 26-10-2012
			US 2010003980 A1 07-01-2010
			WO 2010002317 A1 07-01-2010

GB 2457656	A	26-08-2009	CN 101981976 A 23-02-2011
			EP 2253165 A1 24-11-2010
			ES 2388482 T3 15-10-2012
			GB 2457656 A 26-08-2009
			RU 2010138617 A 27-03-2012
			US 2011044253 A1 24-02-2011
			WO 2009103678 A1 27-08-2009

US 2011264780	A1	27-10-2011	NONE
