**Title:** LAWFUL INTERCEPTION SOLUTIONS FOR LOCAL OFFLOAD TRAFFIC, LOCAL CACHED TRAFFIC AND LOCAL IP ACCESS TRAFFIC

**Abstract:** A lawful interception (Li) unit may establish a secure tunnel with an evolved home nodeB (HeNB). Over the secured tunnel, the Li unit may receive local offload data for a user. The local offload data for the user may be received over an LO interface. The Li unit may receive an Li configuration signal from an evolved packet core (EPC) unit. The Li configuration signal may indicate to the Li unit that the user is subject of lawful interception. The Li unit may copy the received local offload data for the user and may forward the copied offload data to a law enforcement agency (LEA).
CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of United States Provisional Patent Application No. 61/862,318, filed August 5, 2013, the disclosure of which is hereby incorporated by reference herein in its entirety.

BACKGROUND

[0002] Small cells (e.g., home nodeBs or evolved home nodeBs (H(e)NBs)) may connect wireless transmit/receive units (WTRUs) over cellular network wireless air interfaces (e.g., Long Term Evolution (LTE)) to a cellular operator's network using a backhaul connection. Offload techniques, such as, for example, local offload and/or Local IP Traffic Access (FLIPA) may bypass the Evolved Packet Core (EPC) and communicate directly with an application server, Content Delivery Network (CDN), content provider, and/or another local user. The local offload techniques may not be used in H(e)NBs and/or Local Gateways (LGW), e.g., due to the requirement of having ability to provide lawful interception (Li) of users by law enforcement agencies, even when user data may not traverse the mobile core network.

[0003] Lawful Interception (LI) deployment used in networks may have the Mobility Management Entity (MME), Serving Gateway (SGW) and Packet Domain Network (PDN)
Gateway (PGW) nodes located within the mobile core network. In local offload cases, the MME, SGW and PGW, which may be located within the mobile core network, may not be able to provide LI services for the offload traffic at the H(e)GW or LGW (e.g., using local offload and/or LIパ). Furthermore, the delivery of content from a cached node at a H(e)NB may not be intercepted for LI, because data delivered from local cache may not traverse through the mobile core network.

SUMMARY
[0004] A lawful interception (LI) unit may establish a secure tunnel with an evolved home nodeB (H(e)NB). Over the secured tunnel, the LI unit may receive local offload data for a user. The local offload data for the user may be received over an LO_{OH} interface.
[0005] The LI unit may receive an LI configuration signal from an evolved packet core (EPC) unit. The LI configuration signal may indicate to the LI unit that the user is subject of lawful interception. The LI unit may copy the received local offload data for the user and may forward the copied offload data to a law enforcement agency (LEA).
[0006] A first device located at an internet service provider (ISP) level may receive a configuration from a core network entity. The configuration may include the identity of a second device to monitor. A tunnel may be established with an entity associated with a local area network. A communication associated with the second device may be intercepted. The communication may be sent via the tunnel with the entity associated with the local area network. Information associated with the communication may be reported to a law-enforcement entity.

BRIEF DESCRIPTION OF THE DRAWINGS
[0007] FIG. 1A is a system diagram of an example communications system in which one or more disclosed embodiments may be implemented.
[0008] FIG. 1B is 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 is 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 is 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 is 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.
FIG. 2 illustrates an example of Lawful Interception (LI) of local offload traffic.

FIG. 3 illustrates an example of LI with a local offload data path.

FIG. 4 illustrates an example of LI of local offload data flow using one or more interfaces.

FIG. 5 illustrates an example of a local offload data path, e.g., over the LOoT Interface.

FIG. 6 illustrates an example of uplink and/or downlink local offload data IP addressing for local offload traffic.

FIG. 7 illustrates an example of LI configuration, e.g., via an LOI Interface.

FIG. 8 illustrates an example of interactions between an LI unit and law enforcement management function (LEMF) entity.

FIG. 9 illustrates an example of the protocol stack and the IP addressing that may be used for signals over the X3 and the H13 interfaces.

FIG. 10 illustrates an example of the protocol stack and the IP addressing that may be used for signals over the X3 and the H13 interfaces.

FIG. 11 illustrates an example message chart when the LI is activated for a user with locally offloaded traffic.

FIG. 12 illustrates an example message chart when the LI is activated for a user with locally offloaded traffic.

FIG. 13 illustrates an example of LI of LI PA traffic.

FIG. 14 illustrates an example of LI PA traffic in normal conditions and when a user is subjected to LI.

FIG. 15 illustrates an example of establishing an IPsec and/or GTP tunnels between the H(e)NB, LGW in the ISP and the SeGW.

FIG. 16 illustrates an example of LI for LTPA traffic.

FIG. 17 illustrates an example of LI for LI PA traffic where one or more WTRUs may be the target of surveillance.

FIG. 18 illustrates an example of LI, e.g., when content is cached locally and delivered by an H(e)NB from the local cache to a local user.

FIG. 19 illustrates an example of LI for caching traffic.

FIG. 20 illustrates an example of LI for caching traffic.

FIG. 21 illustrates an example of LI for caching traffic.

FIG. 22 illustrates an example of LI of content that may be delivered from a local cache.
[0033] FIG. 23 illustrates an example of LI of cached content, where the content from a CDN may be placed on an ESF located within an SCN.

[0034] FIG. 24 illustrates an example of LI of cached content, where a LEA may indicate to perform CC surveillance of a user.

[0035] FIG. 25 illustrates one or more examples of LI in presence of one or more LI Proxies.

DETAILED DESCRIPTION

[0036] A detailed description of illustrative embodiments may 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 disclosure. In addition, the figures may illustrate message charts, 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 and additional flows may be added.

[0037] FIG. 1A is a diagram of an example communications system 100 in which one or more disclosed embodiments may be implemented. The communications system 100 may be a multiple access system that provides content, such as voice, data, video, messaging, broadcast, etc., to multiple wireless users. The communications system 100 may enable multiple wireless users to access such content through the sharing of system resources, including wireless bandwidth. For example, the communications systems 100 may employ one or more channel access methods, such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), orthogonal FDMA (OFDMA), single-carrier FDMA (SC-FDMA), and the like.

[0038] As shown in FIG. 1A, the communications system 100 may include wireless transmit/receive units (WTRUs) 102a, 102b, 102c, and/or 102d (which generally or collectively may be referred to as WTRU 102), a radio access network (RAN) 103/104/105, a core network 106/107/109, a public switched telephone network (PSTN) 108, the Internet 110, and other networks 112, though it will be appreciated that the disclosed embodiments contemplate any number of WTRUs, base stations, networks, and/or network elements. Each of the WTRUs 102a, 102b, 102c, 102d may be any type of device configured to operate and/or communicate in a wireless environment. By way of example, the WTRUs 102a, 102b, 102c, 102d may be configured to transmit and/or receive wireless signals and may include wireless transmit/receive unit (WTRU), 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.

[0039] 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 106/107/109, 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 will be appreciated that the base stations 114a, 114b may include any number of interconnected base stations and/or network elements.

[0040] The base station 114a may be part of the RAN 103/104/105, 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, e.g., one for each sector of the cell. In an embodiment, the base station 114a may employ multiple-input multiple output (MIMO) technology and, therefore, may utilize multiple transceivers for each sector of the cell.

[0041] The base stations 114a, 114b may communicate with one or more of the WTRUs 102a, 102b, 102c, 102d over an air interface 115/116/117, which may be any suitable wireless communication link (e.g., radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, etc). The air interface 115/116/117 may be established using any suitable radio access technology (RAT).

[0042] 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 103/104/105 and the WTRUs 102a, 102b, 102c may implement a radio technology such as Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access (UTRA), which may establish the air interface 115/116/117 using wideband CDMA (WCDMA). WCDMA may include communication protocols such as High-Speed Packet
Access (HSPA) and/or Evolved HSPA (HSPA+). HSPA may include High-Speed Downlink Packet Access (HSDPA) and/or High-Speed Uplink Packet Access (HSUPA).

[0043] In an embodiment, the base station 114a and the WTRUs 102a, 102b, 102c may implement a radio technology such as Evolved UMTS Terrestrial Radio Access (E-UTRA), which may establish the air interface 115/116/117 using Long Term Evolution (LTE) and/or LTE-Advanced (LTE-A).

[0044] In an embodiment, the base station 114a and the WTRUs 102a, 102b, 102c may implement radio technologies such as IEEE 802.16 (e.g., Worldwide Interoperability for Microwave Access (WiMAX)), CDMA2000, CDMA2000 IX, 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.

[0045] 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 an embodiment, the base station 114b and the WTRUs 102c, 102d may implement a radio technology such as IEEE 802.15 to establish a wireless personal area network (WPAN). In yet an 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 106/107/109.

[0046] The RAN 103/104/105 may be in communication with the core network 106/107/109, 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 106/107/109 may provide call control, billing services, mobile location-based services, pre-paid calling, Internet connectivity, video distribution, etc., and/or perform high-level security functions, such as user authentication. Although not shown in FIG. 1A, it will be appreciated that the RAN 103/104/105 and/or the core network 106/107/109 may be in direct or indirect communication with other RANs that employ the same RAT as the RAN 103/104/105 or a different RAT. For example, in addition to being connected to the RAN 103/104/105, which
may be utilizing an E-UTRA radio technology, the core network 106/107/109 may also be in communication with a RAN (not shown) employing a GSM radio technology.

[0047] The core network 106/107/109 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 a core network connected to one or more RANs, which may employ the same RAT as the RAN 103/104/105 or a different RAT.

[0048] Some or all of the WTRUs 102a, 102b, 102c, 102d in the communications system 100 may include multi-mode capabilities, e.g., the WTRUs 102a, 102b, 102c, 102d may include multiple transceivers for communicating with different wireless networks over different wireless links. For example, the WTRU 102c shown in FIG. 1A may be configured to communicate with the base station 114a, which may employ a cellular-based radio technology, and with the base station 114b, which may employ an IEEE 802 radio technology.

[0049] 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 will be appreciated that the WTRU 102 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment. Also, embodiments contemplate that the base stations 114a and 114b, and/or the nodes that base stations 114a and 114b may represent, such as but not limited to transceiver station (BTS), a Node-B, a site controller, an access point (AP), a home node-B, an evolved home node-B (eNodeB), a home evolved node-B (FleNB), a home evolved node-B gateway, and proxy nodes, among others, may include some or each of the elements depicted in FIG. 1B and described herein.

[0050] 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 will be appreciated that the processor 118 and the transceiver 120 may be integrated together in an electronic package or chip.

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 115/116/117. For example, in one embodiment, the transmit/receive element 122 may be an antenna configured to transmit and/or receive RF signals. In an embodiment, the transmit/receive element 122 may be an emitter/detector configured to transmit and/or receive IR, LTV, 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 will be appreciated that the transmit/receive element 122 may be configured to transmit and/or receive any combination of wireless signals.

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 115/116/117.

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.

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 an embodiment, 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).

[0055] 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.

[0056] 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 115/116/117 from a base station (e.g., base stations 114a, 114b) and/or determine its location based on the timing of the signals being received from two or more nearby base stations. It will be appreciated that the WTRU 102 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

[0057] 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.

[0058] FIG. 1C is a system diagram of the RAN 103 and the core network 106 according to an embodiment. As noted above, the RAN 103 may employ a UTRA radio technology to communicate with the WTRUs 102a, 102b, 102c over the air interface 115. The RAN 103 may also be in communication with the core network 106. As shown in FIG. 1C, the RAN
103 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 115.
The Node-Bs 140a, 140b, 140c may each be associated with a particular cell (not shown)
within the RAN 103. The RAN 103 may also include RNCs 142a, 142b. It will be
appreciated that the RAN 103 may include any number of Node-Bs and RNCs while
remaining consistent with an embodiment.

[0059] 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, macro diversity, security
functions, data encryption, and the like.

[0060] The core network 106 shown in FIG. 1C may include a media gateway (MGW)
144, a mobile switching center (MSG) 146, a serving GPRS support node (SGSN) 148,
and/or a gateway GPRS support node (GGSN) 150. While each of the foregoing elements are
depicted as part of the core network 106, it will be appreciated that any one of these elements
may be owned and/or operated by an entity other than the core network operator.

[0061] The RNC 142a in the RAN 103 may be connected to the MSG 146 in the core
network 106 via an IuCS interface. The MSG 146 may be connected to the MGW 144. The
MSG 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.

[0062] The RNC 142a in the RAN 103 may also be connected to the SGSN 148 in the
core network 106 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.

[0063] As noted above, the core network 106 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.
FIG. 1D is a system diagram of the RAN 104 and the core network 107 according to an embodiment. As noted above, the RAN 104 may employ an E-UTRA radio technology to communicate with the WTRUs 102a, 102b, 102c over the air interface 116. The RAN 104 may also be in communication with the core network 107.

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

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

The core network 107 shown in FIG. 1D may include a mobility management gateway (MME) 162, a serving gateway 164, and a packet data network (PDN) gateway 166. While each of the foregoing elements are depicted as part of the core network 107, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

The MME 162 may be connected to each of the eNode-Bs 160a, 160b, 160c in the RAN 104 via an S1 interface and may serve as a control node. For example, the MME 162 may be responsible for authenticating users of the WTRUs 102a, 102b, 102c, bearer activation/deactivation, selecting a particular serving gateway during an initial attach of the WTRUs 102a, 102b, 102c, and the like. The MME 162 may also provide a control plane function for switching between the RAN 104 and other RANs (not shown) that employ other radio technologies, such as GSM or WCDMA.

The serving gateway 164 may be connected to each of the eNode-Bs 160a, 160b, 160c in the RAN 104 via the S1 interface. The serving gateway 164 may generally route and forward user data packets to/from the WTRUs 102a, 102b, 102c. The serving gateway 164 may also perform other functions, such as anchoring user planes during inter-eNodeB 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.
The saving gateway 6 4 may also be connected to the PDN gateway 166, which may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between the WTRUs 102a, 102b, 102c and IP-enabled devices.

The core network 107 may facilitate communications with other networks. For example, the core network 107 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 107 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 107 and the PSTN 108. In addition, the core network 107 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.

FIG. 1E is a system diagram of the RAN 105 and the core network 109 according to an embodiment. The RAN 105 may be an access service network (ASN) that employs IEEE 802.16 radio technology to communicate with the WTRUs 102a, 102b, 102c over the air interface 117. As will be further discussed below, the communication links between the different functional entities of the WTRUs 102a, 102b, 102c, the RAN 105, and the core network 109 may be defined as reference points.

As shown in FIG. 1E, the RAN 105 may include base stations 180a, 180b, 180c, and an ASN gateway 182, though it will be appreciated that the RAN 105 may include any number of base stations and ASN gateways while remaining consistent with an embodiment. The base stations 180a, 180b, 180c may each be associated with a particular cell (not shown) in the RAN 105 and may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 117. In one embodiment, the base stations 180a, 180b, 180c may implement MIMO technology. Thus, the base station 180a, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 102a. The base stations 180a, 180b, 180c 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 182 may serve as a traffic aggregation point and may be responsible for paging, caching of subscriber profiles, routing to the core network 109, and the like.

The air interface 117 between the WTRUs 102a, 102b, 102c and the RAN 105 may be defined as an R1 reference point that implements the IEEE 802.16 specification. In
addition, each of the WTRUs 102a, 102b, 102c may establish a logical interface (not shown) with the core network 109. The logical interface between the WTRUs 102a, 102b, 102c and the core network 109 may be defined as an R2 reference point, which may be used for authentication, authorization, IP host configuration management, and/or mobility management.

[0075] The communication link between each of the base stations 180a, 180b, 180c 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 180a, 180b, 180e and the ASM gateway 182 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.

[0076] As shown in FIG. IE, the RAN 105 may be connected to the core network 109. The communication link between the RAN 105 and the core network 109 may be defined as an R3 reference point that includes protocols for facilitating data transfer and mobility management capabilities, for example. The core network 109 may include a mobile IP home agent (MIP-HA) 184, an authentication, authorization, accounting (AAA) server 186, and a gateway 188. While each of the foregoing elements are depicted as part of the core network 109, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0077] The MIP-HA may be responsible for IP address management, and may enable the WTRUs 102a, 102b, 102c to roam between different ASNs and/or different core networks. The MIP-HA 184 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 186 may be responsible for user authentication and for supporting user services. The gateway 188 may facilitate interworking with other networks. For example, the gateway 188 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. In addition, the gateway 188 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.

[0078] Although not shown in FIG. IE, it will be appreciated that the RAN 105 may be connected to other ASNs and the core network 109 may be connected to other core networks. The communication link between the RAN 105 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 105 and the other ASNs. The communication link between the core network 109 and the other core networks may be defined as an R5 reference, which may include protocols for facilitating interworking between home core networks and visited core networks.

[0079] In this document, the term converged gateway (CGW) may be used to mean CGW, H(e)NB, small cell network (SCN) controller or an edge node entity that sits at the edge of a LAN. CGW functionality may be incorporated in an LGW. While embodiments may be illustrated with reference to a particular device, other of the devices may be used.

[0080] Lawful Interception (LI) may involve a CGW, an H(e)NB, or a similar entity (e.g., an edge node entity) that may support local offload and/or LTPA. A CGW, for example, may make a copy of the local offload or LIPA data, for example, to satisfy the LI requirements. The converged gateway (CGW) may be a CGW, an LGW, an H(e)NB, a small cell network (SCN) controller, or an edge node entity that may sit at the edge of a LAN. The CGW may forward data to one or more LI functions within the mobile core network and/or a law enforcement agency (LEA). While this is a feasible solution, there may be a risk of exposing that the user is the target of surveillance because the entity making the data copy may be located in the local area network. The target of surveillance may look at the volume of traffic leaving the CGW and may determine that it is making a copy of data for LI. The CGW may be an intercepting network element (TNE) and/or an intercepting control element (ICE) and may extend an LI function from the core network, e.g., via the X1-1, X2, and/or X3 interfaces to the CGW. Delivery of cached content from a local server may be used for data delivery, e.g., via local offload and/or LIPA.

[0081] For traffic (e.g., IP traffic) that is offloaded via local offload and/or LIPA, or delivered from a local cache by the H(e)NB, CGW, or a similar edge node entity, the aid of the internet service providers (ISPs) may be enlisted. Such aid may be enlisted with cooperation between the ISP and the mobile core network owner. In such a case, the target of surveillance may be less likely to discover they are the target of surveillance. One or more interfaces (e.g., standard based interfaces) between the ISP and the mobile core network entities and protocols for the interfaces may be provided. The interfaces between the ISP and the mobile core network may be a standard interface and may use a standard protocol, e.g., with a standard set of messages and procedures. One or more of the mobile node operator (MNO) functionality may be integrated into the ISP network.
An interface may be defined between the SCN and the EPC that may allow the SCN to inform the EPC that content has been delivered by cache. The EPC may provide that content to law enforcement by indicating to the CDN to send the data to the LEA or by indicating to the EPC to send the data to the LEA.

Cached content may be delivered from a local cache node in a SCN. In an SCN, e.g., an area serviced by an H(e)NB and/or LGW, or a set of H(e)NBs and/or LGWs, one or more nodes may include content. This content may be placed in the cached node by a CDN or by an equivalent content provider or by a content owner. A local cache may deliver content to an end-user in this way. Since the data may be delivered from the local cache to an end user, the data may not traverse the mobile core network. The data path may be established from the cache node that may be in the small cell network to the H(e)NB and to the end user device. An LGW may be placed in the ISP network, e.g., when content is to be delivered from this local node. The data path may be established from the cache node, to the LGW in the ISP, where the data may be lawfully intercepted, to the H(e)NB and to the end-user device. A copy of the data in the core network and/or a copy of the cached content may be provided to the LEA when the content is delivered from this local cache node. The local cache node may inform the core network of the data that may be delivered along with a digest value. The digest value may be used to determine integrity of the delivered data.

An interface between an ISP and one or more mobile core network operators may be provided for lawful interception. The interface may enable the mobile core network to inform the ISP that a specific user’s traffic may be subject of lawful interception. The interface may enable the ISP to copy the local offload data, LIPA data, or locally cached data and to forward the same to a law enforcement agency.

Mobile network operator (MNO) functionality may be placed in an ISP network. The MNO functionality may be placed in the customer premises or the mobile operator’s core network and may aid in supporting the LI of traffic that may not be routed through the MNO.

An interface from a SCN to an EPC may be used to facilitate compliance with the LI requirements when content is delivered from a cache local to the SCN.

The H(e)NB (or other edge node entity, such as CGW) may identify the traffic that may be offloaded from the MNO or delivered from a local cache. Such information may be provisioned in the H(e)NB. The information may be provided by the H(e)NB Management System (H(e)MS) or other entity. The H(e)NB may decide to locally offload some traffic, use LIPA on other traffic, and/or deliver some content via cache.
FIG. 2 illustrates an example of LI of local offload traffic. As illustrated in FIG. 2, a local area network 202 may be served by a small cell H(e)NB 204. One or more WTRUs 206 may connect to the H(e)NB 204 using an air interface. The H(e)NB 204 may be connected to the public Internet 208, e.g., via a digital subscriber line (DSL) modem 210 (or equivalent, such as a cable modem, a T1 line, etc.). As illustrated in FIG. 2, an evolved packet core (EPC) network 212 may comprise one or more EPC based components and may be connected to the public Internet 208 by a Secure Gateway (SeGW) 214. The SeGW 214 may be placed at the boundary between the EPC 212 and the public Internet 208. One or more of the application servers 216, CDNs, content providers, law enforcement agencies 218, and/or one or more ISPs 220 may be present on the public Internet 208. An ISP network 220 may include one or more components, including, for example a Digital Subscriber Line Access Multiplexer (DSLAM) 222 or an equivalent unit, an LI functionality, a Broadband Remote Access Server (BRAS) 226 or an equivalent, and other one or more routers 228. The LI functionality of an TSP 22.0 may be handled by an LI unit 22.4 or by a third party platform. The LI functionality may be placed within the ISP network 220 and may be responsible for interfacing with one or more law enforcement agencies and may be placed on the traffic data paths within the TSP 22.0. The third party platforms and ISPs may conform their interfaces to the H[1], H[2], H[3] interfaces, for example, as used by LEAs. As illustrated in FIG. 2, the LI functionality may be placed in line with the ISP Network data path. In other cases, one or more devices in the ISP network 220 may send a copy of the data to a third party LI functional entity. One or more devices may be placed outside the ISP network 22.0 and may send a copy of the data to a third party LI functional entity. The endpoint of local offload traffic sourced through the H(e)NB 204 may be the LI unit 224. For cached content, an LGW may be introduced in the ISP network 220.

Lawful interception of local offload traffic may be provided. As illustrated in FIG. 2, LI of local offload traffic, one or more interfaces (e.g., two interfaces) and/or a reference interface may be provided. An interface 227 may be provided between the H(e)NB 204 and the LI unit 224 within the ISP network 22.0. This interface 227 may be an L1/L2 interface and may be used to route local offload traffic between a WTRU and a destination on the public Internet 208 such that it bypasses the EPC 212. An interface 228 may be an interface between the LI unit 224 and LI functions 2.30 within the EPC, and may be designated as LI/L3 interface and may be used to inform the LI unit 224 if local offload traffic may be captured and routed to law enforcement for the purpose of surveillance. The LI unit 224 may have one or more
interfaces with the LEA 218. The LOI interface 228 may be used to provide the LI unit 224 in the ISP network 2.20 information about the cellular identity of a user (e.g., the IP address assigned by the EPC 212). Using the information about the identity of the user, the LI unit 224 may duplicate and/or forward the traffic of a user under surveillance to a law enforcement entity (e.g., an LEA unit).

[0090] FIG. 3 is an example diagram of a LI system 300 illustrating an example local offload data path. As illustrated in FIG. 3, an H(e)NB 302 may route data through a DSL modem 304, into a DSLAM 306, and into a LI unit 308 placed within an ISP network 310, e.g., uplink data. The data (whether uplink and/or downlink) may be checked to determine if it should be copied and sent to LEA 324. The data may traverse the BRAS 312 and the public Internet 314, e.g., via a router/network address translation (NAT) function 316 at the edge of the ISP network 310. After reaching the public Internet 314, the uplink data may reach an application server 318. This data may not touch the core network elements. The corresponding downlink data may traverse the reverse path.

[0091] In FIG. 3, non-offloaded data, e.g., EPC-based data, may be illustrated for reference. As this non-offloaded data traverses an EPC 320, if the user is the target of surveillance, this EPC-based data may be forwarded to LI functions 322 within the EPC 320 and forwarded to the LEA 324.

[0092] A local offload data path may be provided. FIG. 4 illustrates LI of local offload data flow using one or more example interfaces. One of the interfaces may be used to provide LI of locally offloaded data flows. As illustrated in FIG. 4, a data path bypassing the EPC and the configuration interface for the LI unit within the EPC may be provided. An LI interface 402 between a LI unit 404 and a LEA 406 may be used as the interface that may be used to carry any local offload data that is identified for LI (e.g., required to be intercepted by law enforcement).

[0093] FIG. 5 illustrates an example of a local offload data path, e.g., over the LOoIr Interface. FIG. 5 illustrates a protocol stack 500 between WTRU 502, H(e)NB 504, LI unit 506, router 508, and application server 510. An IPsec tunnel 512 may be established between the H(e)NB 504 and the LI unit 506. As illustrated in FIG. 5, the IPsec tunnel 512 may be used to transport locally offloaded traffic between the H(e)NB 504 and LI unit 506. The LI unit 506 may support IP Sec and may use a NAT function.

[0094] FIG. 6 illustrates an example of uplink and downlink local offload data IP addressing, e.g., for local offload traffic. As illustrated in FIG. 6, the uplink and downlink data may be encapsulated using the IPsec tunnel between the H(e)NB 602 and the LI unit
The NAT function may be performed at the LI unit 604 and/or the router 606 at the edge of the ISP network.

[0095] FIG. 7 illustrates an example of LI configuration, e.g., via an LOu interface 702. FIG. 7 further illustrates the protocol stack of the signals between the LEA 704 and the LI unit 706. The signaling between the LI unit 706 and an LI function in the EPC, e.g., admin function 708, may be provided. As illustrated in FIG. 7, the signaling between the LEA 704 and the admin function 708 of the LI functional component within the EPC may be provided. An interface between the LEA 704 and the admin function 708 may be provided. The signaling between the admin function 708 and LI unit 706 may use the SeGW of the EPC to provide a secure interface between the admin function 708 and the LI unit 706. As illustrated in FIG. 7, the traffic outside the EPC, e.g., between the LI unit 706 and the SeGW 710 (and between the SeGW 710 and the LEA 704, for example) may be secured by means of IP Sec encryption.

[0096] FIG. 8 illustrates an example of interactions between an LI unit 802 and LEA entity 804, e.g., for LI configuration. FIG. 8 further illustrates the IP addressing used as messages may travel between the LI unit 802 and the admin function 806, e.g., over the LOu interface. An interface (e.g., tIli interface) between the admin function 806 and the LEA entity 804 may be provided.

[0097] X3 and HI3 interfaces may be provided. The X3 interface between the LI unit and the mediation function in the ISP network and the HI3 interface between a mediation function in the ISP network and the LEA may be used. The mediation function may be an ISP entity that may be responsible for formatting data so that the data may be interpreted by a law enforcement agency. The interfaces may pass the content of communication captured by the LI unit for traffic that may be locally offloaded for users who may be subject of surveillance. FIGS. 9 and 10 illustrate an example of the protocol stack 900 and IP addressing that may be used for signals over the X3 and the HI3 interfaces.

[0098] FIGS. 11 and 12 illustrate a message chart (MC) when LI may be activated for a user with locally offloaded traffic. FIGS. 11 and 12 may illustrate non-locally offloaded traffic paths. As illustrated in FIG. 11, an IPsec tunnel 1102 may be established between the H(e)NB 1104 and the SeGW 1106. The H(e)NB 1104 may contact the H(e)MS 1108 and provision the H(e)MS 1108 at 1110, for example, with LI unit information and/or an offload policy. An object (e.g., a data object) may include the LI unit contact information. The LI unit contact information (e.g., an FQDN or an IP address) may be secured and may not be readily available to an entity that may access the H(e)NB 1104. The communication between
the H(e)NB 1104 and H(e)MS 1108 may be encapsulated in the IPsec tunnel 1102 between
the H(e)NB 1104 and SeGW 1106 at the edge of the mobile core network. The IPsec tunnel
1102 at the H(e)NB 1104 may terminate at the trusted environment (TrE) within the device.
IPsec may be used between the H(e)NB 1104 and SeGW 1106. The communication between
the H(e)NB 1104 and H(e)MS 1108 may be secured and may be used to secure -information
(e.g., LI unit contact information).

[0099] The offload policy to be employed by the H(e)NB 1104 may be provisioned
during the LI of local offload traffic. The H(e)NB 1104 may receive the policy information.
The H(e)NB 1104 may create an IPsec tunnel 1112 with the LI unit 1114 at 1116. This IPsec
tunnel 1112 in the H(e)NB 1104 may terminate at the TrE within the device. The interface
between the two endpoints may be secured.

[0100] As illustrated in FIG. 11 at 1120, a WTRU 1118 may attach to the EPC and a
bearer (e.g., a default bearer and/or a dedicated bearer) may be established. As illustrated in
FIG. 11, a GPRS tunneling protocol (GTP) tunnel 1122 from the H(e)NB to the SeGW may
be established. As illustrated by example in FIG. 11, the non-local offload path data may
traverse the EPC.

[0101] FIG. 12 illustrates an example of traffic flow in case of a local offload. As
illustrated in FIG. 12, the H(e)NB 1202 may place uplink traffic that is to be locally offloaded
into the IPsec tunnel 1204 with the LI unit 1206. The LI unit 1206 may extract the traffic
from the IPsec tunnel 1204. The LI unit 1206 may NAT the source IP address and push the
packet towards the router 1208. The router 1208 may perform NAT and push the packet
towards the Application Server 1210. For downlink traffic received at the router of the ISP
Network, the router 1208 may perform a NAT and push the packet towards the LI unit 1206.
Once the LI unit 1206 receives this packet, it may perform a NAT and push the packet
towards the H(e)NB 1202 using the IPsec tunnel 1204. At the H(e)NB 1202, the IP Sec
tunnel 1204 may be terminated and the packet may be sent (e.g., over the air) to the WTRU
1212.

[0102] As illustrated in FIG. 12, the LEA 1214 may activate surveillance of a user. At
1216, the LEA 1214 may send a command to the admin function 1218 within the EPC, e.g.,
using the H[1] interface, which may indicate that a user is subject to surveillance. The admin
function 1218 may learn, e.g., from the Home Subscriber Server (HSS), the location of the
SGW and MME that may service the WTRU 1212 at 1220. The admin function may
configure the MME and SGW to perform LI functions. The admin function may learn that the
WTRU 1212 is eligible for local offload (or local offload is active for this user) and that the
LI unit 1206 that may be servicing the WTRU 1212. The admin function may configure the LI unit 1206 to perform LI for the user (e.g., using the IP address assigned to the WTRU 1212) at 1222. The LI unit 1206 may reply with an acknowledgement at 1224, e.g., upon receipt of the request. Data to or from the user may be copied for the purposes of LI. The LI unit 1206 may send a copy of data to a mediation function in the ISP network, e.g., using the X3 interface. The mediation function may send the copied data to the LEA, e.g., using the HI3 interface at 1226. Interfaces from the LI unit 1206 to the mediation functions and from the mediation functions to the LEA may be provided. The cellular local offload data that is subject to surveillance may be copied to law enforcement, e.g., via the ISP’s LI unit 1206.

[0103] One or more entities (e.g., network elements) may be provided that may use the one or more interfaces described herein for LI of local offload traffic. The entities may include one or more of a H(e)NB, a LI unit, or one or more admin functions of the EPC.

[0104] A H(e)NB (e.g., modified H(e)MB) may be provided to support LI for local offload traffic as described herein. The H(e)NB may support an IPsec tunnel to the LI unit and may be enabled to analyze and route uplink and/or downlink traffic related to a particular WTRU. The H(e)NB may create an IPsec tunnel with the LI Unit in the ISP Network. The IPsec tunnel may be provisioned with security keys and/or certificates and with the fully qualified domain name (FQDN) of the LI unit. The H(e)NB may interact with the H(e)MS, and the H(e)NB may be provisioned with the IP address of the LI unit.

[0105] An uplink (UL) packet may be received from a WTRU. The H(e)NB may analyze the packet and may push the packet towards the EPC using a GTP/IPsec tunnel, e.g., using the routing policies at the H(e)NB. The traffic may be pushed towards the LI unit using the IP Sec tunnel that may exist between the H(e)NB and the LI unit, e.g., if the traffic is eligible for local offload. For downlink traffic, the H(e)NB may receive traffic for a specific WTRU via the OTP tunnel with the SGW or via the IPsec tunnel with the LI unit (e.g., for local offload traffic). EPC-routed traffic may be received from the SGW, e.g., via the GTP tunnel while downlink traffic associated with local offload traffic may be received from the LI unit, e.g., via the IPsec tunnel between the LI unit and the H(e)NB.

[0106] The LI unit may be within the ISP network and may support one or more of IPsec, routing of local offload traffic to/from a WTRU, an interface to the LI functions within the EPC, and/or replicating of local offload traffic, e.g., related to a user that may be a target of surveillance. The LI unit may be enabled to establish an IPsec tunnel with the H(e)NB. The IPsec tunnel may be provisioned with one or more keys and/or one or more certificates. The LI unit may support an LO_{1,1} interface to the EPC. The LO_{1,1} interface may have an IPsec
tunnel to the SeGW of the EPC. Using the LO_{1,1} interface, the LI unit may be configured for the traffic that may be captured for LI purposes. The LI unit may be configured to analyze the local offload traffic that may pass through it. The LI unit may be enabled to detect any packets that may match a criterion. The criterion may be configured over the LO_{1,1} interface. The LI unit may be enabled to push a copy of this traffic to a mediation function found in the ISP network.

[0107] The LI unit may be enabled to provide NAT that may be used for the local offload traffic traversing through the LI unit. For uplink traffic, NAT may replace the source address of the WTRU in the data with its own address and may send the packet towards the router at the edge of the ISP network. For downlink traffic, NAT may replace the destination address in the data with the WTRU’s IP address. For uplink traffic, the LI unit may extract the packets from the IP Sec tunnel, and for downlink traffic, the LI unit may insert the traffic into the IPsec tunnel.

[0108] An admin function may be provided, e.g., as described for example in FIG. 12. When the admin function receives a request to perform LI of a user, e.g., identified by an international mobile subscriber identity (IMSI), the admin function may determine the location of the WTRU by communicating with the HSS. Once it determines the WTRU’s location, the admin function may contact the one or more MMEs and/or SGWs to set up the desired level of surveillance.

[0109] The admin function may determine that the LI unit may be performing local offload for this particular user, e.g., to support LI for local offload traffic. The admin function may communicate with the HSS to determine whether the user is eligible for local offload of their traffic. The admin function may determine the H(e)NB that may service the WTRU and/or the ISP network it may contact. The admin function may send the order to perform surveillance for the IP Address of the user. The admin function may send one or more orders to disable surveillance. The LI unit in the ISP may provide similar administrative functions to the SGW and MME in the EPC.

[0110] Lawful Interception (LI) of LIPA Traffic may be provided. FIG. 13 illustrates an example of LI of LIPA traffic. As illustrated in FIG. 13, an LOW 1302 may be placed in the ISP network 1304. The LI unit 1306 may be placed in the ISP network data path, e.g., the LI unit 1306 may be co-located with the LGW 1302 or the LGW 1302 may be located serially in-line with the LI unit 1306 within the ISP network 1304. One or more interfaces (e.g., associated with the LI unit) may terminate at the LGW 1302. The LGW 1302 may perform LI of LIPA traffic, local offload traffic, and/or traffic delivered from cached content. LIPA
traffic may be routed by the H(e)NB 1308 to the receiving local end-user. A management interface between the LGW 1302 and other network elements, such as the MME 1310, may be provided. The management interface may be used to configure the non-U functionality of the LGW 1302, such as configuring it for LIPA bearers.

Fig. 14 illustrates an example of LIPA traffic in normal conditions (e.g., without surveillance) and when a user is subjected to LI. As illustrated in Fig. 14, the LIPA traffic may be routed by the H(e)NB 1402 to the LGW 1404 within the ISP network 1406, and the LGW 1404 may send the traffic back to the H(e)NB 1402 for the local delivery. When LI is activated, the LGW 1404 may be configured to forward a copy of the LIPA data to either the LEA 1408, e.g., as described herein, or the LI function 1410 in the EPC (e.g., when the LI interfaces may be extended outside the EPC). As illustrated in Fig. 14, the traffic may be routed into the LGW 1404 of the ISP network 1406 and may be offloaded from the EPC 1412.

Fig. 15 illustrates an example messaging for establishing IPsec and/or GTP tunnels between the H(e)NB 1502, LGW 1504 in the ISP and the SeGW 1506. As illustrated in Fig. 15, the H(e)NB 1502 may establish an IPsec tunnel 1508 with the SeGW 1506 of the EPC. The H(e)NB 1502 may communicate with the H(e)MS 1510 of the EPC to be provisioned. The H(e)NB 1502 may receive one or more standard defined parameters. The H(e)NB 1502 may receive the LGW location in the ISP at 1512. At 1514, the H(e)NB 1502 may contact the LGW 1504 and form an IPsec tunnel 1516 with the LGW, e.g., when the H(e)NB may receive the LGW information.

As illustrated in Fig. 15, the H(e)NB 1502 may establish an SI session with the MME at 1518, and WTRU 1 and WTRU 2 may attach to the EPC using the H(e)NB. At 1520, the WTRUs may complete the Initial Attach procedure and establish the default bearer. The WTRUs may establish a local PDN connection, which may be anchored at the LGW 1504 in the ISP network, for LIPA traffic. The LIPA traffic may establish a distinct PDN connection, e.g., using a LIPA access point name (APN). The LIPA traffic may use a PDN connection and a NAT at the H(e)NB 1502 or LGW 1504 to determine whether the traffic is a LIPA traffic or destined for the EPC. Assuming each of the WTRUs may use a separate PDN connection for LIPA traffic, each of the WTRUs may be associated with one or more (e.g., two) GTP tunnels. A GTP tunnel 1522 may be established between the H(e)NB 1502 and the SeGW 1506, e.g., for handling the EPC bound traffic. A GTP tunnel 1524 may be established between the H(e)NB 1502 and the LGW 1504 in the ISP network, e.g., for LIPA traffic.
FIG. 16 illustrates an example of LI for LIPA traffic. As illustrated in FIG. 16, the data path of LIPA traffic may be established between WTRU 1 and WTRU 2. For data from WTRU 1 to WTRU 2 or from WTRU 2 to WTRU 1 the path traversed may be the same, but in an opposite direction. For data sourced at WTRU 1 and destined for WTRU 2, WTRU 1 may send the data over the air to the H(e)NB 1602. The H(e)NB 1602 may determine that it is LIPA traffic and may forward it to the LGW 1604 within the ISP, e.g., using the established IPsec tunnel and GTP tunnel as described herein. The LGW 1604 may inspect the data and, e.g., based on the destination, may route the data back to the H(e)NB 1602 using an IPsec tunnel (e.g., the same IPsec tunnel) and the GTP tunnel established for the user. The data may be received by the H(e)NB 1602, and may be sent over the air to WTRU 2. Data sourced at WTRU 2 and destined for WTRU 1 may follow the reverse path.

FIG. 17 illustrates an example of LI for LIPA traffic where one or more WTRUs (e.g., WTRU 1 and/or WTRU 2) may be the target of surveillance. The LEA 1702 may inform the admin function 1704 in the EPC, e.g., using the HIT interface, that one or more users (e.g., WTRU 1 and/or WTRU 2) are the target of surveillance at 1706. The admin function 1704 within the EPC may inform one or more of SGW, PGW, or MME nodes located within the EPC that the user may be a target of surveillance. The admin function 1704 may know about the presence of the LGW 1708 and that the WTRU(s) may have a LIPA connection to it. The admin function 1704 may inform the LGW 1708 to copy and/or forward traffic to or from the user to the LEA 1702 at 1710. The LGW may confirm the receipt of this command at 1712. Assuming the target of surveillance is WTRU 1, any traffic that reaches the LGW 1708 that is sourced from WTRU 1 or sent to WTRU 1 may be replicated and sent to the LEA 1702, e.g., via the mediation functions within the ISP network. The LGW 1708 may forward this data to the LI functions in the EPC and may forward the data to the LEA 1702. The node forwarding the data into the LI functions of the EPC may be the LGW 1708 in the ISP.

One or more network elements (e.g., H(e)NB, LGW in the ISP network, admin function of the EPC, etc.) may be provided, e.g., to support the interfaces described herein. As described herein, H(e)NB may support LI for LIPA traffic. The H(e)NB may be enabled to establish an IPsec tunnel to the LGW and to analyze and/or route uplink and/or downlink traffic related to a WTRU. The H(e)NB may establish an IPsec tunnel with the LGW in the ISP network. The IPsec tunnel may be provisioned with one or more keys and/or certificates and with the fully qualified domain name (FQDN) of the LGW. The H(e)NB may
be provisioned with the IP address of the LGW. H(e)NB may communicate with the H(e)MS in the EPC (e.g., using one or more LGW parameters), e.g., to perform the provisioning.

[0118] The H(e)NB may analyze an UL packet e.g., when the UL packet is received from a WTRU over the air. The H(e)NB may push the traffic towards the LGW using the IP Sec/GTP tunnels that may exist between the H(e)NB and the LGW, e.g., when the destination is local (e.g., another WTRU in the same small cell network). The H(e)NB may push the traffic over the air to the destination WTRU, e.g., when the H(e)NB may receive traffic from the LGW in the ISP Network, e.g., via the IP Sec and/or GTP tunnels. The EPC based traffic to the H(e)NB may be passed through without any change.

[0119] An LGW within the ISP network may be based on a standard (e.g., 3GPP standard). The LGW may support LI of LIPA traffic. The LGW may be enabled to establish IPsec and/or GTP tunnels and receive LIPA traffic from a H(e)NB, route LIPA traffic to a H(e)NB, interface to the LI functions within the EPC, and replicate LIPA traffic related to a user who may be target of surveillance.

[0120] The LGW may be enabled to establish an IPsec tunnel and/or GTP tunnels with the H(e)NB. The LGW may be provisioned with one or more keys and/or certificates to create an IPsec tunnel. The LGW may be enabled to support an LOLI interface to the EPC. The LOLI interface may establish an IPsec tunnel to the SeGW of the EPC. Over the LOLI interface, the LGW may be configured to capture traffic that may be under surveillance for LI purposes.

[0121] The LGW may be configured to analyze the LIPA traffic that may pass through the LGW and may detect the packets that may match the criteria, e.g., as configured over the LOI interface. The LI unit may push a copy of the traffic to the mediation functions found in the ISP Network. The LGW may route LIPA traffic to the H(e)NB for delivery to the local intended recipient of the data.

[0122] Admin function may be provided in the EPC. The admin function may receive a request to perform LI associated with a user, e.g., by IMSL. The admin function may determine the location of the WTRU by communicating with the HSS. The admin function may contact the appropriate MME and/or SGW (or MMEs and SGWs) to set up the desired level of surveillance. The admin function may learn from the user that a LGW may support LI for LIPA. The admin function may communicate with the HSS to determine that the user is eligible for LIPA of the traffic from the user. The admin function may determine mapping of the H(e)NB servicing the WTRU and the LGW within the ISP network the admin function may contact. The admin function may determine LGW's existence and location and pass
along the LI order to perform surveillance for the IP Address of the user. The admin function may pass along any orders with regard to disabling surveillance. The LGW in the ISP may serve a similar function to the SGW and MME in the EPC, for LI.

[0123] Lawful interception of content delivered from a local cache may be provided. FIG. 18 illustrates an example of LI, e.g., when content is cached locally and delivered by a H(e)NB from a local cache to a local user. As illustrated in FIG. 18, a LAN may include a WTRU 1802, an H(e)NB 1804, and an edge server farm (ESF) 1806. Content may be stored (e.g., cached) at the ESF 1806 and delivered from the ESF 1806. For example, the ESF content may be provided transparently or in a managed fashion by content delivery network (CDN). The ISP network 1808 may include an LGW\textsuperscript{7} 1810, e.g., for supporting LI for LGW traffic. One or more interfaces between the H(e)NB 1804 and LGW\textsuperscript{7} 1810 and between the LGW 1810 and one or more EPC components may be provided.

[0124] The interface between the H(e)NB 1804 and LGW 1810 may be used to carry traffic between the WTRU 1802 and the ESF 1806. One or more requests for content may be transmitted over the air from the WTRU 1802 to the H(e)NB 1804. The H(e)NB 1804 may forward the request to the LGW 1810, which in turn may forward it to the ESF 1806 in the local network. The content may be delivered, e.g., via the reverse path, from the ESF 1806 to the LGW 1810 in the ISP network, then to the H(e)NB 1804 and finally to the WTRU 1802. The portion of the data path between the H(e)NB 1804 and LGW\textsuperscript{7} 1810 may be denoted as LOO\textsubscript{r}, as described herein. The interface between the LGW 1810 and the LI functions 1812 within the EPC 1814 may be denoted as the LOLI interface. The LOO\textsubscript{r} and LQLI interfaces may be configured to support LI for LIPA traffic, as described herein.

[0125] FIGS. 19, 20, and 21 illustrate examples associated with LI for traffic delivered from a cache. As illustrated in FIG. 19, IPsec and GTP tunnels may be established between the H(e)NB 1902, LGW 1904 in the ISP, and the SeGW 1906. The H(e)NB 1902 may establish an IPsec tunnel 1908 with the SeGW 1906 of the EPC at 1910. The H(e)NB 1902 may communicate with the H(e)MS 1912 of the EPC to be provisioned at 1914 with, for example, the location and/or other information associated with the LGW 1904. The H(e)NB 1902 may receive one or more parameters (e.g., standard defined parameters). The H(e)NB 1902 may receive the location of the LGW\textsuperscript{7} 1904 located in the ISP. The H(e)NB 1902 may contact the LGW 1904 and establish an IPsec tunnel 1915 with the LGW 1904 at 1916. The H(e)NB 1902 may establish an S1 session with the MME at 1918, for example, when the H(e)NB is provisioned by the H(e)MS in the EPC. A local caching node, e.g., within the SCN may be provided.
As illustrated in FIG. 19 at 120, the WTRU 1 may attach to the EPC using the H(e)NB 1902. The WTRU may complete the initial attach procedure. As illustrated in FIG. 19, the WTRU 1 may establish the default bearer. The WTRU may establish a local PDN connection, anchored at the LGW in the ISP network, for LIPA traffic. The LIPA traffic may be handled in one or more ways, for example, via a distinct PDN connection that may be established using a LIPA APN, and/or via a PDN connection with a NAT function that may be used at the H(e)NB (or LGW) to decide whether traffic is LIPA traffic or destined for the EPC. The WTRU may be configured to establish one or more (e.g., two) GTP tunnels, e.g., if the WTRU uses a separate PDN connection for LIPA traffic. A GTP tunnel 1922 may be established between the H(e)NB 1902 and the SeGW 1906. This GTP tunnel 1922 may be used for the EPC bound traffic. A GTP tunnel 1924 may be established between the H(e)NB 1902 and the LGW 1904 in the ISP network. This GTP tunnel may be used for LIPA traffic.

As illustrated in FIG. 20, a cache entity may have some type of content locally cached within it. A path may be established between a WTRU (e.g., WTRU 1) and the cache node 2002. The path traversed by the data from the WTRU to the cache node 2002 or from the cache node 2002 to the WTRU may be the same (except in an opposite direction). For a request from the WTRU to the cache node 2002, the WTRU may send the request over the air to the H(e)NB 2004. The H(e)NB 2004 may notice that the traffic destined for the cache node 2002 and may forward it to the LGW 2006 within the ISP, e.g., using established IPsec tunnel and/or GTP tunnels. The LGW 2006 may determine, e.g., based on the destination, to route the traffic back towards the small cell network (SCN), e.g., the local network in FIG. 18. The SCN may send the traffic back to the DSL modem 2008 at the edge of the SCN. The DSL modem 2008 may forward the traffic to the cache node 2002. A response from the cache node 2002 to the WTRU may follow the same path in reverse direction.

As illustrated in FIG. 21, the WTRU, e.g., WTRU 1, (or the cache node 2102) may be target of surveillance. The LEA 2104 may inform the admin function 2106 in the EPC, e.g., using the H1 interface that the WTRU and/or the cache node 2102 is the target of surveillance at 2108. The admin function 2106 may inform the SGW, PGW, and MME nodes located within the EPC that the user is a target of surveillance. The admin function may know about the presence of the LGW 2110 and that the WTRU might be accessing the local cache node 2102 (or any other local node). As illustrated in FIG. 21, the admin function may inform the LGW 2110 to copy and/or forward any traffic to and/or from the user to LEA at 2112. As illustrated in FIG. 21, the LGW may confirm the receipt of the command at 2114. The traffic sourced from and/or destined to a WTRU under surveillance...
that may reach the LGW 2110 may be replicated and sent to the LEA, e.g., by the mediation functions within the ISP network. This may include traffic between the WTRU and the cache node 2102. The LGW 2110 may forward this data to the LI functions in the EPC. The LI functions may forward this data to the LEA 2104.

[0129] In some cases, the LI of Local SIPTO traffic may be provided. In such a case, the content provider may be a local cache, for example, similar to the case where a content server may be located on the public internet. As described herein, the interfaces and network elements (e.g., the H(e)NB, LGW in the ISP network, and admin function of the EPC) may be provided.

[0130] FIG. 22 illustrates an example of LI of content that may be delivered from a local cache. As illustrated in FIG. 22, the ISP-EPC interface may not be provided for the LI requirements for content delivered via cache. The user may not be aware they are the target of surveillance as the user experience may not be degraded. The cached content may exist in multiple identical copies. A small cell network may be used at the mobile core and the destination from which the WTRU requested it from the cloud. The content (e.g., static content) may not be reported to LI simultaneously when a user under surveillance may access the content. The system may desynchronize the reporting and access events. The reporting and access events may be separated.

[0131] FIG. 22 illustrates an example of LI for cached content. As illustrated in FIG. 22, a Small Cell Network (SCN) 2202 may include one or more of H(e)NBs, LGWs, or equivalent. One or more Edge Server Farms (ESFs) 2204 used to cache content may be placed in the SCN 2202 or outside the SCN 2202. As illustrated in FIG. 22, a DSL Modem, cable modem, T1 line, or any connection to the public Internet may be provided at the edge of the SCN 2202. The modem may act as a router, e.g., by interconnecting entities within the SCN 2202, such as the H(e)NB and the ESF 2204.

[0132] FIG. 22 illustrates a public Internet 2206 with an ISP network 2208 (e.g., for the DSL modem), an LEA 2210 and a content delivery network (CDN) 2212 or equivalent content provider. As illustrated in FIG. 22, an EPC 2214 with the non-LI elements (e.g., MME, SGW, PGW, policy charging and rules function (PCRF), etc.) and the LI functions 2216 (e.g., admin function, delivery function 2 and delivery function 3). The EPC 2214 may include an ESF 2218.

[0133] As illustrated in FIG. 22, the EPC 2214 may know the content stored at the ESF 2204. The EPC 2214 may know the source of the content (e.g., the CDN 2212) or may have a local copy in the ESF 2218, e.g., within the EPC 2214. The H(e)NB and/or the LGW (or
equivalent) may inform the EPC 2214 of the content that may be delivered to an end-user over cache. Upon being informed by a H(e)NB/LGW (or equivalent) that content was delivered to that particular user from a local cache, the EPC 2214 may forward a copy of the content to the LEA 2210. The copy being supplied by the ESF may be available within the EPC 2214 or may be supplied by the CDN 2210 that may have provided the content originally.

[0134] FIGS. 23 and 24 illustrate LI for cached content. An ESF node may be in the EPC 2214 or outside the EPC 2214. If the EPC 2214 does not include the ESF, the task of maintaining a list of content cached at each of the SCNs and the source CDN (or equivalent) of the cached content may be performed by a node in the EPC 2214, e.g., the Policy and Charging Rules Function (PCRF) node. The actual content may not be cached. The PCRF node may not be used for actual data storage.

[0135] As illustrated in FIG. 23, the content from a CDN 2302 may be placed on an ESF 2304 located within an SCN. The content may also be placed on the ESF 2306 within the EPC. The H(e)NB and/or the LGW may be made aware of this content that may be available (e.g., locally available) to the SCN. For example, the content may be denoted by x and y. As illustrated in FIG. 23, the ESF 2306 in the EPC may know where the contents x and y may be placed. For example, the ESF 2304 may be placed in SCN 1. The ESF may know that the source of the original content is CDN 2302.

[0136] As illustrated in FIG. 23, a user device, e.g., WTRU 1 may connect to the EPC via an initial attach procedure at 2308. A default bearer may be created, and a dedicated bearer and/or LIPA bearer may be established. The WTRU 1 may request content x at 2310. The H(e)NB/LGW may redirect this request to the ESF 2304 in SCN 1 at 2312. The SCN 1 may deliver the content x to WTRU 1 at 2314. The ESF 2304 in SCN 1 may inform the ESF 2306 in the EPC that it has delivered content x to WTRU 1 at 2316. The ESF 2306 in the EPC may do nothing further, if WTRU 1 is not the target of surveillance.

[0137] As illustrated in FIG. 24, a LEA 2402 may indicate to perform CC surveillance of a user, e.g., of WTRU 1. The EPC, e.g., via the interface between the EPC and the LEA 2402, may be directed to perform surveillance of WTRU 1 at 2404. The admin function in the Li functions 2406 of the EPC may inform the INE and ICE elements of the EPC to perform surveillance of WTRU 1. The admin function may inform the ESF 2408 in the EPC to perform surveillance of WTRU 1 at 2410.

[0138] The WTRU 1 (e.g., marked for surveillance) may request content y at 2412. When the H(e)NB and/or the LGW receives the request for content y, the request may be redirected
to the ESF 2414 in SCN 1 at 2416. The ESF 2414, upon receipt of this request for content \( y \), may send the requested content to WTRU 1, e.g., via the H(e)NB at 2418. The H(e)NB may inform the ESF 2408 in the EPC that it is sending content \( y \) to WTRU 1 at 2420. The ESF 2408 in the EPC may send the content to the LEA 2402. The EPC may have a local, identical copy of the content \( y \) that may be stored at the local ESF 2414 in SCN 1. The EPC may forward this local copy to the LEA 2402, e.g., using the LI functions 2406 of the EPC. The EPC may determine the CDN (e.g., CDN 2422) that may have sourced the content \( y \). The EPC may contact that CDN and direct it to send the content \( y \) to the LEA 2402 directly. The EPC may determine the CDN (e.g., CDN 2422) that may have sourced the content \( y \). The EPC may contact the CDN and direct it to send the content \( y \) to the ESF 2408 in the EPC. The ESF 2408 in the EPC may forward the content received from the CDN to the LEA 2402, e.g., via the LI functions 2406 in the EPC.

[0139] The ESF 2414 in the SCN may send a digest value in the message in the SCN to the ESF 2408 in the EPC. The digest value may be based on the delivered content. The ESF 2408 in the EPC may compare the received digest value of the content stored within the EPC with the digest value of the content actually delivered to the user by local cache. The ESF 2408 in the EPC may certify that the content in the ESF 2408 of the EPC is identical to the content delivered to the user.

[0140] A message from the ESF 2414 in the SCN to the ESF 2408 in the EPC may include metadata of the content delivered from cache to the user. The metadata may include one or more of the characteristics of the data, the time the data was placed within the cache, the time the data was downloaded, the tools used to create the data, the author of the content, the owner of the content, and/or another characteristic or characteristics that may describe the content or that may differentiate the content from other content.

[0141] Lawful Interception in the presence of a Li proxy may be provided. One or more of LEAs, ISPs, or EPCs may connect to a Li Proxy. The Li proxy may be an aggregator. One or more of LEAs, ISPs, or EPCs may abstain from directly interfacing to one or more of the entities that may require interaction. An ISP may connect to an Li proxy, and the proxy may interface to the one or more LEAs that may exist. An Li proxy may be located between an ISP or EPC network and LEAs.

[0142] FIG. 25 illustrates one or more examples of Li in presence of one or more Li proxies. As illustrated in FIG. 25, the LOO \( f \) and/or LO \( 1 \) interfaces may be provided. The LO\( \text{LOI} \) interface may be provided between the EPC 2502 and the ISP network 2504. The LO\( \text{LOI} \)
interface may be routed through the LI proxy 2506. The LEA may communicate directly with the ISP network 2504, e.g., via the LI proxy 2506 to inform the ISP network 2504 that traffic may be captured. The LEA may communicate with the EPC 2502, e.g., to determine the traffic that may be offloaded for a user. The LGW may be co-located at the LI unit 2508 in the ISP network 2504 and may interface with the LI unit 2508 and LI proxy 2506 to provide LI for LIPA and cache traffic for the interface between the LI proxy 2506 and the ISP network 2504, as described herein.

Although features and elements are described above in particular combinations, each feature or element can be used alone or in any combination with the other features and elements. Additionally, while features and elements are described in a particular order, these features and elements are not limited to the order described. Further, 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.
CLAIMS

What is Claimed:

1. A method for lawful interception of a communication, the method comprising:
   receiving, at a first device located at an internet service provider (ISP) level, a
   configuration from a core network entity, wherein the configuration includes the identity of a
   second device to monitor:
      establishing a tunnel with an entity associated with a local area network;
      intercepting a communication associated with the second device, wherein the
      communication is sent via the tunnel with the entity associated with the local area network;
      and
      reporting information associated with the communication to a law enforcement entity.

2. The method of claim 1, wherein the tunnel is established between a home
   eNodeB (HeNB) and a lawful interception (LI) unit,

3. The method of claim 2, further comprising:
   configuring the LI unit to monitor a communication associated with the second
   device; and
   sending an acknowledgement from the LI unit to a core network entity.

4. The method of claim 1, further comprising sending data associated with the
   second device to the core network entity.

5. The method of claim 1, further comprising reporting information associated
   with the second device to the law enforcement entity.

6. The method of claim 1, further comprising communicating data from the
   second device to a third device.

7. The method of claim 6, wherein the first device is an LGW device.

8. The method of claim 6, further reporting information associated with the
   communicated data to a law enforcement entity.
9. The method of claim 1, further comprising detecting local offload traffic that matches a local offload criterion.

10. The method of claim 9, further comprising pushing a copy of the local offload traffic that matches the local offload criterion to a mediation function.

11. A device configured to perform lawful interception of a communication, the device comprising:
   - a processor comprising processor-readable instructions that when executed, cause the device to receive, at a first device located at an internet service provider (ISP) level, a configuration from a core network entity, wherein the configuration includes the identity of a second device to monitor;
   - establish a tunnel with an entity associated with a local area network;
   - intercept a communication associated with the second device, wherein the communication is sent via the tunnel with the entity associated with the local area network; and
   - report information associated with the communication to a law enforcement entity.

12. The device of claim 11, wherein the tunnel is established between a home eNodeB (HeNB) and a lawful interception (LI) unit.

13. The method of claim 12, wherein the processor is further configured to:
   - configure the LI unit to monitor a communication associated with the second device; and
   - send an acknowledgement from the LI unit to a core network entity.

14. The device of claim 11, wherein the processor is further configured to send data associated with the second device to the core network entity.

15. The device of claim 11, wherein the processor is further configured to report information associated with the second device to the law enforcement entity.
16. The device of claim 11, wherein the device is further configured to communicate data from the second device to a third device.

17. The device of claim 16, wherein the first device is an LGW device.

18. The device of claim 16, wherein the processor is further configured to report information associated with the communicated data to a law enforcement entity.

19. The device of claim 11, wherein the processor is further configured to detect local offload traffic that matches a local offload criterion.

20. The device of claim 19, wherein the processor is further configured to push a copy of the local offload traffic that matches the local offload criterion to a mediation function.
FIG. 16

LEA

Admin Function

H(e)MS

LIPA traffic with no lawful interception

SGW/PGW/ MME/HSS

SeGW

LGW 1624

Destination is local to H(e)NB so LGW may wrap back to H(e)NB. May check if user is target of surveillance.

H(e)NB 1622

Destination is local to H(e)NB. May check if user is target of surveillance.

WTRU 2

WTRU 1

SCN

EPC
WTRU 1 may attach and receive default bearer and/or a dedicated bearer or a LIPA bearer.

For network based traffic:
- GTP tunnel inside IPSec tunnel

For LIPA traffic:
- GTP tunnel inside IPSec tunnel
Initial WTRU attach, default bearer, dedicated bearer, LIPA bearer procedures as needed

No LI of WTRU 1 enabled, so no reporting of cached content delivery to LEA.
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 H04W12/02

ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>

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

**I** 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

**S** document member of the same patent family

Date of the actual completion of the international search

14 November 2014

Date of mailing of the international search report

24/11/2014

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

Kopp, Klaus
### DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2774005 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 102598634 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2471245 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2804358 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20120080619 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2012214445 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2011053040 A2</td>
</tr>
<tr>
<td>EP 2152032 A1</td>
<td>10-02-2010</td>
<td>NONE</td>
</tr>
</tbody>
</table>