



- (51) **International Patent Classification:**
H04W 12/04 (2009.01) *H04W 72/00* (2009.01)
- (21) **International Application Number:**
PCT/US2016/040318
- (22) **International Filing Date:**
30 June 2016 (30.06.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/316,335 31 March 2016 (31.03.2016) US
62/327,650 26 April 2016 (26.04.2016) US
- (71) **Applicant:** INTEL IP CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).
- (72) **Inventors:** OUZIELI, Ido; Fireberg 35 St., 6382732 Tel Aviv (IL). HAREUVENI, Ofer; 58 Harishonim St., Kiryat Haim, 26302 Haifa (IL). SIROTKIN, Alexander; House 172, 90901 Giv'on Hachadasha (IL).
- (74) **Agent:** SHICHRUR, Naim Avraham; Shichrur & Co., Azrieli Business Center, 132 Menachem Begin Blvd., Triangle Tower, 38th Floor, Tel Aviv 6701101 (IL).
- (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *of inventorship (Rule 4.17(iv))*

Published:

- *with international search report (Art. 21(3))*

- (54) **Title:** APPARATUS, SYSTEM AND METHOD OF SELECTIVELY UPDATING KEY INFORMATION OF A SECURED WLAN CONNECTION BETWEEN A UE AND A WLAN AP

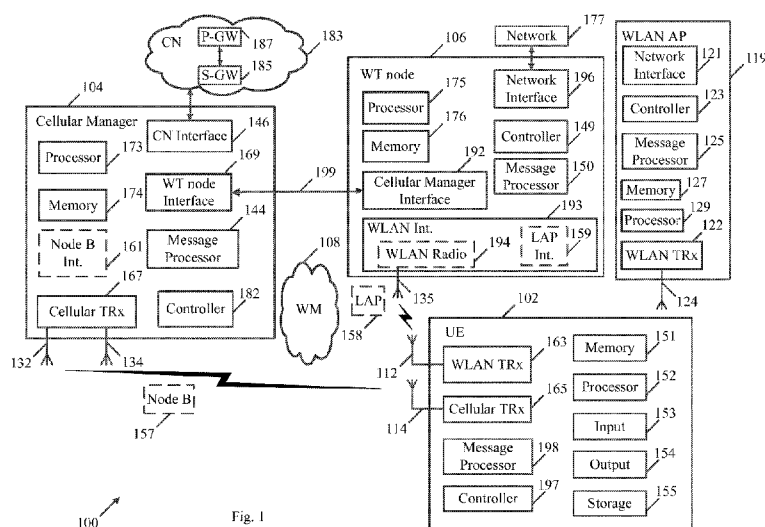


Fig. 1

- (57) **Abstract:** Some demonstrative embodiments include devices, systems and/or methods of selectively updating key information of a secured Wireless Local Area Network (WLAN) connection between a User Equipment (UE) and a WLAN Access Point (AP). For example, an Evolved Node B (eNB) may be configured to control selective transfer of first key information from the eNB to a UE and second key information from the eNB to a WLAN AP, and to select to defer transferring of the first key information to the UE and the second key information to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

**APPARATUS, SYSTEM AND METHOD OF SELECTIVELY UPDATING KEY
INFORMATION OF A SECURED WLAN CONNECTION BETWEEN A UE AND A
WLAN AP**

CROSS REFERENCE

5 [001] This application claims the benefit of and priority from US Provisional Patent
Application No. 62/316,335 entitled “LTE-WLAN AGGREGATION WI-FI REKEYING
AND ENODEB HANDOVER”, filed March 31, 2016, and from US Provisional Patent
Application No. 62/327,650 entitled “LTE-WLAN AGGREGATION WI-FI REKEYING
AND ENODEB HANDOVER”, filed April 26, 2016, the entire disclosures of which are
10 incorporated herein by reference.

TECHNICAL FIELD

[002] Some embodiments described herein generally relate to selectively updating key
information of a secured Wireless Local Area Network (WLAN) connection between a User
15 Equipment (UE) and a WLAN Access Point (AP).

BACKGROUND

[003] A wireless communication device, e.g., a mobile device, may be configured to utilize
20 multiple wireless communication technologies.

[004] For example, a User Equipment (UE) device may be configured to utilize a cellular
connection, e.g., a Universal Mobile Telecommunications System (UMTS) cellular
connection or a Long Term Evolution (LTE) connection, as well as a wireless-local-area-
network (WLAN) connection, e.g., a Wireless-Fidelity (WiFi) connection.

25 [005] There is a need for efficient interworking, integration and/or management of the
cellular and WLAN radio access technologies.

BRIEF DESCRIPTION OF THE DRAWINGS

[006] For simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity of presentation. Furthermore, reference numerals may be repeated among the figures to indicate corresponding or analogous elements. The figures are listed below.

[007] Fig. 1 is a schematic block diagram illustration of a system, in accordance with some demonstrative embodiments.

[008] Fig. 2 is a schematic illustration of operations and communications between a User Equipment (UE), first and second cellular managers, and a Wireless Local Area Network (WLAN) Access point (AP), in accordance with some demonstrative embodiments.

[009] Fig. 3 is a schematic illustration of elements of a UE, in accordance with some demonstrative embodiments.

[0010] Fig. 4 is a schematic flow-chart illustration of a method of selectively updating key information of a secured WLAN connection between a UE and a WLAN AP, in accordance with some demonstrative embodiments.

[0011] Fig. 5 is a schematic flow-chart illustration of a method of selectively updating key information of a secured WLAN connection between a UE and a WLAN AP, in accordance with some demonstrative embodiments.

[0012] Fig. 6 is a schematic flow-chart illustration of a method of selectively updating key information of a secured WLAN connection between a UE and a WLAN AP, in accordance with some demonstrative embodiments.

[0013] Fig. 7 is a schematic illustration of a product, in accordance with some demonstrative embodiments.

DETAILED DESCRIPTION

[0014] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of some embodiments. However, it will be understood by persons of ordinary skill in the art that some embodiments may be practiced without these specific details. In other instances, well-known methods, procedures, components, units and/or circuits have not been described in detail so as not to obscure the discussion.

[0015] Discussions herein utilizing terms such as, for example, “processing”, “computing”, “calculating”, “determining”, “establishing”, “analyzing”, “checking”, or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulate and/or transform data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information storage medium that may store instructions to perform operations and/or processes.

[0016] The terms “plurality” and “a plurality”, as used herein, include, for example, “multiple” or “two or more”. For example, “a plurality of items” includes two or more items.

[0017] References to “one embodiment,” “an embodiment,” “demonstrative embodiment,” “various embodiments,” etc., indicate that the embodiment(s) so described may include a particular feature, structure, or characteristic, but not every embodiment necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrase “in one embodiment” does not necessarily refer to the same embodiment, although it may.

[0018] As used herein, unless otherwise specified the use of the ordinal adjectives “first,” “second,” “third,” etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0019] Some embodiments may be used in conjunction with various devices and systems, for example, a Personal Computer (PC), a desktop computer, a mobile computer, a laptop computer, a notebook computer, a tablet computer, a Smartphone device, a server computer, a handheld computer, a handheld device, a Personal Digital Assistant (PDA) device, a handheld PDA device, an on-board device, an off-board device, an Internet of Things (IoT) device, a sensor device, a wearable device, a hybrid device, a vehicular device, a non-

vehicular device, a mobile or portable device, a consumer device, a non-mobile or non-portable device, a wireless communication station, a wireless communication device, a wireless Access Point (AP), a wired or wireless router, a wired or wireless modem, a video device, an audio device, an audio-video (A/V) device, a wired or wireless network, a wireless area network, a cellular network, a cellular node, a cellular device, a Wireless Local Area Network (WLAN), a Multiple Input Multiple Output (MIMO) transceiver or device, a Single Input Multiple Output (SIMO) transceiver or device, a Multiple Input Single Output (MISO) transceiver or device, a device having one or more internal antennas and/or external antennas, Digital Video Broadcast (DVB) devices or systems, multi-standard radio devices or systems, a wired or wireless handheld device, e.g., a Smartphone, a Wireless Application Protocol (WAP) device, vending machines, sell terminals, and the like.

[0020] Some embodiments may be used in conjunction with devices and/or networks operating in accordance with existing 3rd Generation Partnership Project (3GPP) and/or Long Term Evolution (LTE) specifications (including 3GPP TS 36.300 (“*TS 36.300 Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2, version 11.7.0 Release 11*”, September 2013); 3GPP TS 36.331 (*ETSI TS 136 331; V12.3.0 (2014-09); LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (3GPP TS 36.331 version 12.3.0 Release 12)*); and/or 3GPP TS 36.463 (*3GPP TS 36.463 V0.2.0 (2015-10) Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and Wireless LAN (WLAN); Xw application protocol (XwAP) (Release 13)*)) and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing Wireless-Gigabit-Alliance (WGA) specifications (*Wireless Gigabit Alliance, Inc WiGig MAC and PHY Specification Version 1.1, April 2011, Final specification*) and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing IEEE 802.11 standards (including IEEE 802.11-201 (*IEEE 802.11-2012, IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, March 29, 2012*); and/or IEEE802.11REVmcTM (*IEEE802.11REVmcTM_D3.0, June 2014, Draft Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan*

Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications)), and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing IEEE 802.16 standards (*IEEE-Std 802.16, 2009 Edition, Air Interface for Fixed Broadband Wireless Access Systems*; *IEEE-Std 802.16e, 2005 Edition, Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*; *amendment to IEEE Std 802.16-2009, developed by Task Group m*) and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing *WirelessHD™* specifications and/or future versions and/or derivatives thereof, units and/or devices which are part of the above networks, and the like.

[0021] Some embodiments may be used in conjunction with one or more types of wireless communication signals and/or systems, for example, Radio Frequency (RF), Frequency-Division Multiplexing (FDM), Orthogonal FDM (OFDM), Single Carrier Frequency Division Multiple Access (SC-FDMA), Time-Division Multiplexing (TDM), Time-Division Multiple Access (TDMA), Extended TDMA (E-TDMA), General Packet Radio Service (GPRS), extended GPRS, Code-Division Multiple Access (CDMA), Wideband CDMA (WCDMA), CDMA 2000, single-carrier CDMA, multi-carrier CDMA, Multi-Carrier Modulation (MDM), Discrete Multi-Tone (DMT), Bluetooth®, Global Positioning System (GPS), Wireless Fidelity (Wi-Fi), Wi-Max, ZigBee™, Ultra-Wideband (UWB), Global System for Mobile communication (GSM), second generation (2G), 2.5G, 3G, 3.5G, 4G, Fifth Generation (5G) mobile networks, 3GPP, Long Term Evolution (LTE) cellular system, LTE advance cellular system, High-Speed Downlink Packet Access (HSDPA), High-Speed Uplink Packet Access (HSUPA), High-Speed Packet Access (HSPA), HSPA+, Single Carrier Radio Transmission Technology (1XRTT), Evolution-Data Optimized (EV-DO), Enhanced Data rates for GSM Evolution (EDGE), and the like. Other embodiments may be used in various other devices, systems and/or networks.

[0022] The term “wireless device”, as used herein, includes, for example, a device capable of wireless communication, a communication device capable of wireless communication, a communication station capable of wireless communication, a portable or non-portable device capable of wireless communication, or the like. In some demonstrative embodiments, a wireless device may be or may include a peripheral that is integrated with a computer, or a peripheral that is attached to a computer. In some demonstrative embodiments, the term “wireless device” may optionally include a wireless service.

[0023] The term “communicating” as used herein with respect to a communication signal includes transmitting the communication signal and/or receiving the communication signal. For example, a communication unit, which is capable of communicating a communication signal, may include a transmitter to transmit the communication signal to at least one other communication unit, and/or a communication receiver to receive the communication signal from at least one other communication unit. The verb communicating may be used to refer to the action of transmitting or the action of receiving. In one example, the phrase “communicating a signal” may refer to the action of transmitting the signal by a first device, and may not necessarily include the action of receiving the signal by a second device. In another example, the phrase “communicating a signal” may refer to the action of receiving the signal by a first device, and may not necessarily include the action of transmitting the signal by a second device.

[0024] As used herein, the term “circuitry” may refer to, be part of, or include, an Application Specific Integrated Circuit (ASIC), an integrated circuit, an electronic circuit, a processor (shared, dedicated, or group), and/or memory (shared, dedicated, or group), that execute one or more software or firmware programs, a combinational logic circuit, and/or other suitable hardware components that provide the described functionality. In some embodiments, the circuitry may be implemented in, or functions associated with the circuitry may be implemented by, one or more software or firmware modules. In some embodiments, circuitry may include logic, at least partially operable in hardware.

[0025] The term “logic” may refer, for example, to computing logic embedded in circuitry of a computing apparatus and/or computing logic stored in a memory of a computing apparatus. For example, the logic may be accessible by a processor of the computing apparatus to execute the computing logic to perform computing functions and/or operations. In one example, logic may be embedded in various types of memory and/or firmware, e.g., silicon blocks of various chips and/or processors. Logic may be included in, and/or implemented as part of, various circuitry, e.g. radio circuitry, receiver circuitry, control circuitry, transmitter circuitry, transceiver circuitry, processor circuitry, and/or the like. In one example, logic may be embedded in volatile memory and/or non-volatile memory, including random access memory, read only memory, programmable memory, magnetic memory, flash memory, persistent memory, and the like. Logic may be executed by one or more processors using memory, e.g., registers, stacks, buffers, and/or the like, coupled to the one or more processors, e.g., as necessary to execute the logic.

[0026] The term “antenna”, as used herein, may include any suitable configuration, structure and/or arrangement of one or more antenna elements, components, units, assemblies and/or arrays. In some embodiments, the antenna may implement transmit and receive functionalities using separate transmit and receive antenna elements. In some embodiments, the antenna may implement transmit and receive functionalities using common and/or integrated transmit/receive elements. The antenna may include, for example, a phased array antenna, a single element antenna, a dipole antenna, a set of switched beam antennas, and/or the like.

[0027] The term “cell”, as used herein, may include a combination of network resources, for example, downlink and optionally uplink resources. The resources may be controlled and/or allocated, for example, by a node (also referred to as a “base station”), or the like. The linking between a carrier frequency of the downlink resources and a carrier frequency of the uplink resources may be indicated in system information transmitted on the downlink resources.

[0028] Some demonstrative embodiments are described herein with respect to a LTE network. However, other embodiments may be implemented in any other suitable cellular network or system, e.g., a Universal Mobile Telecommunications System (UMTS) cellular system, a GSM network, a 3G cellular network, a 4G cellular network, a 4.5G network, a 5G cellular network, a WiMAX cellular network, and the like.

[0029] Some demonstrative embodiments are described herein with respect to a WLAN system, a WiFi system, and/or a WiGig system. However, other embodiments may be implemented in any other suitable non-cellular network.

[0030] Some demonstrative embodiments are described herein with respect to a WLAN Termination (WT) node. However, other embodiments may be implemented in any other WLAN controller, WLAN access device, WLAN Access Point (AP), WLAN access controller (AC), and/or WLAN access manager, node, and/or interface.

[0031] Some demonstrative embodiments may be used in conjunction with a Heterogeneous Network (HetNet), which may utilize a deployment of a mix of technologies, frequencies, cell sizes and/or network architectures, e.g., including cellular, millimeter wave (“mmWave” or “mmW”), and/or the like. In one example, the HetNet may include a radio access network having layers of different-sized cells ranging from large macrocells to small cells, for example, picocells and femtocells. Other embodiments may be used in conjunction with any other suitable wireless communication network.

[0032] Other embodiments may be used in conjunction with any other suitable wireless communication network.

[0033] Reference is now made to Fig. 1, which schematically illustrates a block diagram of a system 100, in accordance with some demonstrative embodiments.

5 [0034] As shown in Fig. 1, in some demonstrative embodiments, system 100 may include one or more wireless communication devices capable of communicating content, data, information and/or signals via one or more wireless mediums (WM) 108. For example, system 100 may include at least one User Equipment (UE) 102 capable of communicating with one or more wireless communication networks, e.g., as described below.

10 [0035] Wireless mediums 108 may include, for example, a radio channel, a cellular channel, an RF channel, a WiFi channel, an IR channel, and the like. One or more elements of system 100 may optionally be capable of communicating over any suitable wired communication links.

[0036] In some demonstrative embodiments, system 100 may include at least one cellular
15 manager 104 to manage communication of a cellular network, e.g., as described below.

[0037] In some demonstrative embodiments, cellular manager 104 may include, may operate as, and/or may perform the functionality of, an Evolved Node B (eNB). For example, cellular manager 104 may be configured to perform radio resource management (RRM), radio bearer control, radio admission control (access control), connection mobility
20 management, resource scheduling between UEs and eNB radios, e.g., Dynamic allocation of resources to UEs in both uplink and downlink, header compression, link encryption of user data streams, packet routing of user data towards a destination, e.g., another eNB or an Evolved Packet Core (EPC), scheduling and/or transmitting paging messages, e.g., incoming calls and/or connection requests, broadcast information coordination, measurement reporting,
25 and/or any other operations, communications, and/or functionality.

[0038] In other embodiments, cellular manager 104 may include any other functionality and/or may perform the functionality of any other cellular node, network controller, base station or any other node or network device.

[0039] In one example, cellular manager 104 may be part of a UMTS. According to this
30 example, cellular manager 104 may perform the functionality of a Radio Network Controller (RNC), which may control a plurality of Node B devices 157. For example, the node B may be configured to communicate directly with UEs, e.g., including UE 102, for example, using

a Wideband Code Division Multiple Access (WCDMA) and/or Time Division Synchronous Code Division Multiple Access (TD-SCDMA) air interface technology. The RNC may include, for example, a UMTS RNC configured to control the Node B devices 157.

[0040] In some demonstrative embodiments, system 100 may include a WLAN Termination (WT) node 106, which may be configured to terminate a WLAN network interface, e.g., as described herein.

[0041] Some demonstrative embodiments are described below with respect to a WT node to terminate a WLAN network interface. In other embodiments and additional or alternative termination node may be used to terminate a network interface of any other non-cellular RAT network, for example, a Bluetooth network, a millimeter wave (mmWave) network, and/or any other network, e.g., in addition to or instead of the WLAN network.

[0042] In some demonstrative embodiments, WT node 106 may be configured to manage access to a non-cellular network 107, for example, a WLAN, e.g., a Service Set (SS), a Basic Service Set (BSS), and Extended Service Set, a Homogenous Extended Service Set (HESS), and the like.

[0043] In some demonstrative embodiments, one or more functionalities of WT node 106 may be implemented, for example, in the form of, or as part of, a WLAN access device, for example, as part of a WLAN Access Point (AP), or a WLAN Access Controller (AC), as part of another device, or as a standalone device.

[0044] In other embodiments, WT node 106 may perform any other functionality and/or may perform at least part of the functionality of any other device capable of controlling and/or managing WLAN radio access to one or more wired networks.

[0045] In one example, WT node 106 may include, operate as, and/or perform the functionality of, an AP, e.g., configured to communicate directly with UE 102 via a WLAN link.

[0046] In another example, WT node 106 may include, operate as, and/or perform the functionality of, an AC. According to this example, WT node 106 may control a plurality of AP devices, e.g., including Lightweight Access Point (LAP) devices 158.

[0047] In some demonstrative embodiments, UE 102 may include, for example, a Mobile Device (MD), a Station (STA), a mobile computer, a laptop computer, a notebook computer, a tablet computer, an Ultrabook™ computer, an Internet of Things (IoT) device, a wearable

device, a sensor device, a mobile internet device, a handheld computer, a handheld device, a storage device, a PDA device, a handheld PDA device, an on-board device, an off-board device, a hybrid device (e.g., combining cellular phone functionalities with PDA device functionalities), a consumer device, a vehicular device, a non-vehicular device, a mobile or portable device, a mobile phone, a cellular telephone, a PCS device, a mobile or portable GPS device, a DVB device, a relatively small computing device, a non-desktop computer, a “Carry Small Live Large” (CSLL) device, an Ultra Mobile Device (UMD), an Ultra Mobile PC (UMPC), a Mobile Internet Device (MID), an “Origami” device or computing device, a video device, an audio device, an A/V device, a gaming device, a media player, a Smartphone, or the like.

[0048] In some demonstrative embodiments, system 100 may include at least one WLAN AP 119. In some demonstrative embodiments, WT node 106 may include, may operate as, and/or may perform one or more functionalities of WLAN AP 119, e.g., as described below. In other embodiments, WLAN AP 119 and WT node 106 may be implemented as two separate and/or independent units, elements, device and/or entities of system 100, e.g., as described below.

[0049] In some demonstrative embodiments, UE 102, cellular manager 104, WT node 106, and/or WLAN AP 119 may include one or more communication interfaces to perform communication between UE 102, cellular manager 104, WT node 106, WLAN AP 119, and/or with one or more other wireless communication devices, e.g., as described below.

[0050] Some demonstrative embodiments include an interface 199 (also referred to as “the access device interface”, “the horizontal interface”, “the “Xw interface”, “the X2-W interface” or “the cellular/WLAN interface”), which may include circuitry and/or logic configured to interface, e.g., directly or indirectly, between a cellular network element, e.g., cellular manager 104, and a WLAN element, e.g., WT node 106, as described in detail below.

[0051] In some demonstrative embodiments, interface 199 may be implemented to interface between an eNB and a WT node, e.g., as described below. However, in other embodiments, the cellular/WLAN interface 199 may be implemented to directly interface between any other cellular device and any other WLAN device. In one example, the cellular/WLAN interface 199 may be implemented to directly interface between an eNB and a WLAN AP or WLAN AC, e.g., WLAN AP 119. In another example, the cellular/WLAN interface 199 may be implemented to directly interface between a UMTS RNC and a WT node. In another

example, the cellular/WLAN interface 199 may be implemented to directly interface between a UMTS RNC and a WLAN AP or AC, e.g., WLAN AP 119.

[0052] In some demonstrative embodiments, interface 199 may be utilized to enhance and/or increase the efficiency of interworking, integration and/or management of the cellular and WLAN radio access technologies.

[0053] In some demonstrative embodiments, interface 199 may be configured to perform and/or support one or more aggregation operations and/or functionalities, for example, to transfer traffic, e.g., in addition to transferring control plane information.

[0054] In some demonstrative embodiments, interface 199 may be utilized to improve efficiency of resource management, to provide efficient load balancing, and/or to improve mobility between Radio Access Technology (RAT) networks.

[0055] In some demonstrative embodiments, cellular manager 104 may include an interface (“Core Network (CN) interface”) 146, e.g., a vertical interface, including circuitry and/or logic configured to communicate with one or more elements of a CN 183, e.g., an Evolved Packet Core (EPC).

[0056] In some demonstrative embodiments, CN interface 146 may include an S1 vertical interface configured to communicate between cellular manager 104 and a Serving Gateway (S-GW) 185 according to an S1 protocol, e.g., if cellular manager 104 performs the functionality of an eNB. According to this example, S-GW 187 may interface between cellular manager 104 and a Packet Data Network (PDN) Gateway (P-GW) 187.

[0057] In other embodiments, CN interface 146 may include any other vertical interface with one or more elements of CN 183. For example, cellular manager 104 may perform the functionality of an RNC, e.g., in a UMTS system. According to this example, CN interface 146 may include an Interface Unit Circuit Switch (Iu-CS) interface and/or an Interface Unit Packet Switch (Iu-PS) interface, to interface between the RNC and one or more packet-switched or circuit-switched CN elements.

[0058] In some demonstrative embodiments, cellular manager 104 may include an interface including circuitry and/or logic to communicate user plane traffic, directly or indirectly, between CN 183 and UE 102.

[0059] In some demonstrative embodiments, cellular manager 104 may communicate the user plane traffic directly with UE 102, for example, if cellular manager 104 performs the

functionality of an eNB. According to these embodiments, cellular manager 104 may include an air interface, for example, a cellular transceiver (TRx) 167, including circuitry and/or logic configured to communicate with UE 102 via a cellular link.

[0060] In other embodiments, cellular manager 104 may communicate the user plane traffic with UE 102 via Node B 157, e.g., if cellular manager 104 performs the functionality of an RNC. According to these embodiments, cellular manager 104 may include a Node B interface 161 to communicate between the RNC and Node B 157. For example, Node B interface 161 may include an Interface Unit b (Iub).

[0061] In some demonstrative embodiments, cellular manager 104 may include a WT node interface 169 (also referred to as “WLAN interface” or “WLAN control interface”) including circuitry and/or logic configured to communicate with WT node 106 and/or with one or more WLAN stations (STAs), e.g., as described below. In one example, interface 169 may include an AP interface, e.g., if WT node 106 performs the functionality of an AP. In another example, interface 169 may include an AC interface, e.g., if WT node 106 performs the functionality of an AC. In another example, interface 169 may include any other non-cellular RAT interface to communicate with a node of a non-cellular RAT network.

[0062] In some demonstrative embodiments, WT node 106 may include a cell manager interface (“the cellular interface”) 192 including circuitry and/or logic configured to communicate with cellular manager 104. In one example, interface 192 may include an eNB interface, e.g., if cellular manager 104 performs the functionality of an eNB. In another example, interface 192 may include a RNC interface, e.g., if cellular manager 104 performs the functionality of a RNC.

[0063] In some demonstrative embodiments, interfaces 169 and 192 may be configured to communicate between cellular manager 104 and WT node 106 via a direct link of interface 199.

[0064] In some demonstrative embodiments, interface 199 may include a Point-to-Point (P2P) link, e.g., as described below.

[0065] In some demonstrative embodiments, interface 199 may be implemented by any wired and/or wireless link, e.g., using any suitable, Physical Layer (PHY) components and/or protocols.

[0066] In some demonstrative embodiments, WT node 106 may include a network interface 196 including circuitry and/or logic configured to communicate network traffic with a wired network 177, e.g., the Internet and/or any other network.

[0067] In some demonstrative embodiments, WT node 106 may include a WLAN interface 193 including circuitry and/or logic configured to communicate the network traffic and/or any other traffic with UE 102 via a WLAN, directly or indirectly.

[0068] In some demonstrative embodiments, WT node 106 may communicate directly with UE 102 via WLAN link, for example, if WT node 106 includes, operates as, or performs the functionality of, a WLAN AP 119. According to these embodiments, WLAN interface 193 may include a WLAN radio 194 including circuitry and/or logic configured to communicate the network traffic and/or any other traffic directly with UE 102, e.g., via a WLAN link between WT node 106 and UE 102, for example, if WT node 106 includes, operates as, or performs the functionality of, a WLAN AP 119.

[0069] In some demonstrative embodiments, WT node 106 may indirectly communicate with UE 102, for example, if WT node 106 performs the functionality of an AC, or if WT node 106 is an entity, which is separate from the WLAN AC or WLAN AP. According to these embodiments, WLAN interface 193 may include, for example, an AP interface, e.g., a LAP interface 159, to communicate the network traffic and/or any other traffic with WLAN AP 119 and/or LAP 158.

[0070] In some demonstrative embodiments, WLAN interface 193 may include any other additional or alternative interfaces to directly and/or indirectly communicate via the WLAN.

[0071] In some demonstrative embodiments, UE 102 may include a non-cellular RAT transceiver (TRx), for example, a WLAN TRx 163, including circuitry and/or logic configured to communicate with a WLAN device, e.g., with WLAN AP 119, WT node 106 and/or with LAP 158, via the WLAN link. Some embodiments are described below with respect to a UE, e.g., UE 102, including a WLAN TRx to communicate over a WLAN. In other embodiments, the UE may include any additional or alternative non-cellular RAT TRx, e.g., a Bluetooth TRx and/or any other TRx, to communicate over any additional or alternative non-cellular RAT network.

[0072] In some demonstrative embodiments, UE 102 may include a cellular transceiver (TRx) 165 including circuitry and/or logic configured to communicate with a cellular

network, for example, via a cellular device, e.g., cellular manager 104 and/or Node B 157, via the cellular link.

[0073] In some demonstrative embodiments, WLAN AP 119 may include a network interface 121 including circuitry and/or logic configured to communicate with at least one network node. In one example, network interface 121 may include a WT node interface to communicate with WT node 106. In another example, network interface 121 may include cellular manager interface to communicate with cellular manager 104, e.g., via interface 199, for example, if WLAN AP 119 is implemented by and/or collocated with WT node 106.

[0074] In some demonstrative embodiments, WLAN AP 119 may include a WLAN TRx 122 including circuitry and/or logic configured to communicate traffic with UE 102, e.g., via a WLAN link between WLAN AP 119 and UE 102.

[0075] In some demonstrative embodiments, WLAN TRx 163, cellular TRx 165, cellular TRx 167, WLAN TRx 122, and/or WLAN radio 194 may include one or more wireless transmitters, receivers and/or transceivers including circuitry and/or logic to process, encode, decode, send and/or receive wireless communication signals, RF signals, frames, blocks, transmission streams, packets, messages, data items, and/or data.

[0076] In some demonstrative embodiments, WLAN TRx 167, WLAN TRx 122, and/or WLAN radio 194 may include one or more wireless receivers (Rx) including circuitry and/or logic to receive wireless communication signals, RF signals, frames, blocks, transmission streams, packets, messages, data items, and/or data; and/or one or more wireless transmitters (Tx) including circuitry and/or logic to send wireless communication signals, RF signals, frames, blocks, transmission streams, packets, messages, data items, and/or data. For example, WLAN TRx 167, WLAN TRx 122, and/or WLAN radio 194 may include circuitry; logic; Radio Frequency (RF) elements, circuitry and/or logic; baseband elements, circuitry and/or logic; modulation elements, circuitry and/or logic; demodulation elements, circuitry and/or logic; amplifiers; analog to digital and/or digital to analog converters; filters; and/or the like.

[0077] In some demonstrative embodiments, cellular TRx 167 and/or cellular TRx 165 may include a multiple input multiple output (MIMO) transmitters receivers system (not shown), which may be capable of performing antenna beamforming methods, if desired. In other embodiments, cellular TRx 167 and/or cellular TRx 165 may include any other transmitters and/or receivers.

[0078] In some demonstrative embodiments, cellular TRx 167 and/or cellular TRx 165 may include LTE, WCDMA and/or TD-SCDMA modulator and/or demodulator circuitry (not shown) configured to modulate and/or demodulate downlink signals to be communicated over downlink channels, e.g., between cellular manager 104 and UE 102, and/or uplink signals to be communicated over uplink channels, e.g., between UE 102 and cellular manager 104. In other embodiments, cellular TRx 167 and/or cellular TRx 165 may include any other modulators and/or demodulators.

[0079] In some demonstrative embodiments, cellular TRx 167 and/or cellular TRx 165 may include a turbo decoder and/or a turbo encoder (not shown) including circuitry and/or logic for encoding and/or decoding data bits into data symbols, if desired. In some demonstrative embodiments, cellular TRx 167 and/or cellular TRx 165 may include OFDM and/or SC-FDMA modulators and/or demodulators (not shown) configured to communicate OFDM signals over downlink (DL) channels, and/or SC-FDMA signals over uplink (UL) channels.

[0080] In some demonstrative embodiments, UE 102 may establish a WLAN link with WLAN AP 119. For example, WLAN TRx 163 may operate as and/or perform the functionality of one or more STAs, e.g., one or more WiFi STAs, WLAN STAs, and/or DMG STAs. The WLAN link may include an uplink and/or a downlink. The WLAN downlink may include, for example, a unidirectional link from the WLAN AP 119 to the one or more STAs. The uplink may include, for example, a unidirectional link from a STA to the WLAN AP 119.

[0081] In some demonstrative embodiments, WT node 106 may be configured to operate as, and/or perform one or more functionalities of, WLAN AP 119, for example, in a collocated LTE/WLAN aggregation implementation.

[0082] In some demonstrative embodiments, WT node 106 may be configured to control and/or communicate with one or more WLAN APs 119, e.g., a plurality of WLAN APs 119, for example, as described below.

[0083] In some demonstrative embodiments, UE 102, cellular manager 104, WLAN AP 119, and/or WT node 106, may include, or may be associated with, one or more antennas. In one example, WLAN TRx 163 and/or cellular TRx 165 may be associated with at least two antennas, e.g., antennas 112 and 114, or any other number of antennas, e.g., one antenna or more than two antennas; cellular TRx 167 may be associated with at least two antennas, e.g., antennas 132 and 134, or any other number of antennas, e.g., one antenna or more than two

antennas; WLAN radio 194 may be associated with one or more antennas 135; and/or WLAN TRx 122 may be associated with one or more antennas 124.

[0084] In some demonstrative embodiments, antennas 112, 114, 132, 134, 135 and/or 124 may include any type of antennas suitable for transmitting and/or receiving wireless communication signals, blocks, frames, transmission streams, packets, messages and/or data. For example, antennas 112, 114, 132, 134, 124, and/or 135 may include any suitable configuration, structure and/or arrangement of one or more antenna elements, components, units, assemblies and/or arrays. For example, antennas 112, 114, 132, 134, 124, and/or 135 may include a phased array antenna, a dipole antenna, a single element antenna, a set of switched beam antennas, and/or the like.

[0085] In some embodiments, antennas 112, 114, 132, 134, 124, and/or 135 may implement transmit and receive functionalities using separate transmit and receive antenna elements. In some embodiments, antennas 112, 114, 132, 134, 124, and/or 135 may implement transmit and receive functionalities using common and/or integrated transmit/receive elements.

[0086] In some demonstrative embodiments, cellular manager 104 may include at least one controller component 182, UE 102 may include at least one controller component 197, WLAN AP 119 may include at least one controller component 123, and/or WT node 106 may include at least one controller component 149. Controllers 182, 197, 123, and/or 149 may be configured to trigger one or more communications, to generate and/or trigger communication of one or more messages and/or transmissions, and/or to perform one or more functionalities, operations and/or procedures, e.g., as described below.

[0087] In some demonstrative embodiments, controllers 182, 197, 123, and/or 149 may include circuitry and/or logic, e.g., one or more processors including circuitry and/or logic, memory circuitry and/or logic, Media-Access Control (MAC) circuitry and/or logic, Physical Layer (PHY) circuitry and/or logic, and/or any other circuitry and/or logic, configured to perform the functionality of controllers 182, 197, 123, and/or 149, respectively. Additionally or alternatively, one or more functionalities of controllers 182, 197, and/or 149 may be implemented by logic, which may be executed by a machine and/or one or more processors, e.g., as described below.

[0088] In one example, controller 182 may include circuitry and/or logic, for example, one or more processors including circuitry and/or logic, configured to cause, request and/or trigger cellular manager 104 to perform one or more operations, communications and/or

functionalities, e.g., as described herein. In one example, controller 197 may include circuitry and/or logic, for example, one or more processors including circuitry and/or logic, configured to cause, request and/or trigger UE 102 to perform one or more operations, communications and/or functionalities, e.g., as described herein. In one example, controller 123 may include
5 circuitry and/or logic, for example, one or more processors including circuitry and/or logic, configured to cause, request and/or trigger WLAN AP 119 to perform one or more operations, communications and/or functionalities, e.g., as described herein. In one example, controller 149 may include circuitry and/or logic, for example, one or more processors including circuitry and/or logic, configured to cause, request and/or trigger WT node 106 to
10 perform one or more operations, communications and/or functionalities, e.g., as described herein.

[0089] In some demonstrative embodiments, cellular manager 104 may include a message processor 144 configured to generate, process and/or access one or messages communicated by cellular manager 104. In one example, message processor 144 may be configured to
15 generate one or more messages to be transmitted by cellular manager 104, and/or message processor 144 may be configured to access and/or to process one or more messages received by cellular manager 104, e.g., as described below.

[0090] In some demonstrative embodiments, UE 102 may include a message processor 198 configured to generate, process and/or access one or messages communicated by UE 102. In
20 one example, message processor 198 may be configured to generate one or more messages to be transmitted by UE 102, and/or message processor 198 may be configured to access and/or to process one or more messages received by UE 102, e.g., as described below.

[0091] In some demonstrative embodiments, WLAN AP 119 may include a message processor 125 configured to generate, process and/or access one or messages communicated
25 by WLAN AP 119. In one example, message processor 125 may be configured to generate one or more messages to be transmitted by WLAN AP 119, and/or message processor 125 may be configured to access and/or to process one or more messages received by WLAN AP 119, e.g., as described below.

[0092] In some demonstrative embodiments, WT node 106 may include a message processor
30 150 configured to generate, process and/or access one or messages communicated by WT node 106. In one example, message processor 150 may be configured to generate one or more messages to be transmitted by WT node 106, and/or message processor 150 may be

configured to access and/or to process one or more messages received by WT node 106, e.g., as described below.

[0093] In some demonstrative embodiments, message processors 144, 198, 125, and/or 150 may include circuitry, e.g., processor circuitry, memory circuitry, Media-Access Control (MAC) circuitry, Physical Layer (PHY) circuitry, and/or any other circuitry, configured to perform the functionality of message processors 144, 198, 125, and/or 150. Additionally or alternatively, one or more functionalities of message processors 144, 198, 125, and/or 150 may be implemented by logic, which may be executed by a machine and/or one or more processors, e.g., as described below.

[0094] In some demonstrative embodiments, at least part of the functionality of message processor 144 may be implemented as part of cellular TRx 167 and/or WT node interface 169; at least part of the functionality of message processor 198 may be implemented as part of cellular TRx 165 and/or WLAN TRx 163; at least part of the functionality of message processor 125 may be implemented as part of WLAN TRx 122; and/or at least part of the functionality of message processor 150 may be implemented as part of interface 192 and/or interface 193.

[0095] In some demonstrative embodiments, at least part of the functionality of message processor 144 may be implemented as part of controller 182, at least part of the functionality of message processor 198 may be implemented as part of controller 197, at least part of the functionality of message processor 125 may be implemented as part of controller 123, and/or at least part of the functionality of message processor 150 may be implemented as part of controller 149.

[0096] In other embodiments, at least part of the functionality of message processor 144 may be implemented as part of any other element of cellular manager 104, at least part of the functionality of message processor 198 may be implemented as part of any other element of UE 102, at least part of the functionality of message processor 125 may be implemented as part of any other element of WLAN AP 119, and/or at least part of the functionality of message processor 150 may be implemented as part of any other element of WT node 106.

[0097] In some demonstrative embodiments, at least part of the functionality of controller 197, and/or message processor 198 may be implemented by an integrated circuit, for example, a chip, e.g., a System on Chip (SoC). In one example, the chip or SoC may be configured to perform one or more functionalities of cellular transceiver 165 and/or WLAN

TRx 163. For example, the chip or SoC may include one or more elements of controller 197, message processor 198, and/or one or more elements of cellular transceiver 165 and/or WLAN TRx 163. In one example, controller 197, message processor 198, cellular transceiver 163, and WLAN TRx 163 may be implemented as part of the chip or SoC. In other
5 embodiments, controller 197, message processor 198, cellular transceiver 165 and/or WLAN TRx 163 may be implemented by one or more additional or alternative elements of UE 102.

[0098] In some demonstrative embodiments, at least part of the functionality of controller 182 and/or message processor 144 may be implemented by an integrated circuit, for example, a chip, e.g., a System on Chip (SoC). In one example, the chip or SoC may be configured to
10 perform one or more functionalities of cellular transceiver 167 and/or WT node interface 169. For example, the chip or SoC may include one or more elements of controller 182, message processor 144, and/or one or more elements of cellular transceiver 167 and/or WT node interface 169. In one example, controller 182, message processor 144, cellular transceiver 167, and WT node interface 169 may be implemented as part of the chip or SoC. In other
15 embodiments, controller 182, message processor 144, cellular transceiver 167 and/or WT node interface 169 may be implemented by one or more additional or alternative elements of cellular manager 104.

[0099] In some demonstrative embodiments, at least part of the functionality of controller 149 and/or message processor 150 may be implemented by an integrated circuit, for example, a chip, e.g., a System on Chip (SoC). In one example, the chip or SoC may be configured to
20 perform one or more functionalities of WLAN interface 193 and/or cellular manager interface 192. For example, the chip or SoC may include one or more elements of controller 149, message processor 150, and/or one or more elements of WLAN interface 193 and/or cellular manager interface 192. In one example, controller 149, message processor 150, WLAN interface 193, and cellular manager interface 192 may be implemented as part of the
25 chip or SoC. In other embodiments, controller 149, message processor 150, WLAN interface 193 and/or cellular manager interface 192 may be implemented by one or more additional or alternative elements of WT node 106.

[00100] In some demonstrative embodiments, at least part of the functionality of controller 123 and/or message processor 125 may be implemented by an integrated circuit, for example, a chip, e.g., a System on Chip (SoC). In one example, the chip or SoC may be configured to
30 perform one or more functionalities of network interface 121 and/or WLAN TRx 122. For example, the chip or SoC may include one or more elements of controller 123, message

processor 125, and/or one or more elements of WLAN TRx 122 and/or network interface 1212. In one example, controller 123, message processor 125, WLAN TRx 122, and network interface 121 may be implemented as part of the chip or SoC. In other embodiments, controller 123, message processor 125, WLAN TRx 122, and/or network interface 121 may be implemented by one or more additional or alternative elements of WLAN AP 119.

[00101] In some demonstrative embodiments, cellular manager 104, WT node 106, WLAN AP 119, and/or UE 102 may also include, for example, one or more of a processor, an input unit, an output unit, a memory unit, and/or a storage unit. For example, cellular manager 104 may include a processor 173 and/or a memory 174; WT node 106 may include a processor 175 and/or a memory 176; WLAN AP may include a processor 129 and/or a memory 127; and/or UE 102 may include a memory 151, a processor 152, an input unit 153, an output unit 154, and/or a storage unit 155. UE 102, cellular manager 104, WLAN AP 119, and/or WT node 106 may optionally include other suitable hardware components and/or software components. In some demonstrative embodiments, some or all of the components of one or more of UE 102, cellular manager 104, WLAN AP 119, and/or WT node 106 may be enclosed in a common housing or packaging, and may be interconnected or operably associated using one or more wired or wireless links. In other embodiments, components of one or more of UE 102, cellular manager 104, WLAN AP 119, and/or WT node 106 may be distributed among multiple or separate devices.

[00102] In some demonstrative embodiments, processors 173, 175, 129, and/or 152 may include, for example, a Central Processing Unit (CPU), a Digital Signal Processor (DSP), one or more processor cores, a single-core processor, a dual-core processor, a multiple-core processor, a microprocessor, a host processor, a controller, a plurality of processors or controllers, a chip, a microchip, one or more circuits, circuitry, a logic unit, an Integrated Circuit (IC), an Application-Specific IC (ASIC), or any other suitable multi-purpose or specific processor or controller. For example, processor 173 may execute instructions, for example, of an Operating System (OS) of cellular manager 104 and/or of one or more suitable applications; processor 175 may execute instructions of an OS of WT node 106 and/or of one or more suitable applications; processor 129 may execute instructions of an OS of WLAN AP 119 and/or of one or more suitable applications; and/or processor 152 may execute instructions of an OS of UE 102 and/or of one or more suitable applications.

[00103] In some demonstrative embodiments, input unit 153 may include, for example, a keyboard, a keypad, a mouse, a touch-screen, a touch-pad, a track-ball, a stylus, a

microphone, or other suitable pointing device or input device. Output unit 154 includes, for example, a monitor, a screen, a touch-screen, a flat panel display, a Light Emitting Diode (LED) display unit, a Liquid Crystal Display (LCD) display unit, a plasma display unit, one or more audio speakers or earphones, or other suitable output devices.

5 [00104] In some demonstrative embodiments, memory unit 174, 176 and/or 151 may include, for example, a Random Access Memory (RAM), a Read Only Memory (ROM), a Dynamic RAM (DRAM), a Synchronous DRAM (SD-RAM), a flash memory, a volatile memory, a non-volatile memory, a cache memory, a buffer, a short term memory unit, a long term memory unit, or other suitable memory units. Storage unit 155 includes, for example, a
10 hard disk drive, a floppy disk drive, a Compact Disk (CD) drive, a CD-ROM drive, a DVD drive, or other suitable removable or non-removable storage units. For example, memory unit 174 may store data processed by cellular manager 104; memory unit 151 may store data processed by UE 102; memory unit 127 may store data processed by WLAN AP 119; and/or memory unit 176 may store data processed by WT node 106.

15 [00105] In some demonstrative embodiments, UE 102 may be configured to utilize a cellular connection, e.g., a LTE cellular connection or any other cellular connection, to communicate with cellular manager 104, and a WLAN connection, e.g., a WiFi connection, a mmWave connection, a wireless P2P connection, or any other WLAN connection, to communicate with WLAN AP 119, which may be, for example, connected to, implemented by, and/or
20 controlled by WT node 106.

[00106] In some demonstrative embodiments, one or more elements of system 100 may perform the functionality of a HetNet, which may utilize a deployment of a mix of technologies, frequencies, cell sizes and/or network architectures, for example, including cellular, WLAN, and/or the like.

25 [00107] For example, the HetNet may be configured to provide a service through a first wireless communication environment, e.g., a cellular network, and to maintain the service when switching to another communication environment, e.g., WLAN. The HetNet architecture may enable utilizing a mixture of wireless communication environments, e.g., a WLAN environment and a cellular environment, for example, to optimally respond to rapid
30 changes in customer demand, reduce power consumption, reduce cost, increase efficiency and/or achieve any other benefit.

[00108] In one example, system 100 may utilize a Multi-tier, Multi-Radio Access Technology (Multi-RAT) Het-Net architecture, including a tier of small cells, e.g., pico, femto, relay stations, WiFi APs, and the like, overlaid on top of a macro cellular deployment to augment network capacity.

- 5 [00109] In another example, system 100 may utilize Multi-RAT small cells integrating multiple radios such as WiFi and 3GPP air interfaces in a single infrastructure device.

[00110] In other embodiments, system 100 may implement any other architecture and/or deployment.

- 10 [00111] In some demonstrative embodiments, UE 102 and/or cellular manager 104 may be configured to establish one or more Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) Radio Access Bearers (E-RABs) between UE 102 and S-GW 185, e.g., via cellular manager 104.

- 15 [00112] In some demonstrative embodiments, UE 102, cellular manager 104 and/or WT node 106 may be configured to communicate according to a LTE/WLAN protocol aggregation (LWA) scheme, e.g., as described below.

[00113] In some demonstrative embodiments, an LTE/WLAN protocol stack aggregation may be configured to enable LTE interworking with a WLAN protocol stack.

[00114] In some demonstrative embodiments, the LTE/WLAN protocol stack aggregation may be configured to anchor WLAN mobility at the cellular manager 104.

- 20 [00115] In some demonstrative embodiments, cellular manager 104 and/or WT node 106 may be configured according to a network architecture of a non-collocated LTE/WLAN aggregation, e.g., in which cellular manager 104 and WT node 106 are not collocated as part of an integrated device and/or in which interface 199 is not an internal interface.

- 25 [00116] In some demonstrative embodiments, cellular manager 104 and/or WT node 106 may be configured according to a network architecture of a collocated LTE/WLAN aggregation, e.g., in which cellular manager 104 and WT node 106 may be collocated as part of an integrated device and/or in which interface 199 is an internal interface.

- 30 [00117] Current solutions for establishing a secure connection between a WLAN station (STA) and a WLAN AP assume that the connection establishment between the WLAN STA and the WLAN AP is applied over the air, which is a shared media and therefore not secured. Accordingly, current solutions require performing an association procedure and/or an

authentication procedure, for example, before allowing communication of secure traffic between the WLAN AP and the WLAN STA.

[00118] For example, some specifications and/or protocols, for example, the *IEEE 802.11 Specifications*, may define one or more protocols (“the IEEE 802.11 protocols”) for establishing a connection between a WLAN STA, e.g., a mobile UE, and a WLAN AP. The IEEE 802.11 protocols all require the wireless station and the WLAN AP to engage in an authentication process and in an association process, for example, in order to establish security keys to be used for establishing a secure connection between the wireless station and the WLAN AP. For example, the IEEE 802.11 protocols require that both the WLAN STA and the WLAN AP are to support and use complicated algorithms and protocols, for example, such as operations and/or procedures according to *IEEE 802.1X Specifications*, operations and/or procedures according to an Extensible Authentication Protocol (EAP), operations and/or procedures according to Secure Attribute Exchange (SAE) protocols, operations and/or procedures according to Finite Field Cryptography protocols, and/or operations and/or procedures according to Elliptic Curve Cryptography protocols, as well as one or more authentication devices in the network, for example, an Authentication, Authorization, and Accounting (AAA) server.

[00119] In some demonstrative embodiments, UE 102 and WLAN AP 119 may be configured to establish a secure connection, for example, according to an authentication process, which may utilize a security key, for example, a Pairwise Master Key (PMK). For example, the PMK may be used, e.g., during a four-way (4-Way) handshake process, to generate one or more security keys, e.g., one or more Transient Keys (TKs), which may be used to secure communication between UE 102 and WLAN AP 119. For example, UE 102 and/or WLAN AP 119 may be configured to use the security keys to encrypt/decrypt traffic transferred from UE 102 to WLAN AP 119 and/or from WLAN AP 119 to UE 102.

[00120] In some demonstrative embodiments, an LWA scheme may utilize a WLAN authentication procedure, which may, for example, exploit a connection between cellular manager 114 and WLAN AP 119, for example, via an internal interface, e.g., if WLAN AP 119 is collocated with cellular manager 114, or via an external interface, for example, via interface 199, and/or WT node 106.

[00121] In some demonstrative embodiments, cellular manager 104 may be configured to enable a coordination of the PMK to be used by the UE 102 and WLAN AP 119, e.g., as described below.

[00122] In some demonstrative embodiments, controller component 182 may be configured to control transferring of first key information from cellular manager 104 to UE 102 and second key information from cellular manager 104 to WLAN AP 119, e.g., as described below.

[00123] In some demonstrative embodiments, the second key information, which is provided to the WLAN AP 119 may be based on the first key information, which is provided to UE 102, e.g., as described below.

[00124] In some demonstrative embodiments, the first and second key information may be configured to facilitate coordination of a PMK to be used by UE 102 and WLAN AP 119, for example, for a 4-way handshake, e.g., as described below.

[00125] In some demonstrative embodiments, the PMK may include a key, denoted $S-K_{WT}$, which may correspond to WT node 106, e.g., as described below.

[00126] In some demonstrative embodiments, the PMK may be based on a combination of a counter value, e.g., a WT counter provided by WT node 106, and a security key, for example, an eNB key (K_{eNB}), denoted K_{enb} , which may be known to cellular manager 104 and UE 102.

[00127] In some demonstrative embodiments, controller 149 may be configured to cause WT node 106 to send the WT counter to cellular manager 104, e.g., via interface 199. In one example, controller 182 may be configured to retrieve the WT counter from WT node 106, for example, when generating a WT session between cellular node 104 and WT node 106, and/or at one or more additional or alternative instances.

[00128] In some demonstrative embodiments, the first key information provided from cellular manager 104 to UE 102 may include the WT counter. For example, controller 182 may be configured to cause cellular manager 104 to send to UE 102 a message, e.g., a Radio Resource Control (RRC) message, including the WT counter.

[00129] In one example, controller 182 may be configured to cause cellular manager 104 to provide the eNB key to UE 102, e.g., via an RRC message, for example, as part of a handshake, e.g., an LTE handshake, between cellular manager 104 and UE 102.

[00130] In some demonstrative embodiments, controller component 197 may be configured to determine the PMK based on the WT counter provided by cellular manager 104 and the eNB key corresponding to cellular manager 104.

[00131] In some demonstrative embodiments, the second key information provided from cellular manager 104 to WLAN AP 119 may include the PMK.

[00132] In some demonstrative embodiments, controller component 182 may be configured to determine the PMK, e.g., based on the WT counter of WT node 106 and the eNB key corresponding to cellular manager 104.

[00133] In some demonstrative embodiments, controller component 182 may be configured to cause cellular manager 104 to provide the second key information including the PMK to WLAN AP 119, e.g., directly or via WT node 106. For example, controller component 182 may be configured to cause cellular manager 104 to send to WT node 106 a message, e.g., via interface 199, including the PMK and an indication of UE 102, e.g., a MAC address of UE 102, and/or an indication of a WLAN AP, e.g., a MAC address or Service Set Identifier (SSID), by which the PMK is to be used.

[00134] In some demonstrative embodiments, an eNB, e.g., cellular manager 104, may generate a PMK, e.g., the key $S-K_{WT}$, to be used for establishing a secure session between a UE, e.g., UE 102, and a WLAN AP, e.g., WLAN AP 119, for example, based on a K_{eNB} of the eNB, and a WT Counter, e.g., a WT counter of WT node 106 connecting between the eNB and the WLAN AP.

[00135] In some demonstrative embodiments, the eNB, e.g., cellular manager 104, may be configured to transfer the key $S-K_{WT}$ to the WT node, e.g., WT node 106, which may provide the key $S-K_{WT}$ to the WLAN AP, e.g., WLAN AP 119.

[00136] In some demonstrative embodiments, the eNB, e.g., cellular manager 104, may transfer the WT counter to the UE 102, e.g., using an RRC protocol, and the UE 102 may derive the key $S-K_{WT}$, e.g., independently, for example, based on the key $S-K_{WT}$ and the K_{eNB} of the eNB.

[00137] In some demonstrative embodiments, the key $S-K_{WT}$ may be used as a PMK by the UE, e.g., UE 102, and the WLAN AP, e.g., WLAN AP 119, for WLAN authentication, for example, when establishing a LWA session between the UE, e.g., UE 102, and the eNB, e.g., cellular manager 104, via the WLAN AP, e.g., WLAN AP 119.

[00138] In some demonstrative embodiments, the coordination and/or synchronization of the key $S\text{-}K_{WT}$ to be used at the UE 102 and the WLAN AP 119 may enable to at least to eliminate a time consuming IEEE 802.1X authentication process, for example, while allowing to only use a 4-way handshake process for generating one or more actual security keys, e.g., the TKs, to secure the communication between the WLAN AP 119 and the UE 102.

[00139] In some demonstrative embodiments, when a LWA session is established using a first version of the PMK, it may be preferred to select not to generate, and/or to select not to use, a new or second version of the PMK during the active LWA session, e.g., as discussed below.

[00140] In some demonstrative embodiments, in some cases, generation of a new K_{eNB} may be triggered, for example, based on or after handover of a UE, e.g., an intra-eNB handover or inter-eNB handover. For example, an intra-eNB handover may include a handover of a UE from a first cell to a second cell within a same eNB. For example, an inter-eNB handover may include handover of a UE from a first cell of a first eNB to a second cell of a second eNB. The inter-eNB handover and/or the intra-eNB handover may trigger generating a new K_{eNB} for the UE being handed over.

[00141] In other embodiments, generation of a new K_{eNB} may be triggered by an eNB based on any other additional or alternative event and/or for any other reason. In one example, an eNB may generate a new K_{eNB} , for example, to periodically refresh the K_{eNB} .

[00142] In some demonstrative embodiments, a first eNB (also referred to as “eNodeB#1”), e.g., a first cellular manager 104, may generate a PMK, for example, based on a K_{eNB} of the eNodeB#1 and a WT counter. The eNodeB#1 may, for example, transfer the PMK to be provided to WLAN AP 119, e.g., by directly providing the PMK to WLAN AP 119, e.g., if the WLAN AP 119 is collocated with the eNodeB#1, or by providing the PMK to the WT node 106 connected to the WLAN AP 119, e.g., if the WLAN AP 119 is not collocated with the eNodeB#1.

[00143] In some demonstrative embodiments, the eNodeB#1 may provide the WT counter to UE 102, e.g., via RRC signaling.

[00144] In some demonstrative embodiments, UE 102, which may have possession of the K_{eNB} of the eNodeB#1, may be able to derive the PMK, e.g., independently, for example, upon LWA activation by the eNodeB#1, and based on the reception of the WT counter.

[00145] In some demonstrative embodiments, for example, once the same PMK is set at WLAN AP 119 and UE 102, the UE 102 and the WLAN AP 119 may start a 4-way handshake process, for example, to generate one or more security keys, e.g., a set of transient keys, which may be used by UE 102 and/or WLAN AP 119 for encryption and/or decryption processes, for example, to secure communication over a WLAN link between WLAN AP 119 and UE 102, e.g., during a LWA session of UE 102 via WLAN AP 119.

[00146] In some demonstrative embodiments, generation of a new K_{eNB} may be triggered, for example, by the eNodeB#1, for example, as a result of an inter-eNB handover or for any other reason; or by a second eNB (also referred to as “eNodeB#2”), e.g., a second cellular manager 104, for example, as a result of an intra-eNB handover.

[00147] For example, following an inter-eNB handover process from the eNodeB#1 to the eNodeB#2, the eNodeB#2 may be in charge of the LWA connection of UE 102.

[00148] In some demonstrative embodiments, it may not be advantageous to have the eNodeB#2 generate a new PMK for UE 102 and WLAN AP 119, e.g., based on a K_{eNB} of the eNodeB#2, and/or to have the UE 102 and the WLAN AP 119 use the new PMK. For example, providing the new PMK to WLAN AP 119 and/or UE 102 may trigger a re-association and/or re-keying process at the WLAN AP 119 and/or the UE 102, which may result in packet loss and/or service degradation.

[00149] In some demonstrative embodiments, it may not be advantageous to generate a new $S-K_{WT}$ and/or PMK at the eNB, and/or to use the new $S-K_{WT}$ and/or PMK at the UE and the WLAN AP, for example, when a LWA is active, for example, even when generation of a new K_{eNB} is triggered, e.g., as discussed below.

[00150] In some demonstrative embodiments, it may not be easy to ensure that the WLAN AP 119 and the UE 102 start using the new PMK at the same time. Accordingly, generating and/or using a new PMK during an active LWA session of UE 102 via WLAN AP 119 may require deactivating the LWA, for example, before switching to use the new PMK, e.g., before handover, and potentially re-activating the LWA, e.g., after handover, to enable to use the new PMK.

[00151] However, the deactivation of the LWA may result at least in service degradation, for example, as LTE capacity without the WLAN connection may be degraded.

[00152] For example, requiring that a new $S-K_{WT}$ and/or PMK is to be generated and used based on when a new K_{eNB} is generated, may result in the WLAN AP and the UE starting a

re-association or re-keying process in order to be able to use the new $S-K_{WT}$ and/or PMK. However, the re-association process may be long, and may result in service degradation. Although a re-keying process may be faster, if the re-keying process is not synchronized between the WLAN AP and the UE some packet loss may occur, as the WLAN AP may
5 buffer and send packets encrypted with old transient keys, which are based on the old PMK. Although in theory, multiple key identifiers may be used for different keys, e.g., for the old and the new keys, in practice this may be rarely implemented. In addition, using the multiple key identifiers may require a complicated synchronization mechanism when roaming between WLAN APs, as each WLAN AP may need to be aware of the key identifier that was
10 used by the previous WLAN AP.

[00153] In some demonstrative embodiments, cellular manager 104, UE 102, WT node 106, and/or WLAN AP 119 may be configured to implement one or more mechanisms, which may be configured to enable, for example, at least a PMK refresh process, which may be more smooth, e.g., with reduced or even no packet loss, e.g., as described below.

15 [00154] In some demonstrative embodiments, cellular manager 104, UE 102, WT node 106, and/or WLAN AP 119 may be configured to selectively defer generating, transferring and/or using key information, e.g., key information of a PMK, while an LWA session of UE 102 via WLAN AP 119 is active, e.g., as described below.

[00155] Some demonstrative embodiments may be implemented, for example, to enhance an
20 LWA scheme, for example, such that a handover, e.g., an LTE handover, may not require LWA deactivation, which, as a result, may require WLAN re-association, which in turn may result in packet loss and/or one or more other adverse effects, e.g., including at least effects which may be noticeable to a user.

[00156] Some demonstrative embodiments may be implemented, for example, to allow intra-
25 eNB handover (HO) and/or inter-eNB HO, for example, while reducing and/or avoiding packet loss on a WLAN link of an active LWA session, e.g., as described below.

[00157] In some demonstrative embodiments, an LWA session may be established between an eNB, e.g., cellular manager 104, and a UE, e.g., UE 102, via a WLAN AP, e.g., WLAN AP 119. For example, the UE, e.g., UE 102, and the WLAN AP, e.g., WLAN AP 119, may
30 establish a secure WLAN connection based a first version of a PMK (“the old PMK” or “the current PMK”), which may be facilitated by the eNB.

[00158] In some demonstrative embodiments, the eNB, e.g., cellular manager 104, may be configured to keep both the WLAN AP, e.g., WLAN AP 119, and the UE, e.g., UE 102, “in the blind” regarding a second version of the PMK (“the new PMK”), for example, as long as the LWA session is active, e.g., as described below.

5 [00159] In some demonstrative embodiments, the eNB, e.g., cellular manager 104, may be configured to differ transferring to both the WLAN AP, e.g., WLAN AP 119, and the UE, e.g., UE 102, key information, which may trigger the new PMK, e.g., as described below. Accordingly, the eNB may allow the UE and the WLAN AP to continue using the same transient-keys, which were generated based on the old PMK, for example, for
10 encryption/decryption of traffic of the LWA session.

[00160] In some demonstrative embodiments, deferring the transferring of the key information to the WLAN AP 119 and the UE 102 may enable to defer a rekeying process to generate new transient keys. Accordingly, deferring the transferring of the key information to the WLAN AP 119 and the UE 102 may enable to maintain the LWA session active, for
15 example, even if the eNB 104 is to generate new key information, e.g., a new K_{eNB} .

[00161] In one example, the new key information may be generated when the UE remains connected to the same WLAN AP 119, e.g., at an intra-eNB HO of a collocated LWA use case, in which the eNB 104 and the WLAN AP 119 are collocated or integrated at the same device. In another example, the new key information may be generated at an inter-eNB HO
20 between two eNBs, which are connected to the same WLAN AP 119.

[00162] In some demonstrative embodiments, cellular node 104, WT node 106, WLAN AP 119 and/or UE 102 may be configured to defer a generation, modification and/or updating of one or more security keys, e.g., one or more transient keys, to secure communication over the WLAN link between WLAN AP 119 and UE 102, for example, when the LWA session of
25 UE 102 via WLAN AP 119 is active, e.g., as described below.

[00163] In some demonstrative embodiments, cellular node 104, WLAN AP 119, WT node 106, and/or UE 102 may be configured to enable not to generate, modify and/or update the one or more security keys, for example, even as long as during a lifetime of the LWA session, e.g., as described below.

30 [00164] In some demonstrative embodiments, cellular node 104, WLAN AP 119, WT node 106, and/or UE 102 may be configured to enable not to generate, modify and/or update the one or more security keys, e.g., the TKs, for example, even during an inter-NB or intra-eNB

handover of the UE 102, and/or even in response to generation of a new version of the new K_{eNB} , which may be different from the version of the K_{eNB} , which was used for generating the PMK, based on which the security keys, e.g., the TKs, were generated by UE 102 and WLAN AP 119.

5 [00165] In some demonstrative embodiments, an eNB, e.g., cellular manager 104, may be configured to selectively defer transferring an updated version of key information to a UE and a WLAN AP, e.g., while an LWA session of the UE via the WLAN AP is active, e.g., as described below. According to these embodiments, for example, the WLAN AP and/or the UE may be unaware of an updated version of the key information, e.g., as long as the updated
10 version of the key information is not transferred from the eNB. Accordingly, the UE and WLAN AP may continue to use the same security keys, e.g., transient keys, to secure traffic communicated between the UE and the WLAN AP, for example, without the need to trigger a re-association process and/or a re-keying process.

[00166] In some demonstrative embodiments, for example, when UE 102 is handed over
15 from the eNodeB# 1 to the eNodeB#2, for example, while UE 102 remains connected to the same WLAN AP 119, the WLAN AP 119 and the UE 102 may be allowed to continue using the same TKs that were generated during the initial 4-way handshake process based on the K_{eNB} and the PMK provided by the eNodeB#1.

[00167] In some demonstrative embodiments, cellular node 104, WT node 106, UE 102,
20 and/or WLAN AP 119 may be configured to cause and/or allow WLAN AP 119 and UE 102 to use the K_{eNB} and the PMK, for example, only during the initial 4-way handshake process for the generation of the transient keys of the LWA session.

[00168] In some demonstrative embodiments, cellular node 104, UE 102, WT node 106,
and/or WLAN AP 119 may be configured to allow not to regenerate, modify and/or update
25 the transient keys of the LWA session, for example, even as long as the LWA session is active.

[00169] In some demonstrative embodiments, cellular node 104, UE 102, WT node 106,
and/or WLAN AP 119 may be configured to allow WLAN AP 119 and UE 102 to be
agnostic to any PMK modifications, for example, even if the eNB has changed, e.g., due to
30 an intra-eNB handover.

[00170] In some demonstrative embodiments, an eNB, e.g., cellular manager 104, may be configured to select not to generate a new PMK for UE 102, for example, as long as there is an active LWA session for UE 102 via WLAN AP 119.

[00171] In some demonstrative embodiments, an eNB, e.g., cellular manager 104, may be configured to, even if a new PMK is generated for UE 102, select to defer updating WLAN AP 119 and/or UE 102 on the new PMK, for example, as long as the LWA session of UE 102 via WLAN AP 119 is active.

[00172] In some demonstrative embodiments, an eNB, e.g., cellular manager 104, may be configured to update WLAN AP 119 and/or UE 102 on a new PMK, for example, only before or during LWA session establishment.

[00173] In some demonstrative embodiments, cellular manager 104 may be configured to selectively defer updating WLAN AP 119 and/or UE 102 on a new PMK, e.g., as described above, for example, at an intra-eNB handover when UE 102 remains connected to the same WLAN AP 119, for example, at a collocated implementation having the eNB is integrated with the WLAN AP.

[00174] In some demonstrative embodiments, controller component 182 may be configured to control selective transfer of first key information from cellular node 104 to UE 102 and second key information from cellular node 104 to WLAN AP 119.

[00175] In some demonstrative embodiments, the second key information may be based on the first key information, e.g., as described above.

[00176] In one example, the first key information may include a WT counter, e.g., corresponding to WT node 106, and the second key information may be based on the WT counter and an eNB key of cellular node 104. For example, the second key information may include a PMK based on the eNB key and the WT counter, e.g., as described above.

[00177] In some demonstrative embodiments, controller component 182 may be configured to select to defer transferring of the first key information to the UE 102 and the second key information to the WLAN AP 119, for example, when an active LWA session of the UE 102 is ongoing via the WLAN AP 119, e.g., as described above.

[00178] In some demonstrative embodiments, controller component 182 may be configured to select to defer transferring of the first key information to the UE 102 and the second key information to the WLAN AP 119, when the first and second key information are based on an

eNB key generated by the eNB 104 after establishment of the LWA session of UE 102 via WLAN AP 119, e.g., as described above.

[00179] In some demonstrative embodiments, controller component 182 may be configured to, prior to establishment of the LWA session, cause the eNB 104 to transfer a first version of the first key information to the UE 102 and a first version of the second key information to the WLAN AP 119, e.g., as described above.

[00180] In some demonstrative embodiments, controller component 182 may be configured to defer transferring a second version of the first key information, which supersedes the first version of the first key information, to the UE 102 and a second version of the second key information, which supersedes the first version of the second key information, to the WLAN AP 119, for example, at least as long as the LWA session is active, e.g., as described above.

[00181] In some demonstrative embodiments, the LWA session may include a session handed over to the eNB 104 from another eNB, for example, according to an intra-eNB handover, e.g., as described above. For example, controller component 182 may be configured to defer transferring of the first key information to the UE 102 and the second key information to the WLAN AP 119, when the first and second key information are to be determined based on the eNB key of eNB 104, e.g., after the handover of UE 102 from another eNB to eNB 104.

[00182] In some demonstrative embodiments, controller component 182 may be configured to defer transferring the first key information to the UE 102 and/or the second key information to the WLAN AP 119, for example, at least as long as the LWA session is active, e.g., as described above. In other embodiments, controller component 182 may be configured to defer transferring the first key information to the UE 102 and/or the second key information to the WLAN AP 119 for any other shorter or longer duration.

[00183] Reference is made to Fig. 2, which schematically illustrates operations and communications between a UE 204, a first eNB 203 (eNodeB#1), a second eNB 233 (eNodeB#2), and a WLAN AP 219, in accordance with some demonstrative embodiments.

[00184] In some demonstrative embodiments, as shown in Fig. 2, eNB 203 may include an LTE component 202, which may be configured to communicate with a WT node 206, e.g., a router, via an interface 210, e.g., an Xw interface; and/or eNB 233 may include an LTE component 232, which may be configured to communicate with WT node 206 via an interface 240, e.g., an Xw interface.

[00185] In some demonstrative embodiments, WT node 206 may be configured to control and/or communicate with one or more WLAN APs, e.g., WLAN AP 219.

[00186] In one example, LTE component 202 may perform one or more roles and/or functionalities of a first cellular manager 104 (Fig. 1), LTE component 232 may perform one or more roles and/or functionalities of a second cellular manager 104 (Fig. 1), WT node 206 may perform one or more roles and/or functionalities of WT node 106 (Fig. 1), WLAN AP 219 may perform one or more roles and/or functionalities of WLAN AP 119 (Fig. 1), and/or interfaces 210 and/or 240 may perform one or more functionalities of interface 199 (Fig. 1).

[00187] In some demonstrative embodiments, LTE component 202 may be configured to communicate with UE 204 via a cellular link 212. For example UE 204 may perform one or more functionalities of UE 102 (Fig. 1).

[00188] In some demonstrative embodiments, as indicated by arrow 262 eNB 203 may trigger UE 204 to set a PMK at UE 204, e.g., based on an eNB key (KeNB#1) of eNB 203, for example, via a secured LTE connection over link 212, e.g., as described above.

[00189] In some demonstrative embodiments, as indicated by arrow 264 eNB 203 may trigger setting the same PMK, which is set at UE 204, at WLAN AP 219, for example, by providing the PMK to WLAN AP 219 via the secured Xw interface 210, e.g., as described above.

[00190] In some demonstrative embodiments, as indicated by block 266, once the PMK is established at WLAN AP 219, WLAN AP 219 may initiate a 4-way handshake with UE 204, for example, to generate one or more Transient-Keys, which are shared between WLAN AP 219 and UE 204, e.g., as described above.

[00191] In some demonstrative embodiments, WLAN AP 219 and UE 204 may start using the transient-keys to secure traffic communicated between UE 204 and WLAN AP 219, e.g., over a WiFi link 239. For example, WLAN AP 219 and UE 204 use the transient keys for encryption and/or decryption, e.g., IEEE 802.11 encryption/decryption, of packets, e.g., PDCP packets, of an LWA session between eNB 203 and UE 204, e.g., as described above.

[00192] In some demonstrative embodiments, eNB 203 may select to refresh the KeNB#1. However, for example, since there is an ongoing session of UE 204 via WLAN AP 219, eNB 203 may select not to generate a new PMK. Accordingly, there may be no need to update the WLAN AP 219 and the UE 204 on the change of the KeNB.

[00193] In some demonstrative embodiments, as indicated by arrow 268, the UE 204 may be handed over from eNB 203 to eNB 233, for example, according to an eNB HO process to enable eNB 233 to replace eNB 203 with respect to UE 204.

[00194] In some demonstrative embodiments, as part of the HO process eNB 233 may be notified that there is already an ongoing LWA session with UE 204. Accordingly, although eNB 233 may use a different or new KeNB (KeNB#2), e.g., instead of the KeNB#1 of eNB 203, the eNB 233 may select not to generate a new PMK for UE 204. Accordingly, there may be no need to update the WLAN AP 219 and the UE 204 on the change of the KeNB.

[00195] Referring back to Fig. 1, in some demonstrative embodiments, cellular node 104 may be configured to perform the selection on whether or not to trigger an update of the security keys between UE 102 and WLAN AP 119, e.g., as described above.

[00196] In some demonstrative embodiments, when an eNB, e.g., cellular manager 104, generates a fresh eNB key and/or PMK, and there is already an established LWA WiFi session of UE 102 via WLAN AP 119, the eNB may select not to update the WLAN AP 119 and/or the UE 102 on the new PMK and/or eNB key, e.g., as described above.

[00197] In some demonstrative embodiments, for example, even if the eNB generates new key information, e.g., a fresh eNB key and/or PMK, and passes the new information to UE 102, WT node 106, and/or WLAN AP 119, the UE 102, WT node 106 and/or the WLAN AP 119 may be configured to select not to use the new information, for example, as long as there is an active LWA WiFi session between the WLAN AP 119 and the UE 102, e.g., as described below. In one example, the new information shall be used, for example, only once the active LWA WiFi session is terminated and a new one is established.

[00198] In some demonstrative embodiments, UE 102 may be configured to select whether to defer an update of the security keys between UE 102 and WLAN AP 119, for example, even if a new version of the first security information is received at UE 102 from cellular node 104, e.g., as described below.

[00199] In some demonstrative embodiments, controller component 197 may be configured to determine a security key based on a first version of key information from an eNB, e.g., cellular mode 104, and, based on the security key, to determine one or more shared keys to secure communication with WLAN AP 119 during the LWA session via the WLAN AP 119.

[00200] For example, the security key may include the PMK, and the first version of the key information may include the first version of the eNB key from cellular node 104, e.g., as described above.

5 [00201] For example, controller component 197 may be configured to determine the one or more shared keys including one or more TKs, for example, according to a four-way handshake with WLAN AP 119 using the PMK, e.g., as described above.

[00202] In some demonstrative embodiments, controller component 197 may be configured to select to continue to use the shared keys, which are based on the first version of the key information, for example, even when a second version of the key information, which
10 supersedes the first version of the key information, is received from the cellular network during the LWA session via WLAN AP 119.

[00203] In some demonstrative embodiments, the first and second versions of the key information may be received from the same eNB.

[00204] For example, UE 102 may receive from cellular node 104 the first version of the
15 eNB key of cellular node 104, e.g., prior to or during establishment of the LWA session, and UE 102 may receive from cellular node 104 the second version of the eNB key of cellular node 104, for example, while the LWA session via WLAN AP 119 is still active, e.g., as described above.

[00205] In some demonstrative embodiments, the first and second versions of the key
20 information may be received from first and second respective eNBs.

[00206] For example, UE 102 may receive from a first cellular node 104 the first version of the eNB key of a first eNB 104, e.g., prior to or during establishment of the LWA session, and UE 102 may receive from a second eNB 104 the second version of the eNB key of the
25 second eNB 104, for example, subsequent to a session handover of the LWA session to the second eNB 104.

[00207] In some demonstrative embodiments, controller component 197 may be configured to select to continue to use the shared keys, which are based on the first version of the key information, for example, at least as long as the LWA session is active, e.g., as described above.

30 [00208] In some demonstrative embodiments, WLAN AP may be configured to select whether to defer an update of the security keys between UE 102 and WLAN AP 119, for

example, even if a new version of the second security information is received at WLAN AP 119 from cellular node 104, e.g., as described below.

[00209] In some demonstrative embodiments, controller component 123 may be configured to determine, based on a first version of a security key from an eNB, e.g., cellular manager 104, one or more shared keys to secure communication during an LWA session of UE 102 via the WLAN AP 119, e.g., as described above.

[00210] For example, controller component 123 may be configured to determine the one or more shared keys, e.g., including one or more transient keys, based on the first version of the security key, which may include a first version of the PMK, which may be based on an eNB key and a WT counter, e.g., as described above.

[00211] For example, controller component 123 may be configured to determine the one or more shared keys, e.g., including one or more transient keys, for example, based on a four-way handshake using the PMK, e.g., as described above.

[00212] In some demonstrative embodiments, controller component 123 may be configured to select to continue to use the shared keys, which are based on the first version of the security key, for example, even when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session of UE 102, e.g., as described above.

[00213] In some demonstrative embodiments, controller component 123 may be configured to select to continue to use the shared keys, which are based on the first version of the security key, for example, even at least as long as the LWA session is active, e.g., as described above.

[00214] In some demonstrative embodiments, WT node 106 may be configured to select whether to defer triggering WLAN AP 119 to update the security keys between UE 102 and WLAN AP 119, for example, even if a new version of the second security information is received at WT node 106 from cellular node 104, e.g., as described below.

[00215] In some demonstrative embodiments, interface 199 may receive from cellular manager 104 a security key corresponding to UE 102. For example, the security key may include a PMK, which may be, for example, based on a WT counter of WT node 106 and an eNB key of cellular manager 104, e.g., as described above.

[00216] In some demonstrative embodiments, controller component 149 may be configured to control selective transfer of the security key to the WLAN AP 119, e.g., as described above.

[00217] In some demonstrative embodiments, controller component 149 may be configured to select to defer transferring of the security key to the WLAN AP 119, for example, when an active LWA session of the UE 102 is ongoing via the WLAN AP 119.

[00218] In some demonstrative embodiments, controller component 149 may be configured to select to defer transferring the security key to the WLAN P 119, for example, at least as long as the LWA session is active.

[00219] In some demonstrative embodiments, controller component 149 may be configured to cause the WT node 106 to transfer to the WLAN AP 119 a first version of the security key, e.g., a first PMK, for example, prior to or during establishment of the LWA session, e.g., as described above.

[00220] In some demonstrative embodiments, controller component 149 may be configured to select to defer transferring to the WLAN AP 119 a second version of the security key, e.g., a second PMK, which may supersede the first version of the security key, for example, at least as long as the LWA session is active.

[00221] For example, interface 192 may receive a first PMK corresponding to UE 102, for example, prior to or during establishment of an LWA session of UE 102 via WLAN AP 119, and controller component 149 may cause WT node 106 to transfer the first PMK to WLAN AP 119, for example, to allow WLAN AP 119 to establish one or more TKs with UE 102 based on the PMK, e.g., as described above.

[00222] For example, interface 192 may receive a second PMK corresponding to UE 102, for example, while the LWA session of UE 102 via WLAN AP 119 is active, e.g., as described above. According to this example, controller component 149 may select to defer transferring the second PMK to WLAN AP 119, for example, as long as the LWA session is active, for example, to allow WLAN AP 119 to continue to use the same TKs, which are based on the first PMK, for the LWA session, e.g., as described above.

[00223] In some demonstrative embodiments, cellular manager 104, WLAN AP 119, and/or UE 102 may be configured to implement a suspend/resume mechanism, which may be configured to controllably suspend and/or resume communication of traffic between WLAN

AP 119 and the UE 102, for example, during a process of updating the transient keys between the WLAN AP 119 and the UE 102, e.g., as described below.

[00224] In some demonstrative embodiments, the suspend/resume mechanism may be configured to enable, for example, a handover, e.g., an inter-eNB handover or intra-eNB handover, for example, while reducing or even avoiding packet loss, e.g., as described below.

[00225] In some demonstrative embodiments, the suspend/resume mechanism may be configured for implementation with respect to intra-eNB handover and/or inter-eNB handover, for example, in a collocated LWA scenario and/or a non-collocated LWA scenario.

[00226] In some demonstrative embodiments, when a PMK update is performed, WLAN AP 119 and/or UE 102 may be able to store traffic to be transmitted (“uplink (UL) data”), for example, until new Transient Keys are generated based the new PMK, e.g., as described below.

[00227] In some demonstrative embodiments, as discussed above, a WLAN AP may be required to start a new rekeying process between the WLAN AP and an UE, for example, when a new PMK based on a new K_{eNB} is generated. This rekeying process may potentially result in packet loss.

[00228] In some demonstrative embodiments, WLAN AP 119 and/or UE 102 may be configured to selectively “suspend” their data transmission in both uplink and downlink, for example, during a Rekeying process, e.g., during a 4-way handshake following a PMK update. For example, WLAN AP 119 and/or UE 102 may be configured resume the data transmission, for example, after fresh transient keys are generated and available at the WLAN AP 119 and the UE 102, e.g., as described below.

[00229] In some demonstrative embodiments, an eNB, e.g., cellular node 104, may be configured to update WLAN AP 119 and/or UE on a PMK (“current PMK”) to be used by WLAN AP 119 and UE 102, for example, when a new LWA WiFi session is established with UE 102 via WLAN AP 119, e.g., as described above. The current PMK may be based, for example, on a current, e.g., a most recent, K_{eNB} .

[00230] In some demonstrative embodiments, the eNB may be configured to update the WLAN AP 119 and UE 102 on a PMK, e.g., the current PMK or a new PMK, which is to supersede the current PMK. For example, controller component 182 may be configured to cause cellular manager 104 to first update the UE 102 about the PMK, for example, before updating the WLAN AP 119 about the PMK. For example, this may allow having the PMK

already installed on the UE 102, e.g., when WLAN AP 119 is to start a 4-way handshake process with UE 102 based on the PMK.

[00231] In some demonstrative embodiments, once a party of the WLAN connection between WLAN AP 119 and UE 102, identifies that the 4-way handshake process has started, the party should stop all UL operations, e.g., by stopping any transmission of data packets to the other party, and should only resume the UL operations to the other party, for example, once the 4-way handshake process is completed and new transient keys were established, e.g., as described below.

[00232] In some demonstrative embodiments, until a party, e.g., each party (either the WLAN AP or the UE), identifies that the other party has initiated/accepted the 4-way handshake process, the party should continue all Downlink (DL) operations based on “old” transient keys, which are based on the current PMK, for example, by accepting encrypted data packets from the other party and decrypting the received packets using the “old” keys, e.g., as described below.

[00233] In some demonstrative embodiments, for example, only after a party, e.g., each party (either WLAN AP or UE), identifies that the other party has initiated/accepted the 4-way handshake process, the party should stop all DL operations, for example, by selecting to stop accepting data packets from the other party and to stop using the “old” keys, e.g., as described below.

[00234] In some demonstrative embodiments, for example, only after the 4-way handshake process is fully completed and new transient keys were established, both parties, e.g., the UE and the WLAN AP, may be allowed to resume the UL & DL operations, for example, using the “new” transient keys, e.g., as described below.

[00235] In some demonstrative embodiments, an eNB, e.g., cellular node 104, may generate a new PMK from a new *KeNB*, for example, due to intra eNB or inter-eNB handover (HO), and/or for any other reason, e.g., as described above.

[00236] In some demonstrative embodiments, the eNB, e.g., cellular node 104, may send a new WT counter to UE 102, which may trigger UE 102 to generate the new PMK, e.g., as described above.

[00237] In some demonstrative embodiments, UE 102 may be configured to wait for WLAN AP 119 to start a 4-way handshake process, for example, based on the new PMK, e.g., as described above.

[00238] In some demonstrative embodiments, UE 102 may be configured to continue to process UL transmissions to WLAN AP 119 and to process DL traffic received from WLAN AP 119, for example, while using one or more “old” or “current” transient-keys, e.g., based on the current PMK, for encryption and/or decryption, e.g., as described above.

- 5 [00239] In some demonstrative embodiments, the eNB, e.g., cellular manager 104, may send the new PMK to the WLAN AP 119, for example, internally or using an Xw interface, e.g., interface 199, for example, via WT node 106, e.g., according to an enhanced eNB Configuration Update Xw-AP procedure.

- 10 [00240] In some demonstrative embodiments, WLAN AP 119 may receive the new PMK and may initiate the 4-way handshake process with UE 102, for example, based on the new PMK.

- 15 [00241] In some demonstrative embodiments, WLAN AP 119 may be configured to suspend or stop all UL operations that are not related to the 4-way handshake, for example, by stopping to transmit data-packets towards UE 102. For example, WLAN AP 119 may store part or all information of the suspended UL transmissions, for example, at least until the 4-way handshake process is completed.

- 20 [00242] In some demonstrative embodiments, WLAN AP 119 may select to continue DL operations, for example, to decrypt received data-packets from UE 102, for example, while using the “old” or “current” transient-keys for decryption, e.g., to prevent loss of packets from UE 102 that were already “on air”.

- 25 [00243] In some demonstrative embodiments, UE 102 may receive a first message of the 4-way handshake process from WLAN AP 119 and may, e.g., immediately, stop or suspend, for example, all UL and DL operations that are related to the 4-way handshake. For example, at the stage of receipt of the first message of the 4-way handshake, there may be no new data-packets expected from the WLAN AP 119.

- 30 [00244] In some demonstrative embodiments, WLAN AP 119 may receive a second message of the 4-way handshake process from UE 102 and may, e.g., immediately, stop or suspend, for example, all DL operations that are not related to the 4-way handshake. For example, at the stage of receipt of the second message of the 4-way handshake, there may be no new data-packets expected from UE 102 and, accordingly, there may be no need to perform decryption operations.

[00245] In some demonstrative embodiments, WLAN AP 119 and UE 102 may be allowed to resume the UL and DL operations, e.g., to communicate data between WLAN AP 119 and UE 102, for example, once the 4-way handshake process is successfully completed, and both parties share the same set of new or fresh Transient-Keys, e.g., based on the new PMK.

5 [00246] In some demonstrative embodiments, controller component 123 may be configured to determine, based on a first version of a security key, e.g., a first PMK, a first version of one or more shared keys, e.g., TKs, to secure communication during an LWA session of UE 102 via WLAN AP 119, e.g., as described above.

[00247] In some demonstrative embodiments, controller component 123 may be configured
10 to initiate a four-way handshake with UE 102 based on a second version of the security key, e.g., based on a second PMK, as described above.

[00248] In some demonstrative embodiments, controller component 123 may be configured to cause WLAN AP 119 to transmit a first message of the four-way handshake to UE 102, and to suspend transmission of traffic of the LWA session to UE 102, e.g., as described
15 above.

[00249] In some demonstrative embodiments, controller component 123 may be configured to cause WLAN AP 119 to continue processing of traffic of the LWA session from UE 102, for example, based on the first version of the shared keys, e.g., as described above.

[00250] In some demonstrative embodiments, controller component 123 may be configured
20 to cause WLAN AP 119 to suspend processing of traffic of the LWA session from UE 102, for example, upon receipt of a second message of the four-way handshake from UE 102, e.g., as described above.

[00251] In some demonstrative embodiments, controller component 123 may be configured to cause WLAN AP 119 to resume communication of the traffic of the LWA session with UE
25 102 upon completion of the four-way handshake with UE 102, for example, based on a second version of the shared keys, which may be generated based on the second version of the security key, e.g., the second PMK, as described above.

[00252] In some demonstrative embodiments, controller component 197 may be configured to determine a security key, e.g., a PMK, based on a first version of key information, e.g., a
30 first version of an eNB key from an eNB; and, based on the security key, to determine one or more shared keys, e.g., one or more TKs, to secure communication with WLAN AP 119 during the LWA session via WLAN AP 119, e.g., as described above.

[00253] In some demonstrative embodiments, controller component 197 may be configured to determine a new security key, e.g., a new PMK, based on a second version of the key information, e.g., a second version of the eNB key, e.g., as described above.

[00254] In some demonstrative embodiments, controller component 197 may be configured to select to continue to use the shared keys, which are based on the first version of the key information, e.g., based the first eNB key, for example, until receipt of the first message of the four-way handshake with WLAN AP 119 based on the new security key, e.g., as described above.

[00255] In some demonstrative embodiments, controller component 197 may be configured to cause UE 102 to suspend communication of traffic of the LWA session upon receipt of the first message, and to resume communication of the traffic of the LWA session, for example, upon completion of the four-way handshake with the WLAN AP 119 based on the new security key, e.g., the new PMK, as described above.

[00256] Reference is made to Fig. 3, which schematically illustrates elements of a UE device 300, in accordance with some demonstrative embodiments. For example, one or more elements of UE device 300 may perform the functionality of one or more elements of UE 102 (Fig. 1). In one example, one or more elements of UE device 300 may be configured to perform one or more operations and/or the functionalities of one or more of cellular TRx 165 (Fig. 1), WLAN TRx 163 (Fig. 1), controller 197 (Fig. 1), message processor 198 (Fig. 1), and/or one or more other elements of UE 102 (Fig. 1). In some demonstrative embodiments, embodiments of a UE may be implemented into a system using any suitably configured hardware and/or software. Fig. 3 illustrates, for one embodiment, example components of UE device 300.

[00257] In some demonstrative embodiments, UE device 300 may include application circuitry 302, baseband circuitry 304, Radio Frequency (RF) circuitry 306, front-end module (FEM) circuitry 308, and one or more antennas 810, coupled together at least as shown.

[00258] In one example, application circuitry 302 may be configured to perform at least part of the functionality of controller 197 (Fig. 1), and/or message processor 198 (Fig. 1); and/or baseband circuitry 304, RF circuitry 306, and/or FEM circuitry 308 may be configured to perform at least part of the functionality of cellular TRx 165 (Fig. 1), WLAN TRx 163 (Fig. 1), controller 197 (Fig. 1), and/or message processor 198 (Fig. 1).

[00259] In some demonstrative embodiments, the application circuitry 302 may include one or more application processors. For example, the application circuitry 302 may include circuitry such as, but not limited to, one or more single-core or multi-core processors. The processor(s) may include any combination of general-purpose processors and dedicated
5 processors (e.g., graphics processors, application processors, etc.). The processors may be coupled with and/or may include memory/storage and may be configured to execute instructions stored in the memory/storage to enable various applications and/or operating systems to run on the system.

[00260] In some demonstrative embodiments, the baseband circuitry 304 may include
10 circuitry such as, but not limited to, one or more single-core or multi-core processors. The baseband circuitry 304 may include one or more baseband processors and/or control logic to process baseband signals received from a receive signal path of the RF circuitry 306 and to generate baseband signals for a transmit signal path of the RF circuitry 306. Baseband processing circuitry 304 may interface with the application circuitry 302, for example, for
15 generation and processing of the baseband signals and for controlling operations of the RF circuitry 306. For example, in some embodiments, the baseband circuitry 304 may include a second generation (2G) baseband processor 304a, a third generation (3G) baseband processor 304b, a fourth generation (4G) baseband processor 304c, and/or other baseband processor(s) 304d for other existing generations, generations in development or to be developed in the
20 future (e.g., fifth generation (5G), 6G, etc.). The baseband circuitry 304 (e.g., one or more of baseband processors 304a-d) may handle various radio control functions that enable communication with one or more radio networks via the RF circuitry 306. The radio control functions may include, but are not limited to, signal modulation/demodulation, encoding/decoding, radio frequency shifting, etc. In some embodiments,
25 modulation/demodulation circuitry of the baseband circuitry 304 may include Fast-Fourier Transform (FFT), precoding, and/or constellation mapping/demapping functionality. In some embodiments, encoding/decoding circuitry of the baseband circuitry 304 may include convolution, tail-biting convolution, turbo, Viterbi, and/or Low Density Parity Check (LDPC) encoder/decoder functionality. Embodiments of modulation/demodulation and
30 encoder/decoder functionality are not limited to these examples and may include other suitable functionality in other embodiments.

[00261] In some demonstrative embodiments, the baseband circuitry 304 may include elements of a protocol stack such as, for example, elements of an evolved universal terrestrial

radio access network (EUTRAN) protocol including, for example, physical (PHY), media access control (MAC), radio link control (RLC), packet data convergence protocol (PDCP), and/or radio resource control (RRC) elements. A central processing unit (CPU) 304e of the baseband circuitry 304 may be configured, for example, to run elements of the protocol stack for signaling of the PHY, MAC, RLC, PDCP and/or RRC layers. In some embodiments, the baseband circuitry may include one or more audio digital signal processor(s) (DSP) 304f. The audio DSP(s) 304f may include elements for compression/decompression and echo cancellation, and/or may include other suitable processing elements in other embodiments. Components of the baseband circuitry 304 may be suitably combined in a single chip, a single chipset, or disposed on a same circuit board in some embodiments. In some embodiments, some or all of the constituent components of the baseband circuitry 304 and the application circuitry 302 may be implemented together such as, for example, on a system on a chip (SOC).

[00262] In some demonstrative embodiments, the baseband circuitry 304 may provide for communication compatible with one or more radio technologies. For example, in some embodiments, the baseband circuitry 304 may support communication with an evolved universal terrestrial radio access network (EUTRAN) and/or other wireless metropolitan area networks (WMAN), a wireless local area network (WLAN), a wireless personal area network (WPAN), and/or one or more additional or alternative networks. Embodiments in which the baseband circuitry 304 is configured to support radio communications of more than one wireless protocol may be referred to as multi-mode baseband circuitry.

[00263] In some demonstrative embodiments, RF circuitry 306 may enable communication with wireless networks using modulated electromagnetic radiation through a non-solid medium. In various embodiments, the RF circuitry 306 may include switches, filters, amplifiers, etc. to facilitate the communication with the wireless network. RF circuitry 306 may include a receive signal path which may include circuitry to down-convert RF signals received from the FEM circuitry 308, and to provide baseband signals to the baseband circuitry 304. RF circuitry 306 may also include a transmit signal path which may include circuitry to up-convert baseband signals provided by the baseband circuitry 304 and provide RF output signals to the FEM circuitry 308 for transmission.

[00264] In some demonstrative embodiments, the RF circuitry 306 may include a receive signal path and a transmit signal path. The receive signal path of the RF circuitry 306 may include mixer circuitry 306a, amplifier circuitry 306b, and filter circuitry 306c. The transmit

signal path of the RF circuitry 306 may include filter circuitry 306c and mixer circuitry 306a. RF circuitry 306 may also include synthesizer circuitry 306d for synthesizing a frequency for use by the mixer circuitry 306a of the receive signal path and the transmit signal path. In some embodiments, the mixer circuitry 306a of the receive signal path may be configured to
5 down-convert RF signals received from the FEM circuitry 308 based on the synthesized frequency provided by synthesizer circuitry 306d. The amplifier circuitry 306b may be configured to amplify the down-converted signals and the filter circuitry 306c may be, for example, a low-pass filter (LPF) or a band-pass filter (BPF), configured to remove unwanted signals from the down-converted signals to generate output baseband signals. Output
10 baseband signals may be provided to the baseband circuitry 304 for further processing. In some embodiments, the output baseband signals may be zero-frequency baseband signals, although this is not a requirement. In some embodiments, mixer circuitry 306a of the receive signal path may comprise passive mixers, although the scope of the embodiments is not limited in this respect.

[00265] In some demonstrative embodiments, the mixer circuitry 306a of the transmit signal path may be configured to up-convert input baseband signals based on the synthesized frequency provided by the synthesizer circuitry 306d to generate RF output signals for the FEM circuitry 308. The baseband signals may be provided by the baseband circuitry 304 and may be filtered by filter circuitry 306c. The filter circuitry 306c may include a low-pass filter
20 (LPF), although the scope of the embodiments is not limited in this respect.

[00266] In some demonstrative embodiments, the mixer circuitry 306a of the receive signal path and the mixer circuitry 306a of the transmit signal path may include two or more mixers and may be arranged for quadrature downconversion and/or upconversion respectively. In some embodiments, the mixer circuitry 306a of the receive signal path and the mixer circuitry
25 306a of the transmit signal path may include two or more mixers and may be arranged for image rejection (e.g., Hartley image rejection). In some embodiments, the mixer circuitry 306a of the receive signal path and the mixer circuitry 306a may be arranged for direct downconversion and/or direct upconversion, respectively. In some embodiments, the mixer circuitry 306a of the receive signal path and the mixer circuitry 306a of the transmit signal
30 path may be configured for super-heterodyne operation.

[00267] In some demonstrative embodiments, the output baseband signals and the input baseband signals may be analog baseband signals, although the scope of the embodiments is not limited in this respect. In some alternate embodiments, the output baseband signals and

the input baseband signals may be digital baseband signals. In these alternate embodiments, the RF circuitry 306 may include analog-to-digital converter (ADC) and digital-to-analog converter (DAC) circuitry, and the baseband circuitry 304 may include a digital baseband interface to communicate with the RF circuitry 306.

- 5 [00268] In some dual-mode embodiments, a separate radio IC circuitry may be provided for processing signals for each spectrum, although the scope of the embodiments is not limited in this respect.

[00269] In some demonstrative embodiments, the synthesizer circuitry 306d may be a fractional-N synthesizer or a fractional $N/N+1$ synthesizer, although the scope of the
10 embodiments is not limited in this respect as other types of frequency synthesizers may be suitable. For example, synthesizer circuitry 306d may be a delta-sigma synthesizer, a frequency multiplier, or a synthesizer comprising a phase-locked loop with a frequency divider.

[00270] In some demonstrative embodiments, the synthesizer circuitry 306d may be
15 configured to synthesize an output frequency for use by the mixer circuitry 306a of the RF circuitry 306 based on a frequency input and a divider control input. In some embodiments, the synthesizer circuitry 306d may be a fractional $N/N+1$ synthesizer.

[00271] In some demonstrative embodiments, frequency input may be provided by a voltage controlled oscillator (VCO), although that is not a requirement. Divider control input may be
20 provided by either the baseband circuitry 304 or the applications processor 302 depending on the desired output frequency. In some embodiments, a divider control input (e.g., N) may be determined from a look-up table based on a channel indicated by the applications processor 302.

[00272] In some demonstrative embodiments, synthesizer circuitry 306d of the RF circuitry
25 306 may include a divider, a delay-locked loop (DLL), a multiplexer and a phase accumulator. In some embodiments, the divider may be a dual modulus divider (DMD) and the phase accumulator may be a digital phase accumulator (DPA). In some embodiments, the DMD may be configured to divide the input signal by either N or $N+1$ (e.g., based on a carry out) to provide a fractional division ratio. In some example embodiments, the DLL may
30 include a set of cascaded, tunable, delay elements, a phase detector, a charge pump and a D-type flip-flop. In these embodiments, the delay elements may be configured to break a VCO period up into N_d equal packets of phase, where N_d is the number of delay elements in the

delay line. In this way, the DLL provides negative feedback to help ensure that the total delay through the delay line is one VCO cycle.

[00273] In some demonstrative embodiments, synthesizer circuitry 306d may be configured to generate a carrier frequency as the output frequency, while in other embodiments, the output frequency may be a multiple of the carrier frequency (e.g., twice the carrier frequency, four times the carrier frequency) and used in conjunction with quadrature generator and divider circuitry to generate multiple signals at the carrier frequency with multiple different phases with respect to each other. In some embodiments, the output frequency may be a LO frequency (fLO). In some embodiments, the RF circuitry 306 may include an IQ/polar converter.

[00274] In some demonstrative embodiments, FEM circuitry 308 may include a receive signal path which may include circuitry configured to operate on RF signals received from one or more antennas 810, amplify the received signals and provide the amplified versions of the received signals to the RF circuitry 306 for further processing. FEM circuitry 308 may also include a transmit signal path which may include circuitry configured to amplify signals for transmission provided by the RF circuitry 306 for transmission by one or more of the one or more antennas 810.

[00275] In some demonstrative embodiments, the FEM circuitry 308 may include a TX/RX switch to switch between transmit mode and receive mode operation. The FEM circuitry may include a receive signal path and a transmit signal path. The receive signal path of the FEM circuitry may include a low-noise amplifier (LNA) to amplify received RF signals and provide the amplified received RF signals as an output (e.g., to the RF circuitry 306). The transmit signal path of the FEM circuitry 308 may include a power amplifier (PA) to amplify input RF signals (e.g., provided by RF circuitry 306), and one or more filters to generate RF signals for subsequent transmission (e.g., by one or more of the one or more antennas 810).

[00276] In some embodiments, the UE device 300 may include one or more additional or alternative elements such as, for example, memory/storage, display, camera, sensor, and/or input/output (I/O) interface.

[00277] Reference is made to Fig. 4, which schematically illustrates a method of selectively updating key information of a secured WLAN connection between a UE and a WLAN AP, in accordance with some demonstrative embodiments. In some embodiments, one or more of the operations of the method of Fig. 4 may be performed by a wireless communication

system, e.g., system 100 (Fig. 1); a cellular manager, for example, an eNB, e.g., cellular manager 104 (Fig. 1), eNB 203 (Fig. 2), and/or eNB 233 (Fig. 2); an interface, e.g., cellular TRx 167 (Fig. 1), and/or WLAN node interface 169 (Fig. 1); a message processor, e.g., message processor 144 (Fig. 1); and/or a controller, e.g., controller 182 (Fig. 1).

- 5 [00278] As indicated at block 402, the method may include communicating, at an eNB, with a WLAN AP. For example, cellular manager 104 (Fig. 1) may communicate with WLAN AP 119 (Fig. 1), e.g., directly or via WT node 106 (Fig. 1), as described above.

[00279] As indicated at block 404, the method may include communicating with a UE via a cellular interface. For example, cellular manager 104 (Fig. 1) may communicate with UE 102 (Fig. 1), e.g., as described above.

[00280] As indicated at block 406, the method may include selecting to defer transferring of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, when an LWA session of the UE is ongoing via the WLAN AP. For example, controller component 182 (Fig. 1) may select to defer transferring of first key information from cellular manager 104 (Fig. 1) to UE 102 (Fig. 1) and second key information from cellular manager 104 (Fig. 1) to WLAN AP 119 (Fig. 1), when an LWA session of UE 102 (Fig. 1) is ongoing via the WLAN AP 119 (Fig. 1), e.g., as described above.

[00281] Reference is made to Fig. 5, which schematically illustrates a method of selectively updating key information of a secured WLAN connection between a UE and a WLAN AP, in accordance with some demonstrative embodiments. In some embodiments, one or more of the operations of the method of Fig. 5 may be performed by a wireless communication system, e.g., system 100 (Fig. 1); a UE, e.g., UE 102 (Fig. 1), UE 204 (Fig. 2), and/or UE 300 (Fig. 3); an interface, e.g., cellular TRx 165 (Fig. 1), and/or WLAN TRx 163 (Fig. 1); a message processor, e.g., message processor 198 (Fig. 1); and/or a controller, e.g., controller 197 (Fig. 1).

[00282] As indicated at block 502, the method may include determining a security key based on a first version of key information from an eNB of a cellular network. For example, controller component 197 (Fig. 1) may determine a security key based on a first version of key information from a cellular manager 104 (Fig. 1) of a cellular network, e.g., as described above.

[00283] As indicated at block 504, the method may include based on the security key, determining one or more shared keys to secure communication with a WLAN AP during an LWA session via the WLAN AP. For example, controller component 197 (Fig. 1) may determine one or more shared keys, e.g., one or more TKs, to secure communication during an LWA session via WLAN AP 119 (Fig. 1), e.g., as described above.

[00284] As indicated at block 506, the method may include, selecting to continue to use the shared keys, which are based on the first version of the key information, for example, even when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session. For example, controller component 197 (Fig. 1) may select to continue to use the shared keys, which are based on the first version of the key information, for example, even when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, e.g., as described above.

[00285] Reference is made to Fig. 6, which schematically illustrates a method of selectively updating key information of a secured WLAN connection between a UE and a WLAN AP, in accordance with some demonstrative embodiments. In some embodiments, one or more of the operations of the method of Fig. 6 may be performed by a wireless communication system, e.g., system 100 (Fig. 1); a WLAN AP, e.g., WLAN AP 119 (Fig. 1), and/or WLAN AP 219 (Fig. 2); an interface, e.g., network interface 121, and/or WLAN TRx 122 (Fig. 1); a message processor, e.g., message processor 125 (Fig. 1); and/or a controller, e.g., controller 123 (Fig. 1).

[00286] As indicated at block 602, the method may include determining, based on a first version of a security key from an eNB, one or more shared keys to secure communication during an LWA session of a UE via the WLAN AP. For example, controller component 123 (Fig. 1) may determine one or more shared keys, e.g., TKs, to secure communication with UE 102 (Fig. 1) during an LWA session, for example, based on a first PMK, e.g., as described above.

[00287] As indicated at block 604, the method may include selecting to continue to use the shared keys, which are based on the first version of the security key, for example, even when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session. For example, controller component 123 (Fig. 1) may select to continue to use the shared keys, which are based on the first version of the PMK, for

example, even when a second version of the PMK, which supersedes the first version of the PMK, is received during the LWA session, e.g., as described above.

[00288] Reference is made to Fig. 7, which schematically illustrates a product of manufacture 700, in accordance with some demonstrative embodiments. Product 700 may include one or more tangible computer-readable non-transitory storage media 702, which may include computer-executable instructions, e.g., implemented by logic 704, operable to, when executed by at least one computer processor, enable the at least one computer processor to implement one or more operations at a cellular manager, for example, an eNB, e.g., cellular manager 104 (Fig. 1), eNB 203 (Fig. 2), and/or eNB 233 (Fig. 2); one or more components of a UE, e.g., UE 102 (Fig. 1), UE 204 (Fig. 2), and/or UE 300 (Fig. 3); one or more components of a WT node, e.g., WT node 106 (Fig. 1); one or more components of a WLAN AP, e.g., WLAN AP 119 (Fig. 1), and/or WLAN AP 219 (Fig. 2); a controller, e.g., controller 182 (Fig. 1), controller 197 (Fig. 1), controller 123 (Fig. 1), and/or controller 149 (Fig. 1); and/or a message processor, e.g., message processor 144 (Fig. 1), message processor 198 (Fig. 1), message processor 125 (Fig. 1), and/or message processor 150 (Fig. 1), and/or to perform, trigger and/or implement one or more operations and/or functionalities described above with reference to Figs. 2, 3, 4, 5, and/or 6, and/or one or more operations and/or functionalities described herein. The phrase “non-transitory machine-readable medium” is directed to include all computer-readable media, with the sole exception being a transitory propagating signal.

[00289] In some demonstrative embodiments, product 700 and/or machine-readable storage medium 702 may include one or more types of computer-readable storage media capable of storing data, including volatile memory, non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and the like. For example, machine-readable storage medium 702 may include, RAM, DRAM, Double-Data-Rate DRAM (DDR-DRAM), SDRAM, static RAM (SRAM), ROM, programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), Compact Disk ROM (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), flash memory (e.g., NOR or NAND flash memory), content addressable memory (CAM), polymer memory, phase-change memory, ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, a disk, a floppy disk, a hard drive, an optical disk, a magnetic disk, a card, a magnetic card, an optical card, a tape, a cassette, and the like. The computer-readable storage media may include any suitable media

involved with downloading or transferring a computer program from a remote computer to a requesting computer carried by data signals embodied in a carrier wave or other propagation medium through a communication link, e.g., a modem, radio or network connection.

[00290] In some demonstrative embodiments, logic 704 may include instructions, data, and/or code, which, if executed by a machine, may cause the machine to perform a method, process and/or operations as described herein. The machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware, software, firmware, and the like.

[00291] In some demonstrative embodiments, logic 704 may include, or may be implemented as, software, a software module, an application, a program, a subroutine, instructions, an instruction set, computing code, words, values, symbols, and the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, and the like. The instructions may be implemented according to a predefined computer language, manner or syntax, for instructing a processor to perform a certain function. The instructions may be implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language, such as C, C++, Java, BASIC, Matlab, Pascal, Visual BASIC, assembly language, machine code, and the like.

EXAMPLES

[00292] The following examples pertain to further embodiments.

[00293] Example 1 includes an apparatus of an Evolved Node B (eNB) comprising a Wireless Local Area Network (WLAN) interface to communicate with a WLAN Access Point (AP); a cellular transceiver to communicate with a User Equipment (UE); and a controller component configured to control selective transfer of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, the second key information is based on the first key information, the controller component configured to select to defer transferring of the first key information to the UE and the second key information to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00294] Example 2 includes the subject matter of Example 1, and optionally, wherein the controller component is configured to, prior to establishment of the LWA session, cause the

eNB to transfer a first version of the first key information to the UE and a first version of the second key information to the WLAN AP, the controller component is configured to defer transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP, at least as long as the LWA session is active,
5 the second version of the first and second key information supersedes the first version of the first and second key information.

[00295] Example 3 includes the subject matter of Example 1, and optionally, wherein the LWA session comprises a session handed over to the eNB from another eNB.

[00296] Example 4 includes the subject matter of any one of Examples 1-3, and optionally,
10 wherein the controller component is to defer transferring the first key information to the UE and the second key information to the WLAN P at least as long as the LWA session is active.

[00297] Example 5 includes the subject matter of any one of Examples 1-4, and optionally, wherein the first key information comprises a WLAN Termination (WT) counter, and the second key information is based on the WT counter and an eNB key of the eNB.

[00298] Example 6 includes the subject matter of Example 5, and optionally, wherein the second key information comprises a Pairwise Master Key (PMK) based on the eNB key and the WT counter.

[00299] Example 7 includes the subject matter of Example 5 or 6, and optionally, wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.

[00300] Example 8 includes the subject matter of any one of Examples 1-7, and optionally,
20 comprising one or more antennas, a memory and a processor.

[00301] Example 9 includes an apparatus comprising circuitry and logic configured to trigger an Evolved Node B (eNB) to communicate with a Wireless Local Area Network (WLAN) Access Point (AP); communicate with a User Equipment (UE) via a cellular interface; and
25 select to defer transferring of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP, the second key information is based on the first key information.

[00302] Example 10 includes the subject matter of Example 9, and optionally, wherein the
30 apparatus is configured to, prior to establishment of the LWA session, cause the eNB to transfer a first version of the first key information to the UE and a first version of the second

key information to the WLAN AP, and to defer transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP, at least as long as the LWA session is active, the second version of the first and second key information supersedes the first version of the first and second key information.

- 5 [00303] Example 11 includes the subject matter of Example 9, and optionally, wherein the LWA session comprises a session handed over to the eNB from another eNB.

[00304] Example 12 includes the subject matter of any one of Examples 9-11, and optionally, wherein the apparatus is configured to cause the eNB to defer transferring the first key information to the UE and the second key information to the WLAN P at least as long as
10 the LWA session is active.

[00305] Example 13 includes the subject matter of any one of Examples 9-12, and optionally, wherein the first key information comprises a WLAN Termination (WT) counter, and the second key information is based on the WT counter and an eNB key of the eNB.

[00306] Example 14 includes the subject matter of Example 13, and optionally, wherein the
15 second key information comprises a Pairwise Master Key (PMK) based on the eNB key and the WT counter.

[00307] Example 15 includes the subject matter of Example 13 or 14, and optionally, wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.

- 20 [00308] Example 16 includes the subject matter of any one of Examples 9-15, and optionally, comprising one or more antennas, a memory and a processor.

[00309] Example 17 includes a system of cellular communication comprising an Evolved Node B (eNB), the eNB comprising one or more antennas; a memory; a processor; a Wireless Local Area Network (WLAN) interface to communicate with a WLAN Access Point (AP); a
25 cellular transceiver to communicate with a User Equipment (UE); and a controller component configured to control selective transfer of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, the second key information is based on the first key information, the controller component configured to select to defer transferring of the first key information to the UE and the second key information to the
30 WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00310] Example 18 includes the subject matter of Example 17, and optionally, wherein the controller component is configured to, prior to establishment of the LWA session, cause the eNB to transfer a first version of the first key information to the UE and a first version of the second key information to the WLAN AP, the controller component is configured to defer
5 transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP, at least as long as the LWA session is active, the second version of the first and second key information supersedes the first version of the first and second key information.

[00311] Example 19 includes the subject matter of Example 17, and optionally, wherein the
10 LWA session comprises a session handed over to the eNB from another eNB.

[00312] Example 20 includes the subject matter of any one of Examples 17-19, and optionally, wherein the controller component is to defer transferring the first key information to the UE and the second key information to the WLAN P at least as long as the LWA session is active.

[00313] Example 21 includes the subject matter of any one of Examples 17-20, and optionally, wherein the first key information comprises a WLAN Termination (WT) counter, and the second key information is based on the WT counter and an eNB key of the eNB.

[00314] Example 22 includes the subject matter of Example 21, and optionally, wherein the second key information comprises a Pairwise Master Key (PMK) based on the eNB key and
20 the WT counter.

[00315] Example 23 includes the subject matter of Example 21 or 22, and optionally, wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.

[00316] Example 24 includes a method to be performed at an Evolved Node B (eNB), the
25 method comprising communicating with a Wireless Local Area Network (WLAN) Access Point (AP); communicating with a User Equipment (UE) via a cellular interface; and selecting to defer transferring of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP, the
30 second key information is based on the first key information.

[00317] Example 25 includes the subject matter of Example 24, and optionally, comprising, prior to establishment of the LWA session, causing the eNB to transfer a first version of the

first key information to the UE and a first version of the second key information to the WLAN AP, and deferring transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP, at least as long as the LWA session is active, the second version of the first and second key information supersedes the first version of the first and second key information.

[00318] Example 26 includes the subject matter of Example 24, and optionally, wherein the LWA session comprises a session handed over to the eNB from another eNB.

[00319] Example 27 includes the subject matter of any one of Examples 24-26, and optionally, comprising deferring transferring the first key information to the UE and the second key information to the WLAN P at least as long as the LWA session is active.

[00320] Example 28 includes the subject matter of any one of Examples 24-27, and optionally, wherein the first key information comprises a WLAN Termination (WT) counter, and the second key information is based on the WT counter and an eNB key of the eNB.

[00321] Example 29 includes the subject matter of Example 28, and optionally, wherein the second key information comprises a Pairwise Master Key (PMK) based on the eNB key and the WT counter.

[00322] Example 30 includes the subject matter of Example 28 or 29, and optionally, wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.

[00323] Example 31 includes a product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one computer processor, enable the at least one computer processor to implement operations at an Evolved Node B (eNB), the operations comprising communicating with a Wireless Local Area Network (WLAN) Access Point (AP); communicating with a User Equipment (UE) via a cellular interface; and selecting to defer transferring of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP, the second key information is based on the first key information.

[00324] Example 32 includes the subject matter of Example 31, and optionally, wherein the operations comprise, prior to establishment of the LWA session, causing the eNB to transfer a first version of the first key information to the UE and a first version of the second key

information to the WLAN AP, and deferring transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP, at least as long as the LWA session is active, the second version of the first and second key information supersedes the first version of the first and second key information.

- 5 [00325] Example 33 includes the subject matter of Example 31, and optionally, wherein the LWA session comprises a session handed over to the eNB from another eNB.

[00326] Example 34 includes the subject matter of any one of Examples 31-33, and optionally, wherein the operations comprise deferring transferring the first key information to the UE and the second key information to the WLAN P at least as long as the LWA session is
10 active.

[00327] Example 35 includes the subject matter of any one of Examples 31-34, and optionally, wherein the first key information comprises a WLAN Termination (WT) counter, and the second key information is based on the WT counter and an eNB key of the eNB.

[00328] Example 36 includes the subject matter of Example 35, and optionally, wherein the
15 second key information comprises a Pairwise Master Key (PMK) based on the eNB key and the WT counter.

[00329] Example 37 includes the subject matter of Example 35 or 36, and optionally, wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.

20 [00330] Example 38 includes an apparatus of cellular communication by an Evolved Node B (eNB), the apparatus comprising means for communicating with a Wireless Local Area Network (WLAN) Access Point (AP); means for communicating with a User Equipment (UE) via a cellular interface; and means for selecting to defer transferring of first key information from the eNB to the UE and second key information from the eNB to the WLAN
25 AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP, the second key information is based on the first key information.

[00331] Example 39 includes the subject matter of Example 38, and optionally, comprising means for, prior to establishment of the LWA session, causing the eNB to transfer a first
30 version of the first key information to the UE and a first version of the second key information to the WLAN AP, and deferring transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP,

at least as long as the LWA session is active, the second version of the first and second key information supersedes the first version of the first and second key information.

[00332] Example 40 includes the subject matter of Example 38, and optionally, wherein the LWA session comprises a session handed over to the eNB from another eNB.

- 5 [00333] Example 41 includes the subject matter of any one of Examples 38-40, and optionally, comprising means for deferring transferring the first key information to the UE and the second key information to the WLAN P at least as long as the LWA session is active.

- [00334] Example 42 includes the subject matter of any one of Examples 38-41, and optionally, wherein the first key information comprises a WLAN Termination (WT) counter,
10 and the second key information is based on the WT counter and an eNB key of the eNB.

[00335] Example 43 includes the subject matter of Example 42, and optionally, wherein the second key information comprises a Pairwise Master Key (PMK) based on the eNB key and the WT counter.

- [00336] Example 44 includes the subject matter of Example 42 or 43, and optionally,
15 wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.

- [00337] Example 45 includes an apparatus of a User Equipment (UE), the apparatus comprising a cellular transceiver to communicate with a cellular network; a Wireless Local Area Network (WLAN) transceiver to communicate with a WLAN Access Point (AP); and a
20 controller component configured to determine a security key based on a first version of key information from an evolved Node B (eNB) and, based on the security key, to determine one or more shared keys to secure communication with the WLAN AP during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP, the controller configured to select to continue to use the shared keys, which are based on the first version of
25 the key information, when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session.

- [00338] Example 46 includes the subject matter of Example 45, and optionally, wherein the controller component is configured to select to continue to use the shared keys, which are
30 based on the first version of the key information, at least as long as the LWA session is active.

[00339] Example 47 includes the subject matter of Example 45 or 46, and optionally, wherein the controller component is configured to determine a new security key based on the second version of the key information, the controller component is configured to select to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, the controller component is configured to cause the UE to suspend communication of traffic of the LWA session upon receipt of the first message, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

[00340] Example 48 includes the subject matter of any one of Examples 45-47, and optionally, wherein the second version of the key information is from the eNB.

[00341] Example 49 includes the subject matter of any one of Examples 45-47, and optionally, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

[00342] Example 50 includes the subject matter of any one of Examples 45-49, and optionally, wherein the controller component is to determine the shared keys according to a four-way handshake with the WLAN AP.

[00343] Example 51 includes the subject matter of any one of Examples 45-50, and optionally, comprising one or more antennas, a memory and a processor.

[00344] Example 52 includes an apparatus comprising circuitry and logic configured to trigger a User Equipment (UE) to determine a security key based on a first version of key information from an evolved Node B (eNB) of a cellular network; based on the security key, determine one or more shared keys to secure communication with a Wireless Local Area Network (WLAN) Access Point (AP) during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP; and when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, select to continue to use the shared keys, which are based on the first version of the key information.

[00345] Example 53 includes the subject matter of Example 52, and optionally, wherein the apparatus is configured to select to continue to use the shared keys, which are based on the first version of the key information, at least as long as the LWA session is active.

[00346] Example 54 includes the subject matter of Example 52 or 53, and optionally, wherein the apparatus is configured to cause the UE to determine a new security key based on the second version of the key information, to select to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, to suspend communication of traffic of the LWA session upon receipt of the first message, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

[00347] Example 55 includes the subject matter of any one of Examples 52-54, and optionally, wherein the second version of the key information is from the eNB.

[00348] Example 56 includes the subject matter of any one of Examples 52-54, and optionally, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

[00349] Example 57 includes the subject matter of any one of Examples 52-56, and optionally, wherein the apparatus is configured to cause the UE to determine the shared keys according to a four-way handshake with the WLAN AP.

[00350] Example 58 includes the subject matter of any one of Examples 52-57, and optionally, comprising one or more antennas, a memory and a processor.

[00351] Example 59 includes a system of cellular communication comprising a User Equipment (UE), the UE comprising one or more antennas; a memory; a processor; a cellular transceiver to communicate with a cellular network; a Wireless Local Area Network (WLAN) transceiver to communicate with a WLAN Access Point (AP); and a controller component configured to determine a security key based on a first version of key information from an evolved Node B (eNB) and, based on the security key, to determine one or more shared keys to secure communication with the WLAN AP during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP, the controller configured to select to continue to use the shared keys, which are based on the first version of the key information, when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session.

[00352] Example 60 includes the subject matter of Example 59, and optionally, wherein the controller component is configured to select to continue to use the shared keys, which are

based on the first version of the key information, at least as long as the LWA session is active.

[00353] Example 61 includes the subject matter of Example 59 or 60, and optionally, wherein the controller component is configured to determine a new security key based on the second version of the key information, the controller component is configured to select to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, the controller component is configured to cause the UE to suspend communication of traffic of the LWA session upon receipt of the first message, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

[00354] Example 62 includes the subject matter of any one of Examples 59-61, and optionally, wherein the second version of the key information is from the eNB.

[00355] Example 63 includes the subject matter of any one of Examples 59-61, and optionally, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

[00356] Example 64 includes the subject matter of any one of Examples 59-63, and optionally, wherein the controller component is to determine the shared keys according to a four-way handshake with the WLAN AP.

[00357] Example 65 includes a method to be performed at a User Equipment (UE), the method comprising determining a security key based on a first version of key information from an evolved Node B (eNB) of a cellular network; based on the security key, determining one or more shared keys to secure communication with a Wireless Local Area Network (WLAN) Access Point (AP) during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP; and when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, selecting to continue to use the shared keys, which are based on the first version of the key information.

[00358] Example 66 includes the subject matter of Example 65, and optionally, comprising selecting to continue to use the shared keys, which are based on the first version of the key information, at least as long as the LWA session is active.

[00359] Example 67 includes the subject matter of Example 65 or 66, and optionally, comprising determining a new security key based on the second version of the key information, selecting to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, suspending communication of traffic of the LWA session upon receipt of the first message, and resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

[00360] Example 68 includes the subject matter of any one of Examples 65-67, and optionally, wherein the second version of the key information is from the eNB.

[00361] Example 69 includes the subject matter of any one of Examples 65-67, and optionally, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

[00362] Example 70 includes the subject matter of any one of Examples 65-69, and optionally, comprising determining the shared keys according to a four-way handshake with the WLAN AP.

[00363] Example 71 includes a product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one computer processor, enable the at least one computer processor to implement operations at a User Equipment (UE), the operations comprising determining a security key based on a first version of key information from an evolved Node B (eNB) of a cellular network; based on the security key, determining one or more shared keys to secure communication with a Wireless Local Area Network (WLAN) Access Point (AP) during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP; and when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, selecting to continue to use the shared keys, which are based on the first version of the key information.

[00364] Example 72 includes the subject matter of Example 71, and optionally, wherein the operations comprise selecting to continue to use the shared keys, which are based on the first version of the key information, at least as long as the LWA session is active.

[00365] Example 73 includes the subject matter of Example 71 or 72, and optionally, wherein the operations comprise determining a new security key based on the second version

of the key information, selecting to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, suspending communication of traffic of the LWA session upon receipt of the first message, and resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

[00366] Example 74 includes the subject matter of any one of Examples 71-73, and optionally, wherein the second version of the key information is from the eNB.

[00367] Example 75 includes the subject matter of any one of Examples 71-73, and optionally, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

[00368] Example 76 includes the subject matter of any one of Examples 71-75 wherein the operations comprise determining the shared keys according to a four-way handshake with the WLAN AP.

[00369] Example 77 includes an apparatus of cellular communication by a User Equipment (UE), the apparatus comprising means for determining a security key based on a first version of key information from an evolved Node B (eNB) of a cellular network; means for, based on the security key, determining one or more shared keys to secure communication with a Wireless Local Area Network (WLAN) Access Point (AP) during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP; and means for, when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, selecting to continue to use the shared keys, which are based on the first version of the key information.

[00370] Example 78 includes the subject matter of Example 77, and optionally, comprising means for selecting to continue to use the shared keys, which are based on the first version of the key information, at least as long as the LWA session is active.

[00371] Example 79 includes the subject matter of Example 77 or 78, and optionally, comprising means for determining a new security key based on the second version of the key information, selecting to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, suspending communication of traffic of the LWA session upon receipt of the first message, and resuming communication of the traffic of the

LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

[00372] Example 80 includes the subject matter of any one of Examples 77-79, and optionally, wherein the second version of the key information is from the eNB.

- 5 [00373] Example 81 includes the subject matter of any one of Examples 77-79, and optionally, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

- [00374] Example 82 includes the subject matter of any one of Examples 77-81, and optionally, comprising means for determining the shared keys according to a four-way
10 handshake with the WLAN AP.

- [00375] Example 83 includes an apparatus of a Wireless Local Area Network (WLAN) Access Point (AP), the apparatus comprising a radio to communicate with a User Equipment (UE); and a controller component configured to determine, based on a first version of a security key from an evolved node B (eNB), one or more shared keys to secure
15 communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE via the WLAN AP, the controller component configured to select to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session.

- 20 [00376] Example 84 includes the subject matter of Example 83, and optionally, wherein the controller component is configured to select to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

- [00377] Example 85 includes the subject matter of Example 83 or 84, and optionally, wherein the controller component is configured to initiate a four-way handshake with the UE
25 based on the second version of the security key, the controller component is configured to cause the WLAN AP to transmit a first message of the four-way handshake to the UE, to suspend transmission of traffic of the LWA session to the UE and to continue processing of traffic of the LWA session from the UE based on the shared keys, the controller component is configured to cause the WLAN AP to suspend processing of traffic of the LWA session from
30 the UE upon receipt of a second message of the four-way handshake from the UE, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

[00378] Example 86 includes the subject matter of any one of Examples 83-85, and optionally, wherein the security key comprises a Pairwise Master Key (PMK) based on an eNB key and a WLAN Termination (WT) counter.

5 [00379] Example 87 includes the subject matter of any one of Examples 83-86, and optionally, comprising one or more antennas, a memory and a processor.

[00380] Example 88 includes an apparatus comprising circuitry and logic configured to trigger a Wireless Local Area Network (WLAN) Access Point (AP) to determine, based on a first version of a security key from an evolved Node B (eNB), one or more shared keys to secure communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of a User Equipment (UE) via the WLAN AP; and select to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session.

15 [00381] Example 89 includes the subject matter of Example 88, and optionally, wherein the apparatus is configured to cause the WLAN AP to select to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

[00382] Example 90 includes the subject matter of Example 88 or 89, and optionally, wherein the apparatus is configured to cause the WLAN AP to initiate a four-way handshake with the UE based on the second version of the security key, to transmit a first message of the four-way handshake to the UE, to suspend transmission of traffic of the LWA session to the UE and to continue processing of traffic of the LWA session from the UE based on the shared keys, to suspend processing of traffic of the LWA session from the UE upon receipt of a second message of the four-way handshake from the UE, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

[00383] Example 91 includes the subject matter of any one of Examples 88-90, and optionally, wherein the security key comprises a Pairwise Master Key (PMK) based on an eNB key and a WLAN Termination (WT) counter.

30 [00384] Example 92 includes the subject matter of any one of Examples 88-91, and optionally, comprising one or more antennas, a memory and a processor.

[00385] Example 93 includes a system of wireless communication comprising a Wireless Local Area Network (WLAN) Access Point (AP), the WLAN AP comprising one or more antennas; a memory; a processor; a radio to communicate with a User Equipment (UE); and a controller component configured to determine, based on a first version of a security key from an evolved node B (eNB), one or more shared keys to secure communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE via the WLAN AP, the controller component configured to select to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session.

[00386] Example 94 includes the subject matter of Example 93, and optionally, wherein the controller component is configured to select to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

[00387] Example 95 includes the subject matter of Example 93 or 94, and optionally, wherein the controller component is configured to initiate a four-way handshake with the UE based on the second version of the security key, the controller component is configured to cause the WLAN AP to transmit a first message of the four-way handshake to the UE, to suspend transmission of traffic of the LWA session to the UE and to continue processing of traffic of the LWA session from the UE based on the shared keys, the controller component is configured to cause the WLAN AP to suspend processing of traffic of the LWA session from the UE upon receipt of a second message of the four-way handshake from the UE, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

[00388] Example 96 includes the subject matter of any one of Examples 93-95, and optionally, wherein the security key comprises a Pairwise Master Key (PMK) based on an evolved Node B (eNB) key and a WLAN Termination (WT) counter.

[00389] Example 97 includes a method to be performed at a Wireless Local Area Network (WLAN) Access Point (AP), the method comprising determining, based on a first version of a security key from an evolved Node B (eNB), one or more shared keys to secure communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of a User Equipment (UE) via the WLAN AP; and selecting to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security

key, which supersedes the first version of the security key, is received during the LWA session.

[00390] Example 98 includes the subject matter of Example 97, and optionally, comprising selecting to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

[00391] Example 99 includes the subject matter of Example 97 or 98, and optionally, comprising initiating a four-way handshake with the UE based on the second version of the security key, transmitting a first message of the four-way handshake to the UE, suspending transmission of traffic of the LWA session to the UE and continuing processing of traffic of the LWA session from the UE based on the shared keys, suspending processing of traffic of the LWA session from the UE upon receipt of a second message of the four-way handshake from the UE, and resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

[00392] Example 100 includes the subject matter of any one of Examples 97-99, and optionally, wherein the security key comprises a Pairwise Master Key (PMK) based on an eNB key and a WLAN Termination (WT) counter.

[00393] Example 101 includes a product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one computer processor, enable the at least one computer processor to implement operations at a Wireless Local Area Network (WLAN) Access Point (AP), the operations comprising determining, based on a first version of a security key from an evolved Node B (eNB), one or more shared keys to secure communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of a User Equipment (UE) via the WLAN AP; and selecting to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session.

[00394] Example 102 includes the subject matter of Example 101, and optionally, wherein the operations comprise selecting to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

[00395] Example 103 includes the subject matter of Example 101 or 102, and optionally, wherein the operations comprise initiating a four-way handshake with the UE based on the

second version of the security key, transmitting a first message of the four-way handshake to the UE, suspending transmission of traffic of the LWA session to the UE and continuing processing of traffic of the LWA session from the UE based on the shared keys, suspending processing of traffic of the LWA session from the UE upon receipt of a second message of the four-way handshake from the UE, and resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

[00396] Example 104 includes the subject matter of any one of Examples 101-103, and optionally, wherein the security key comprises a Pairwise Master Key (PMK) based on an evolved Node B (eNB) key and a WLAN Termination (WT) counter.

[00397] Example 105 includes an apparatus of communication by a Wireless Local Area Network (WLAN) Access Point (AP), the apparatus comprising means for determining, based on a first version of a security key from an evolved Node B (eNB), one or more shared keys to secure communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of a User Equipment (UE) via the WLAN AP; and means for selecting to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session.

[00398] Example 106 includes the subject matter of Example 105, and optionally, comprising means for selecting to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

[00399] Example 107 includes the subject matter of Example 105 or 106, and optionally, comprising means for initiating a four-way handshake with the UE based on the second version of the security key, means for transmitting a first message of the four-way handshake to the UE, means for suspending transmission of traffic of the LWA session to the UE and continuing processing of traffic of the LWA session from the UE based on the shared keys, means for suspending processing of traffic of the LWA session from the UE upon receipt of a second message of the four-way handshake from the UE, and means for resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

[00400] Example 108 includes the subject matter of any one of Examples 105-107, and optionally, wherein the security key comprises a Pairwise Master Key (PMK) based on an evolved Node B (eNB) key and a WLAN Termination (WT) counter.

5 [00401] Example 109 includes an apparatus of a Wireless Local Area Network (WLAN) Termination (WT) node, the apparatus comprising a first interface to communicate with a WLAN Access Point (AP); a second interface to receive from an evolved node B (eNB) a security key corresponding to a User Equipment (UE); and a controller component configured to control selective transfer of the security key to the WLAN AP, the controller component configured to select to defer transferring of the security key to the WLAN AP,
10 when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00402] Example 110 includes the subject matter of Example 109, and optionally, wherein the controller component is to defer transferring the security key to the WLAN P at least as long as the LWA session is active.

15 [00403] Example 111 includes the subject matter of Example 109 or 110, and optionally, wherein the controller component is configured to, prior to establishment of the LWA session, cause the WT node to transfer a first version of the security key to the WLAN AP, the controller component is configured to defer transferring a second version of the security key to the WLAN AP, at least as long as the LWA session is active, the second version of the
20 security key supersedes the first version of the security key.

[00404] Example 112 includes the subject matter of any one of Examples 109-111, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00405] Example 113 includes the subject matter of any one of Examples 109-112, and optionally, wherein the security is based on a WT counter of the WT node and an eNB key of
25 the eNB.

[00406] Example 114 includes the subject matter of any one of Examples 109-113, and optionally, comprising one or more antennas, a memory and a processor.

[00407] Example 115 includes an apparatus comprising circuitry and logic configured to trigger a Wireless Local Area Network (WLAN) Termination (WT) node to receive from an
30 evolved node B (eNB) a security key corresponding to a User Equipment (UE); and select to defer transferring of the security key to a WLAN Access Point (AP), when an active Long-

Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00408] Example 116 includes the subject matter of Example 115, and optionally, wherein the apparatus is configured to cause the WT node to defer transferring the security key to the WLAN P at least as long as the LWA session is active.

[00409] Example 117 includes the subject matter of Example 115 or 116, and optionally, wherein the apparatus is configured to cause the WT node to, prior to establishment of the LWA session, transfer a first version of the security key to the WLAN AP, and defer transferring a second version of the security key to the WLAN AP, at least as long as the LWA session is active, the second version of the security key supersedes the first version of the security key.

[00410] Example 118 includes the subject matter of any one of Examples 115-117, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00411] Example 119 includes the subject matter of any one of Examples 115-118, and optionally, wherein the security is based on a WT counter of the WT node and an eNB key of the eNB.

[00412] Example 120 includes the subject matter of any one of Examples 115-119, and optionally, comprising one or more antennas, a memory and a processor.

[00413] Example 121 includes a system of wireless communication comprising a Wireless Local Area Network (WLAN) Termination (WT) node, the WT node comprising one or more antennas; a memory; a processor; a first interface to communicate with a WLAN Access Point (AP); a second interface to receive from an evolved node B (eNB) a security key corresponding to a User Equipment (UE); and a controller component configured to control selective transfer of the security key to the WLAN AP, the controller component configured to select to defer transferring of the security key to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00414] Example 122 includes the subject matter of Example 121, and optionally, wherein the controller component is to defer transferring the security key to the WLAN P at least as long as the LWA session is active.

[00415] Example 123 includes the subject matter of Example 121 or 122, and optionally, wherein the controller component is configured to, prior to establishment of the LWA session, cause the WT node to transfer a first version of the security key to the WLAN AP, the controller component is configured to defer transferring a second version of the security key to the WLAN AP, at least as long as the LWA session is active, the second version of the security key supersedes the first version of the security key.

[00416] Example 124 includes the subject matter of any one of Examples 121-123, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00417] Example 125 includes the subject matter of any one of Examples 121-124, and optionally, wherein the security is based on a WT counter of the WT node and an eNB key of the eNB.

[00418] Example 126 includes a method to be performed at a Wireless Local Area Network (WLAN) Termination (WT) node, the method comprising receiving from an evolved node B (eNB) a security key corresponding to a User Equipment (UE); and selecting to defer transferring of the security key to a WLAN Access Point (AP), when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00419] Example 127 includes the subject matter of Example 126, and optionally, comprising deferring transferring the security key to the WLAN P at least as long as the LWA session is active.

[00420] Example 128 includes the subject matter of Example 126 or 127, and optionally, comprising, prior to establishment of the LWA session, transferring a first version of the security key to the WLAN AP, and deferring transferring a second version of the security key to the WLAN AP, at least as long as the LWA session is active, the second version of the security key supersedes the first version of the security key.

[00421] Example 129 includes the subject matter of any one of Examples 126-128, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00422] Example 130 includes the subject matter of any one of Examples 126-129, and optionally, wherein the security is based on a WT counter of the WT node and an eNB key of the eNB.

[00423] Example 131 includes a product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one computer processor, enable the at least one computer processor to implement operations at a Wireless Local Area Network (WLAN) Termination (WT) node, the operations comprising receiving from an evolved node B (eNB) a security key corresponding to a User Equipment (UE); and selecting to defer transferring of the security key to a WLAN Access Point (AP), when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00424] Example 132 includes the subject matter of Example 131, and optionally, wherein the operations comprise deferring transferring the security key to the WLAN P at least as long as the LWA session is active.

[00425] Example 133 includes the subject matter of Example 131 or 132, and optionally, wherein the operations comprise, prior to establishment of the LWA session, transferring a first version of the security key to the WLAN AP, and deferring transferring a second version of the security key to the WLAN AP, at least as long as the LWA session is active, the second version of the security key supersedes the first version of the security key.

[00426] Example 134 includes the subject matter of any one of Examples 131-133, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00427] Example 135 includes the subject matter of any one of Examples 131-134, and optionally, wherein the security is based on a WT counter of the WT node and an eNB key of the eNB.

[00428] Example 136 includes an apparatus of wireless communication by a Wireless Local Area Network (WLAN) Termination (WT) node, the apparatus comprising means for receiving from an evolved node B (eNB) a security key corresponding to a User Equipment (UE); and means for selecting to defer transferring of the security key to a WLAN Access Point (AP), when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.

[00429] Example 137 includes the subject matter of Example 136, and optionally, comprising means for deferring transferring the security key to the WLAN P at least as long as the LWA session is active.

[00430] Example 138 includes the subject matter of Example 136 or 137, and optionally, comprising means for, prior to establishment of the LWA session, transferring a first version

of the security key to the WLAN AP, and deferring transferring a second version of the security key to the WLAN AP, at least as long as the LWA session is active, the second version of the security key supersedes the first version of the security key.

5 [00431] Example 139 includes the subject matter of any one of Examples 136-138, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00432] Example 140 includes the subject matter of any one of Examples 136-139, and optionally, wherein the security is based on a WT counter of the WT node and an eNB key of the eNB.

10 [00433] Functions, operations, components and/or features described herein with reference to one or more embodiments, may be combined with, or may be utilized in combination with, one or more other functions, operations, components and/or features described herein with reference to one or more other embodiments, or vice versa.

15 [00434] While certain features have been illustrated and described herein, many modifications, substitutions, changes, and equivalents may occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall within the true spirit of the disclosure.

CLAIMS

What is claimed is:

1. An apparatus of an Evolved Node B (eNB) comprising:
 - a Wireless Local Area Network (WLAN) interface to communicate with a WLAN
 - 5 Access Point (AP);
 - a cellular transceiver to communicate with a User Equipment (UE); and
 - a controller component configured to control selective transfer of first key information from the eNB to the UE and second key information from the eNB to the WLAN AP, the second key information is based on the first key information, the controller
 - 10 component configured to select to defer transferring of the first key information to the UE and the second key information to the WLAN AP, when an active Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of the UE is ongoing via the WLAN AP.
2. The apparatus of claim 1, wherein the controller component is configured to, prior to establishment of said LWA session, cause the eNB to transfer a first version of the first key
- 15 information to the UE and a first version of the second key information to the WLAN AP, the controller component is configured to defer transferring a second version of the first key information to the UE and a second version of the second key information to the WLAN AP, at least as long as the LWA session is active, the second version of the first and second key information supersedes the first version of the first and second key information.
- 20 3. The apparatus of claim 1, wherein the LWA session comprises a session handed over to the eNB from another eNB.
4. The apparatus of claim 1, wherein the controller component is to defer transferring the first key information to the UE and the second key information to the WLAN P at least as long as the LWA session is active.
- 25 5. The apparatus of any one of claims 1-4, wherein the first key information comprises a WLAN Termination (WT) counter, and the second key information is based on the WT counter and an eNB key of the eNB.
6. The apparatus of claim 5, wherein the second key information comprises a Pairwise Master Key (PMK) based on the eNB key and the WT counter.

7. The apparatus of claim 5, wherein the eNB key comprises a key generated by the eNB after establishment of the LWA session.
8. The apparatus of any one of claims 1-4 comprising one or more antennas, a memory and a processor.
- 5 9. An apparatus comprising circuitry and logic configured to trigger a User Equipment (UE) to:
- determine a security key based on a first version of key information from an evolved Node B (eNB) of a cellular network;
- based on the security key, determine one or more shared keys to secure
- 10 communication with a Wireless Local Area Network (WLAN) Access Point (AP) during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP; and
- when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, select to continue to use the shared keys, which are based on the first version of the key information.
- 15 10. The apparatus of claim 9 configured to select to continue to use the shared keys, which are based on the first version of the key information, at least as long as the LWA session is active.
11. The apparatus of claim 9 or 10 configured to cause the UE to determine a new security key based on the second version of the key information, to select to continue to use
- 20 the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key, to suspend communication of traffic of the LWA session upon receipt of the first message, and to resume communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.
- 25 12. The apparatus of claim 9 or 10, wherein the second version of the key information is from the eNB.
13. The apparatus of claim 9 or 10, wherein the second version of the key information is from another eNB, subsequent to session handover to the another eNB.

14. The apparatus of claim 9 or 10 configured to cause the UE to determine the shared keys according to a four-way handshake with the WLAN AP.

15. The apparatus of claim 9 or 10 comprising one or more antennas, a memory and a processor.

5 16. A product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one computer processor, enable the at least one computer processor to implement operations at a User Equipment (UE), the operations comprising:

10 determining a security key based on a first version of key information from an evolved Node B (eNB) of a cellular network;

based on the security key, determining one or more shared keys to secure communication with a Wireless Local Area Network (WLAN) Access Point (AP) during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session via the WLAN AP; and

15 when a second version of the key information, which supersedes the first version of the key information, is received from the cellular network during the LWA session, selecting to continue to use the shared keys, which are based on the first version of the key information.

17. The product of claim 16, wherein the operations comprise selecting to continue to use the shared keys, which are based on the first version of the key information, at least as
20 long as the LWA session is active.

18. The product of claim 16 or 17, wherein the operations comprise determining a new security key based on the second version of the key information, selecting to continue to use the shared keys, which are based on the first version of the key information, until receipt of a first message of a four-way handshake with the WLAN AP based on the new security key,
25 suspending communication of traffic of the LWA session upon receipt of the first message, and resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the WLAN AP based on the new security key.

19. The product of claim 16 or 17, wherein the second version of the key information is from the eNB.

20. The product of claim 16 or 17, wherein the operations comprise determining the shared keys according to a four-way handshake with the WLAN AP.

21. A method to be performed at a Wireless Local Area Network (WLAN) Access Point (AP), the method comprising:

5 determining, based on a first version of a security key from an evolved Node B (eNB), one or more shared keys to secure communication during a Long-Term-Evolution (LTE) WLAN Aggregation (LWA) session of a User Equipment (UE) via the WLAN AP; and

10 selecting to continue to use the shared keys, which are based on the first version of the security key, when a second version of the security key, which supersedes the first version of the security key, is received during the LWA session.

22. The method of claim 21 comprising selecting to continue to use the shared keys, which are based on the first version of the security key, at least as long as the LWA session is active.

15 23. The method of claim 21 comprising initiating a four-way handshake with the UE based on the second version of the security key, transmitting a first message of the four-way handshake to the UE, suspending transmission of traffic of the LWA session to the UE and continuing processing of traffic of the LWA session from the UE based on the shared keys, suspending processing of traffic of the LWA session from the UE upon receipt of a second
20 message of the four-way handshake from the UE, and resuming communication of the traffic of the LWA session upon completion of the four-way handshake with the UE based on the second version of the security key.

24. The method of claim 21, wherein the security key comprises a Pairwise Master Key (PMK) based on an eNB key and a WLAN Termination (WT) counter.

25 25. A product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one computer processor, enable the at least one computer processor to perform the method of any one of claims 21-24.

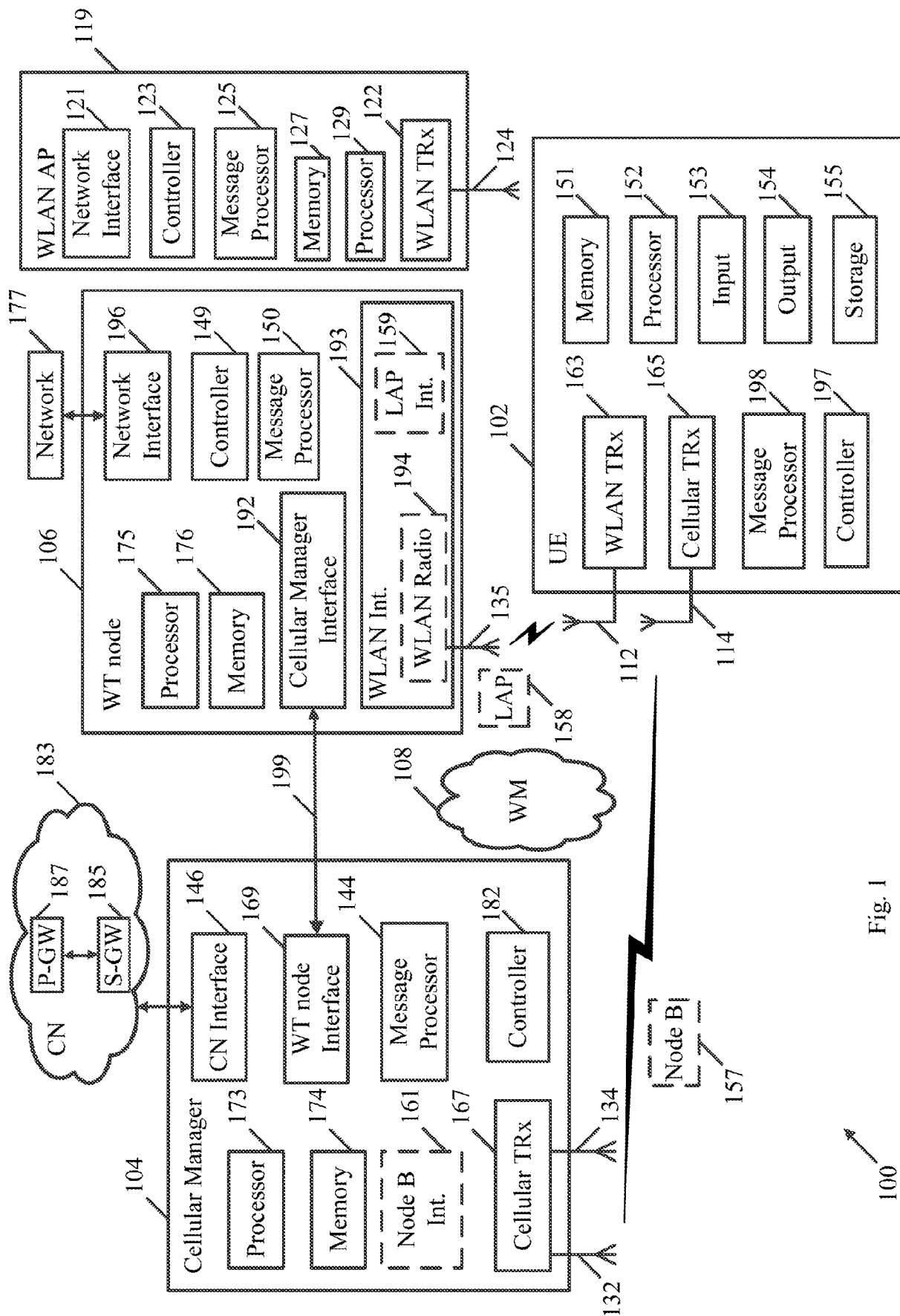


Fig. 1

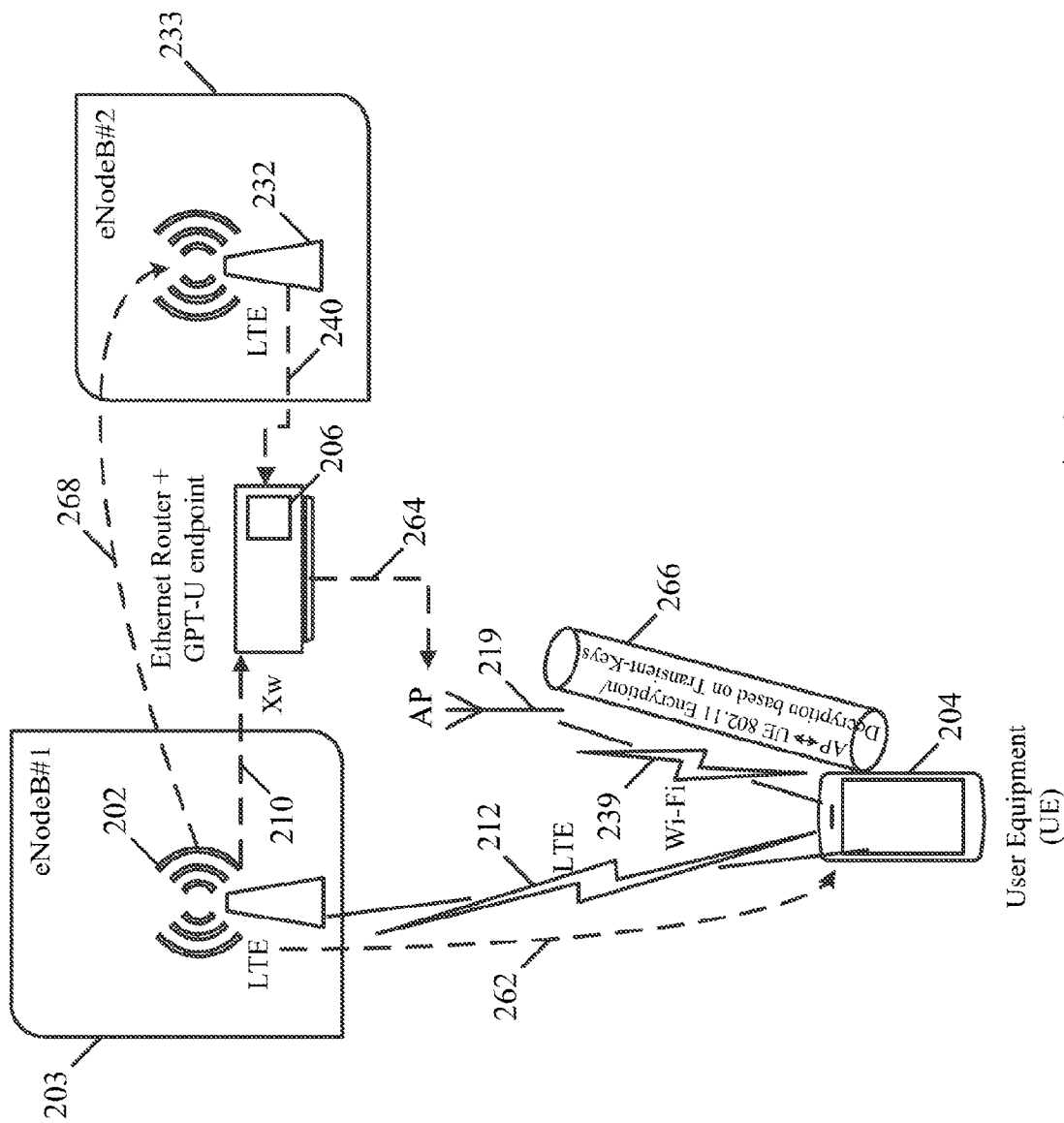


Fig. 2

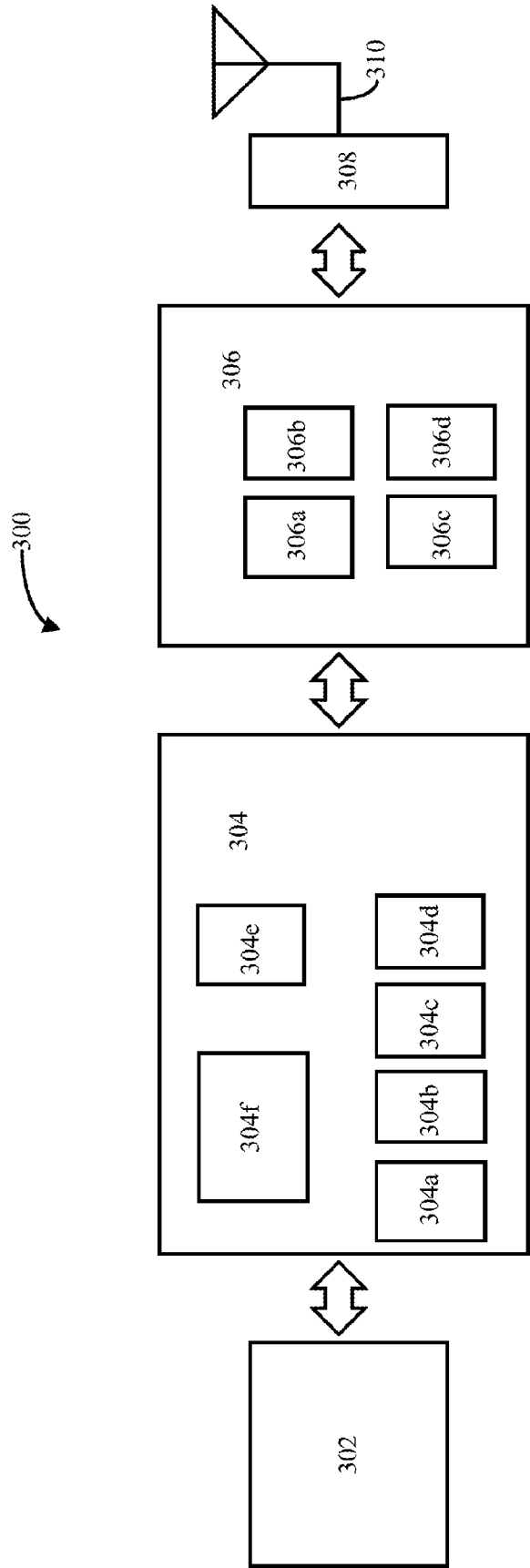


Fig. 3

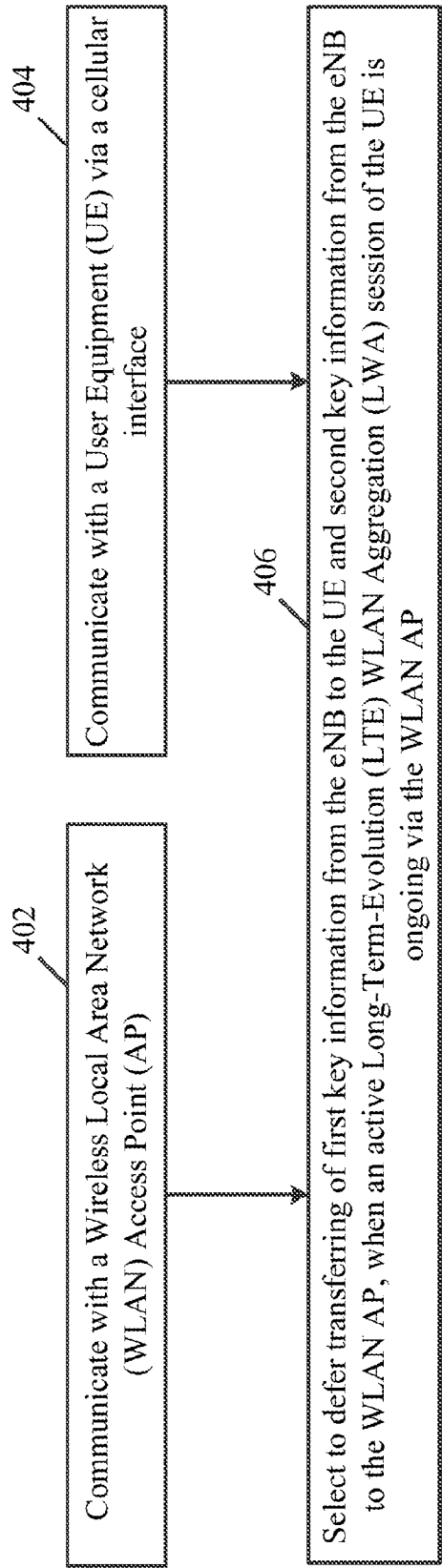


Fig. 4

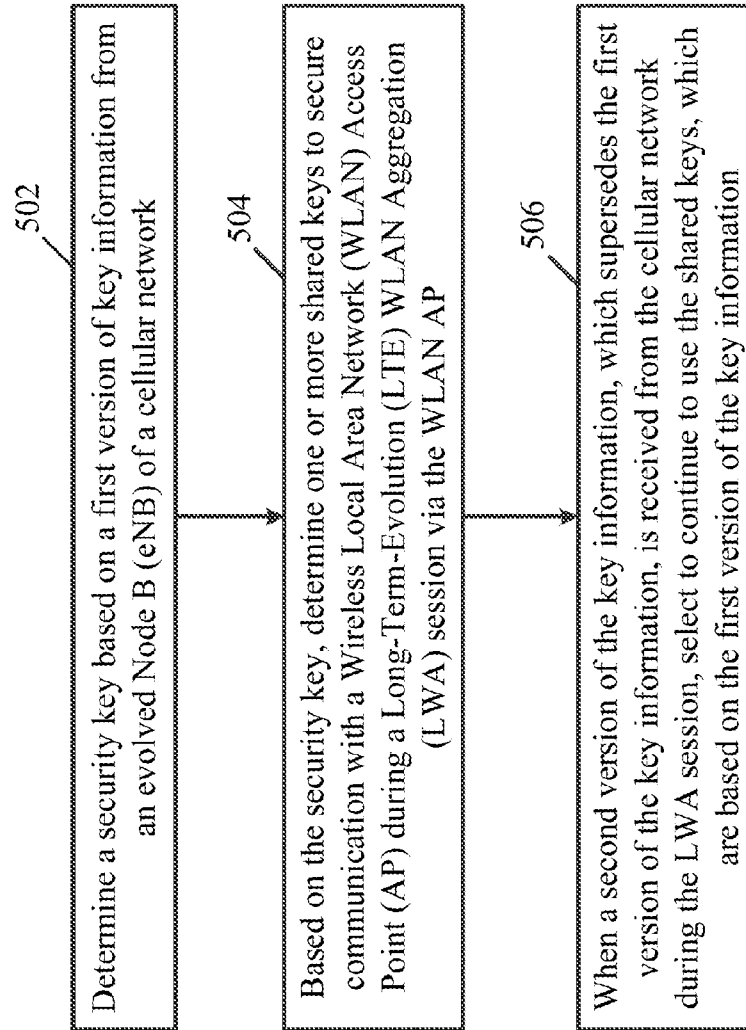


Fig. 5

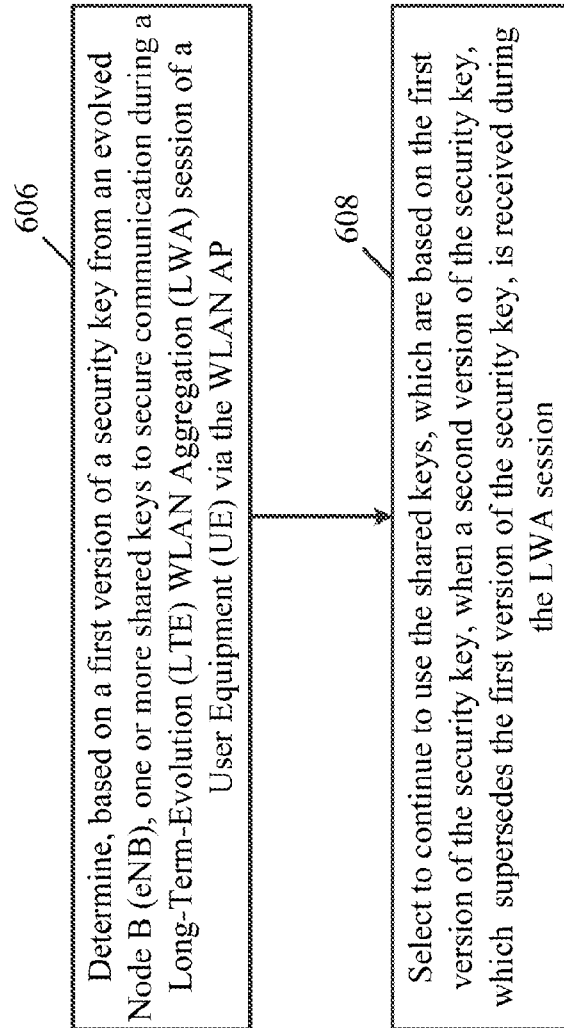


Fig. 6

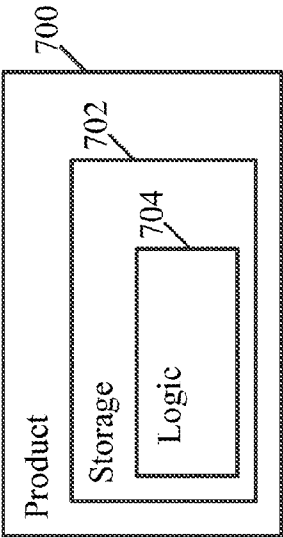


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/040318

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/04 H04W72/00
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, 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	WO 2016/036296 A1 (ERICSSON TELEFON AB L M [SE]) 10 March 2016 (2016-03-10) page 1, line 1 - page 3, line 23 page 6, lines 28-34 page 16, lines 1-10 page 37, line 28 - page 40, line 5 page 51, line 14 - page 52, line 29 -----	1-25
A	WO 2015/148434 A1 (INTEL IP CORP [US]) 1 October 2015 (2015-10-01) page 1, paragraphs 81-86, 120-122, 156-159 -----	1-25



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

29 August 2016

Date of mailing of the international search report

05/09/2016

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

Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/040318

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016036296	A1	10-03-2016	NONE

WO 2015148434	A1	01-10-2015	CA 2937908 A1 01-10-2015
		WO 2015148434 A1	01-10-2015
