



(51) International Patent Classification:

H04L 9/08 (2006.01) H04W 12/08 (2009.01)

(21) International Application Number:

PCT/FI2018/050290

(22) International Filing Date:

24 April 2018 (24.04.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/502,002 05 May 2017 (05.05.2017) US

(71) Applicant: NOKIA TECHNOLOGIES OY [FI/FI];

Karaportti 3, 02610 Espoo (FI).

(72) Inventors: KOSKELA, Jarkko; Kajuuttapiha 3, 90500

Oulu (FI). KOSKINEN, Jussi-Pekka; Kipinäkuja 10,

90420 Oulu (FI). TURPINEN, Samuli; Poolatie 3 A,

91100 Ii (FI).

(74) Agent: NOKIA TECHNOLOGIES OY et al.; Ari Aarnio,

IPR Department, Karakaari 7, 02610 Espoo (FI).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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).

Published:

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

(54) Title: PROVIDING SECURITY INFORMATION

(57) Abstract: Systems, methods, apparatuses, and computer program products relating for providing security information, for example, in 5G or new radio access technology (NR) are provided. One method may include transmitting in advance, by a network node, a new parameter used to generate security keys to at least one user equipment. The method may also include performing an integrity check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.



PROVIDING SECURITY INFORMATION

CROSS REFERENCE TO RELATED APPLICATIONS:

- 5 **[0001]** This application claims priority from United States Provisional Application No. 62/502,002, filed on May 5, 2017. The entire contents of this earlier filed application are hereby incorporated by reference in their entirety.

BACKGROUND:

10 **Field:**

- [0002]** Embodiments of the invention generally relate to wireless or mobile communications networks, such as, but not limited to, the Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (UTRAN), Long Term Evolution (LTE) Evolved UTRAN (E-UTRAN), LTE-Advanced (LTE-
15 A), LTE-A Pro, and/or 5G radio access technology or new radio access technology (NR). Some embodiments may generally relate to security handling, for example, in 5G or NR.

Description of the Related Art:

- [0003]** Universal Mobile Telecommunications System (UMTS) Terrestrial Radio
20 Access Network (UTRAN) refers to a communications network including base stations, or Node Bs, and for example radio network controllers (RNC). UTRAN allows for connectivity between the user equipment (UE) and the core network. The RNC provides control functionalities for one or more Node Bs. The RNC and its corresponding Node Bs are called the Radio Network Subsystem (RNS). In case
25 of E-UTRAN (enhanced UTRAN), no RNC exists and radio access functionality is provided by an evolved Node B (eNodeB or eNB) or many eNBs. Multiple eNBs are involved for a single UE connection, for example, in case of Coordinated Multipoint Transmission (CoMP) and in dual connectivity.

- [0004]** Long Term Evolution (LTE) or E-UTRAN refers to improvements of the
30 UMTS through improved efficiency and services, lower costs, and use of new

spectrum opportunities. In particular, LTE is a 3GPP standard that provides for uplink peak rates of at least, for example, 75 megabits per second (Mbps) per carrier and downlink peak rates of at least, for example, 300 Mbps per carrier. LTE supports scalable carrier bandwidths from 20 MHz down to 1.4 MHz and supports both Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD).

[0005] As mentioned above, LTE may also improve spectral efficiency in networks, allowing carriers to provide more data and voice services over a given bandwidth. Therefore, LTE is designed to fulfill the needs for high-speed data and media transport in addition to high capacity voice support. Advantages of LTE include, for example, high throughput, low latency, FDD and TDD support in the same platform, an improved end-user experience, and a simple architecture resulting in low operating costs.

[0006] Certain releases of 3GPP LTE (e.g., LTE Rel-10, LTE Rel-11, LTE Rel-12, LTE Rel-13) are targeted towards international mobile telecommunications advanced (IMT-A) systems, referred to herein for convenience simply as LTE-Advanced (LTE-A).

[0007] LTE-A is directed toward extending and optimizing the 3GPP LTE radio access technologies. A goal of LTE-A is to provide significantly enhanced services by means of higher data rates and lower latency with reduced cost. LTE-A is a more optimized radio system fulfilling the international telecommunication union-radio (ITU-R) requirements for IMT-Advanced while maintaining backward compatibility. One of the key features of LTE-A, introduced in LTE Rel-10, is carrier aggregation, which allows for increasing the data rates through aggregation of two or more LTE carriers.

[0008] 5th generation (5G) or new radio (NR) wireless systems refer to the next generation (NG) of radio systems and network architecture. It is estimated that 5G will provide bitrates on the order of 10-20 Gbit/s. 5G will support at least enhanced mobile broadband (eMBB) and ultra-reliable low-latency-communication (URLLC). 5G is also expected to increase network expandability up to hundreds of thousands of connections. The signal technology of 5G is anticipated to be improved for

greater coverage as well as spectral and signaling efficiency. 5G is expected to deliver extreme broadband and ultra-robust, low latency connectivity and massive networking to support the Internet of Things (IoT). With IoT and machine-to-machine (M2M) communication becoming more widespread, there will be a growing need for networks that meet the needs of lower power, low data rate, and long battery life. In 5G or NR, the node B or eNB may be referred to as a next generation node B (gNB).

SUMMARY:

10 **[0009]** One embodiment is directed to a method that may include transmitting in advance, by a network node, a new parameter used to generate security keys to at least one user equipment. The method may also include performing an integrity check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.

15 **[0010]** Another embodiment is directed to an apparatus that may include at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus at least to transmit in advance a new parameter used to generate security keys to at least one user equipment, and to perform an integrity check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.

20 **[0011]** Another embodiment is directed to an apparatus that may include transmitting means for transmitting in advance, by a network node, a new parameter used to generate security keys to at least one user equipment, and performing means for performing an integrity check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.

25 **[0012]** Another embodiment is directed to a non-transitory computer readable medium comprising program instructions stored thereon for performing at least the following: transmitting in advance, by a network node, a new parameter used to generate security keys to at least one user equipment, and performing an integrity

30

check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.

[0013] Another embodiment is directed to a method that may include receiving in advance, from a network node, a new parameter used to generate security keys for a user equipment. The method may also include generating, by the user equipment, new security keys based on at least one of the new parameter or a cell identifier of a cell that the user equipment is camped on.

[0014] Another embodiment is directed to an apparatus that may include at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus at least to receive in advance, from a network node, a new parameter used to generate security keys for the apparatus, and to generate new security keys based on at least one of the new parameter or a cell identifier of a cell that the apparatus is camped on.

[0015] Another embodiment is directed to an apparatus that may include receiving means for receiving in advance, from a network node, a new parameter used to generate security keys for the apparatus, and generating means for generating new security keys based on at least one of the new parameter or a cell identifier of a cell that the apparatus is camped on.

[0016] Another embodiment is directed to a non-transitory computer readable medium comprising program instructions stored thereon for performing at least the following: receiving in advance, from a network node, a new parameter used to generate security keys for a user equipment, and generating, by the user equipment, new security keys based on at least one of the new parameter or a cell identifier of a cell that the user equipment is camped on.

BRIEF DESCRIPTION OF THE DRAWINGS:

[0017] For proper understanding of the invention, reference should be made to the accompanying drawings, wherein:

[0018] Fig. 1 illustrates a block diagram depicting an example of a UE state machine and state transitions in NR;

[0019] Fig. 2a illustrates an example block diagram of an apparatus, according to an embodiment;

5 [0020] Fig. 2b illustrates an example block diagram of an apparatus, according to another embodiment;

[0021] Fig. 3a illustrates an example flow diagram of a method, according to an embodiment; and

10 [0022] Fig. 3b illustrates an example flow diagram of a method, according to another embodiment.

DETAILED DESCRIPTION:

[0023] It will be readily understood that the components of the invention, as generally described and illustrated in the figures herein, may be arranged and designed in a wide variety of different configurations. Thus, the following detailed description of the embodiments of systems, methods, apparatuses, and computer program products relating to security handling, for example, in 5G or new radio access technology (NR), as represented in the attached figures and described below, is not intended to limit the scope of the invention but is representative of selected
15
20 embodiments of the invention.

[0024] The features, structures, or characteristics of the invention described throughout this specification may be combined in any suitable manner in one or more embodiments. For example, the usage of the phrases “certain embodiments,” “some embodiments,” or other similar language, throughout this specification refers to the fact that a particular feature, structure, or characteristic described in
25 connection with the embodiment may be included in at least one embodiment of the present invention. Thus, appearances of the phrases “in certain embodiments,” “in some embodiments,” “in other embodiments,” or other similar language, throughout this specification do not necessarily all refer to the same group of embodiments, and

the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

[0025] Additionally, if desired, the different functions discussed below may be performed in a different order and/or concurrently with each other. Furthermore, if
5 desired, one or more of the described functions may be optional or may be combined. As such, the following description should be considered as merely illustrative of the principles, teachings and embodiments of this invention, and not in limitation thereof.

[0026] Fig. 1 illustrates a block diagram depicting an example of a UE state
10 machine and state transitions in NR. As illustrated in Fig. 1, NR radio resource control (RRC) may include three states models: RRC_IDLE, RRC_CONNECTED, and RRC_INACTIVE. In RRC_IDLE, there is cell re-selection mobility (it is to be determined if the UE AS context is not stored in any gNB or in the UE), paging is initiated by the core network (CN), and paging area is managed by CN. In
15 RRC_INACTIVE, there is cell re-selection mobility, CN – NR RAN connection (both C/U-planes) has been established for UE, the UE AS context is stored in at least one gNB and the UE, paging is initiated by NR RAN, RAN-based notification area is managed by NR RAN, and NR RAN knows the RAN-based notification area which the UE belongs to. In RRC_CONNECTED, the UE has an NR RRC
20 connection, the UE has an AS context in NR, NR RAN knows the cell which the UE belongs to, transfer of unicast data to/from the UE, and network controlled mobility, i.e., handover within NR and to/from E-UTRAN.

[0027] Certain embodiments of the present disclosure may relate to NR RRC_INACTIVE state and security handling.

[0028] Normally, when a UE establishes or resumes a RRC connection with a
25 network, new security keys need to be generated. This currently works in a manner that the UE sends a message in uplink (e.g., RRCConnectionResumeRequest) and the network responds with a key update proposal (e.g., RRCConnectionResume with next hop chaining count (NCC) field). The UE may confirm reception of this
30 and use the new keys (e.g., with RRCConnectionResumeComplete). It has been

proposed to omit the third step by giving the UE the next hop chaining counter (NCC) in the release/inactivation message (message moving UE to INACTIVE state) already, and then the UE would not be required to confirm reception of update proposal of security keys. However, this approach would not work in the case where the UE is not getting release command from the network, e.g., in case of radio link failure (RLF) or handover (HO) failure or a RRC connection reconfiguration failure or any other failure that may lead to a RRC connection re-establishment attempt.

[0029] According to an embodiment, a UE is given new NCC or equivalent parameter used to generate keys when the UE moves to a CONNECTED state and/or has activated the security for the current connection. As a result, when the UE experiences, for example, RLF or HO failure or reconfiguration failure or any other radio failure and it resumes/re-establishes the RRC connection it can use new keys generated based on the new NCC already from the start, such as for generating proper MAC-I/short MAC-I for the resume message from which the network can determine the integrity of the UE's RRC message and authenticate the UE, and the COMPLETE message sending (i.e., msg5) can be omitted. This may also enable the UE to transmit new data already along with the resume message as the new keys can be applied for the data encryption.

[0030] In an embodiment, the network may update the NCC, for instance, with RRCConnectionReconfiguration message and confirm the reception of the new NCC with the UE's RRCConnectionReconfigurationComplete message. According to some embodiments, the failure event, such as RLF, HO failure, reconfiguration failure, etc. may serve as a trigger for the UE to apply a new NCC.

[0031] In certain embodiments, the UE may apply a new NCC only if it selected or re-selected a new cell after the failure event and/or upon RRC connection resume. This may enable the old security key to be used when there is no need to change the key (i.e., when the serving network node is the same). According to some embodiments, the network may configure a UE with a cell list and/or a RAN notification area list (which may be a list of RAN notification area IDs) within

which the UE may not apply a new NCC or shall apply a new NCC once selecting or re-selecting a cell belonging to one of the lists. In one embodiment, the UE may apply a new NCC if it determines that the cell it has selected or re-selected belongs to a different network node than the cell it was served previously (i.e., before the failure event or inactivation). The UE may be able to determine this from a network node ID and/or gNB ID broadcasted in the system information.

[0032] In one embodiment, if the network tried to update the NCC for the UE and reconfiguration failure (HO failure is a special case of this) happened for that message, the network may update the NCC in the Resume message it sends to the UE, and this may trigger the UE to send a RRCConnectionResumeComplete message to the network. According to certain embodiments, the network may determine that the UE did not use the correct NCC with an integrity check. This may require that both the old and new NCC are forwarded by the previous gNB to the new gNB upon context fetch. Alternatively, the network may reject the UE's resume request in which case the UE will go to IDLE mode and start its connection establishment attempt from scratch.

[0033] Fig. 2a illustrates an example of an apparatus 10 according to an embodiment. In an embodiment, apparatus 10 may be a node, host, or server in a communications network or serving such a network. For example, apparatus 10 may be a base station, a node B, an evolved node B, 5G node B or access point, next generation node B (NG-NB or gNB), WLAN access point, mobility management entity (MME), or subscription server associated with a radio access network, such as a GSM network, LTE network, 5G or NR.

[0034] It should be understood that apparatus 10 may be comprised of an edge cloud server as a distributed computing system where the server and the radio node may be stand-alone apparatuses communicating with each other via a radio path or via a wired connection, or they may be located in a same entity communicating via a wired connection. It should be noted that one of ordinary skill in the art would understand that apparatus 10 may include components or features not shown in Fig.

2a.

[0035] As illustrated in Fig. 2a, apparatus 10 may include a processor 12 for processing information and executing instructions or operations. Processor 12 may be any type of general or specific purpose processor. In fact, processor 12 may include one or more of general-purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs), field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), and processors based on a multi-core processor architecture, as examples. While a single processor 12 is shown in Fig. 2a, multiple processors may be utilized according to other embodiments. For example, it should be understood that, in certain embodiments, apparatus 10 may include two or more processors that may form a multiprocessor system (i.e., in this case processor 12 represents a multiprocessor) that may support multiprocessing. In certain embodiments, the multiprocessor system may be tightly coupled or loosely coupled (e.g., to form a computer cluster).

[0036] Processor 12 may perform functions associated with the operation of apparatus 10 which may include, for example, precoding of antenna gain/phase parameters, encoding and decoding of individual bits forming a communication message, formatting of information, and overall control of the apparatus 10, including processes related to management of communication resources.

[0037] Apparatus 10 may further include or be coupled to a memory 14 (internal or external), which may be coupled to processor 12, for storing information and instructions that may be executed by processor 12. Memory 14 may be one or more memories and of any type suitable to the local application environment, and may be implemented using any suitable volatile or nonvolatile data storage technology such as a semiconductor-based memory device, a magnetic memory device and system, an optical memory device and system, fixed memory, and removable memory. For example, memory 14 can be comprised of any combination of random access memory (RAM), read only memory (ROM), static storage such as a magnetic or optical disk, hard disk drive (HDD), or any other type of non-transitory machine or computer readable media. The instructions stored in memory 14 may include

program instructions or computer program code that, when executed by processor 12, enable the apparatus 10 to perform tasks as described herein.

[0038] In an embodiment, apparatus 10 may further include or be coupled to (internal or external) a drive or port that is configured to accept and read an external computer readable storage medium, such as an optical disc, USB drive, flash drive, or any other storage medium. For example, the external computer readable storage medium may store a computer program or software for execution by processor 12 and/or apparatus 10.

[0039] In some embodiments, apparatus 10 may also include or be coupled to one or more antennas 15 for transmitting and receiving signals and/or data to and from apparatus 10. Apparatus 10 may further include or be coupled to a transceiver 18 configured to transmit and receive information. The transceiver 18 may include, for example, a plurality of radio interfaces that may be coupled to the antenna(s) 15. The radio interfaces may correspond to a plurality of radio access technologies including one or more of GSM, NB-IoT, LTE, 5G, WLAN, Bluetooth, BT-LE, NFC, radio frequency identifier (RFID), ultrawideband (UWB), and the like. The radio interface may include components, such as filters, converters (for example, digital-to-analog converters and the like), mappers, a Fast Fourier Transform (FFT) module, and the like, to generate symbols for a transmission via one or more downlinks and to receive symbols (for example, via an uplink). As such, transceiver 18 may be configured to modulate information on to a carrier waveform for transmission by the antenna(s) 15 and demodulate information received via the antenna(s) 15 for further processing by other elements of apparatus 10. In other embodiments, transceiver 18 may be capable of transmitting and receiving signals or data directly.

[0040] In an embodiment, memory 14 may store software modules that provide functionality when executed by processor 12. The modules may include, for example, an operating system that provides operating system functionality for apparatus 10. The memory may also store one or more functional modules, such as an application or program, to provide additional functionality for apparatus 10. The

components of apparatus 10 may be implemented in hardware, or as any suitable combination of hardware and software.

[0041] In certain embodiments, apparatus 10 may be a network node or RAN node, such as a base station, access point, node B, eNB, 5G or new radio node B (gNB) or access point, WLAN access point, or the like. According to certain
5 embodiments, apparatus 10 may be controlled by memory 14 and processor 12 to perform the functions associated with any of the embodiments described herein.

[0042] In an embodiment, apparatus 10 may be controlled by memory 14 and processor 12 to transmit, to a UE, a new NCC in advance (e.g., during a previous
10 RRC connection), for example in a RRCConnectionReconfiguration message, SecurityModeCommand message, RRCConnectionSetup message, or RRCConnectionResume message. For instance, in an embodiment, apparatus 10 may be controlled by memory 14 and processor 12 to immediately transmit, to the UE, the new NCC when the UE moves to a connected state. Then, the UE can
15 immediately apply a new security key calculated based on the pre-provisioned new NCC and a cell ID of the cell that the UE is camped on. For instance, the UE may calculate the new key when UE switches from an inactive mode (e.g., RRC_INACTIVE mode) to a connected mode (e.g., RRC_CONNECTED mode), or when UE transmits small data via a ResumeRequest message in inactive mode
20 without switching to a connected mode, or when the UE meets radio failures like RLF or HO failure. It is noted that, if the new NCC was not provided to the UE in advance, the UE would need to use the old key to encrypt data to be sent along with the ResumeRequest message. This would mean that the old RAN node (i.e., apparatus 10) is the only one allowed to decrypt the data packet. According to an
25 embodiment, by providing the NCC beforehand, the UE can immediately apply the new key for the data to send along with the ResumeRequest message, which the new RAN node is allowed to decipher itself once it fetches the UE context.

[0043] In one embodiment, apparatus 10 may be controlled by memory 14 and processor 12 to determine whether the UE used the correct NCC by using an
30 integrity check. For example, in an embodiment, apparatus 10 may be controlled by

memory 14 and processor 12 to perform the integrity check in a RRCConnectionResume message. Previously, the RRCResumeComplete message served the purpose of verifying the UE integrity since the NCC would be included in the Resume message. However, since, according to certain embodiments of the present disclosure, the NCC is provided during the previous RRC connection, the integrity verification may be made from the RRCConnectionResume message and the RRCResumeComplete message can be omitted.

[0044] Fig. 2b illustrates an example of an apparatus 20 according to another embodiment. In an embodiment, apparatus 20 may be a node or element in a communications network or associated with such a network, such as a UE, mobile equipment (ME), mobile station, mobile device, stationary device, IoT device, or other device. As described herein, UE may alternatively be referred to as, for example, a mobile station, mobile equipment, mobile unit, mobile device, user device, subscriber station, wireless terminal, tablet, smart phone, IoT device or NB-IoT device, or the like. As one example, apparatus 20 may be implemented in, for instance, a wireless handheld device, a wireless plug-in accessory, or the like.

[0045] In some example embodiments, apparatus 20 may include one or more processors, one or more computer-readable storage medium (for example, memory, storage, and the like), one or more radio access components (for example, a modem, a transceiver, and the like), and/or a user interface. In some embodiments, apparatus 20 may be configured to operate using one or more radio access technologies, such as GSM, LTE, LTE-A, NR, 5G, WLAN, WiFi, NB-IoT, Bluetooth, NFC, and any other radio access technologies. It should be noted that one of ordinary skill in the art would understand that apparatus 20 may include components or features not shown in Fig. 2b.

[0046] As illustrated in Fig. 2b, apparatus 20 may include or be coupled to a processor 22 for processing information and executing instructions or operations. Processor 22 may be any type of general or specific purpose processor. In fact, processor 22 may include one or more of general-purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs), field-

programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), and processors based on a multi-core processor architecture, as examples. While a single processor 22 is shown in Fig. 2b, multiple processors may be utilized according to other embodiments. For example, it should be understood that, in certain embodiments, apparatus 20 may include two or more processors that may form a multiprocessor system (i.e., in this case processor 22 represents a multiprocessor) that may support multiprocessing. In certain embodiments, the multiprocessor system may be tightly coupled or loosely coupled (e.g., to form a computer cluster).

[0047] Processor 22 may perform functions associated with the operation of apparatus 20 including, without limitation, precoding of antenna gain/phase parameters, encoding and decoding of individual bits forming a communication message, formatting of information, and overall control of the apparatus 20, including processes related to management of communication resources.

[0048] Apparatus 20 may further include or be coupled to a memory 24 (internal or external), which may be coupled to processor 22, for storing information and instructions that may be executed by processor 22. Memory 24 may be one or more memories and of any type suitable to the local application environment, and may be implemented using any suitable volatile or nonvolatile data storage technology such as a semiconductor-based memory device, a magnetic memory device and system, an optical memory device and system, fixed memory, and removable memory. For example, memory 24 can be comprised of any combination of random access memory (RAM), read only memory (ROM), static storage such as a magnetic or optical disk, or any other type of non-transitory machine or computer readable media. The instructions stored in memory 24 may include program instructions or computer program code that, when executed by processor 22, enable the apparatus 20 to perform tasks as described herein.

[0049] In an embodiment, apparatus 20 may further include or be coupled to (internal or external) a drive or port that is configured to accept and read an external computer readable storage medium, such as an optical disc, USB drive, flash drive,

or any other storage medium. For example, the external computer readable storage medium may store a computer program or software for execution by processor 22 and/or apparatus 20.

[0050] In some embodiments, apparatus 20 may also include or be coupled to one or more antennas 25 for receiving a downlink signal and for transmitting via an uplink from apparatus 20. Apparatus 20 may further include a transceiver 28 configured to transmit and receive information. The transceiver 28 may also include a radio interface (e.g., a modem) coupled to the antenna 25. The radio interface may correspond to a plurality of radio access technologies including one or more of GSM, LTE, LTE-A, 5G, NR, WLAN, NB-IoT, Bluetooth, BT-LE, NFC, RFID, UWB, and the like. The radio interface may include other components, such as filters, converters (for example, digital-to-analog converters and the like), symbol demappers, signal shaping components, an Inverse Fast Fourier Transform (IFFT) module, and the like, to process symbols, such as OFDMA symbols, carried by a downlink or an uplink.

[0051] For instance, transceiver 28 may be configured to modulate information on to a carrier waveform for transmission by the antenna(s) 25 and demodulate information received via the antenna(s) 25 for further processing by other elements of apparatus 20. In other embodiments, transceiver 28 may be capable of transmitting and receiving signals or data directly. Apparatus 20 may further include a user interface, such as a graphical user interface or touchscreen.

[0052] In an embodiment, memory 24 stores software modules that provide functionality when executed by processor 22. The modules may include, for example, an operating system that provides operating system functionality for apparatus 20. The memory may also store one or more functional modules, such as an application or program, to provide additional functionality for apparatus 20. The components of apparatus 20 may be implemented in hardware, or as any suitable combination of hardware and software.

[0053] According to one embodiment, apparatus 20 may be a UE, mobile device, mobile station, ME, IoT device and/or NB-IoT device, for example. According to

certain embodiments, apparatus 20 may be controlled by memory 24 and processor 22 to perform the functions associated with embodiments described herein. For example, in some embodiments, apparatus 20 may be configured to perform one or more of the processes depicted in any of the flow charts or signaling diagrams described herein. According to certain embodiments, apparatus 20 may be controlled by memory 24 and processor 22 to receive a new NCC in advance, for instance, during a previous RRC connection. For example, in certain embodiments, the new NCC may be received in a RRCConnectionReconfiguration message, SecurityModeCommand message, RRCConnectionSetup message, or RRCConnectionResume message.

[0054] In one embodiment, apparatus 20 may be controlled by memory 24 and processor 22 to calculate or generate a new security key(s) based on the pre-provisioned new NCC and/or a cell ID of the cell that apparatus 20 is camped on. In an embodiment, apparatus 20 may also be controlled by memory 24 and processor 22 to apply the new security key(s), for example, when apparatus 20 switches from an inactive state (e.g., RRC_INACTIVE mode) to a connected state (e.g., RRC_CONNECTED mode), or when apparatus 20 transmits small data via ResumeRequest message in inactive mode without switching to RRC_CONNECTED mode, or when apparatus 20 meets radio failures such as RLF or HO failure.

[0055] Thus, according to certain embodiments, by being provided the new NCC in advance or immediately when the RRC connection has been setup, apparatus 20 can seek to re-establish a RRC connection with a Resume procedure and may immediately apply the new security key(s) based on the pre-provisioned new NCC and the network connection can be re-established more quickly, as well as allow for data multiplexing.

[0056] Fig. 3a illustrates an example flow diagram of a method, according to one embodiment. The method of Fig. 3a may be performed, for example, by a network node, such as a base station, access point, eNB, gNB, or the like. As illustrated in Fig. 3a, the method may include, at 300, transmitting in advance, to one or more

UEs, a new NCC (e.g., during a previous RRC connection). In one embodiment, the transmitting of the new NCC may include transmitting the new NCC in a RRCConnectionReconfiguration message, SecurityModeCommand message, RRCConnectionSetup message, or RRCConnectionResume message. Then, the

5 UE(s) can immediately apply a new security key calculated based on the pre-provisioned new NCC and a cell ID of the cell that the UE is camped on. For instance, the UE(s) may calculate the new security key when the UE(s) switches from an inactive mode (e.g., RRC_INACTIVE mode) to a connected mode (e.g., RRC_CONNECTED mode), or when the UE(s) transmits small data via a

10 ResumeRequest message in inactive mode without switching to a connected mode, or when the UE(s) meets radio failures like RLF or HO failure. In one embodiment, the method may also include, at 310, using an integrity check to determine whether the UE used the correct NCC. For example, in an embodiment, the using step may include performing the integrity check in a RRCConnectionResume message. Since,

15 according to certain embodiments of the present disclosure, the NCC may be provided during the previous RRC connection, the integrity verification may be made from the RRCConnectionResume message and a RRCResumeComplete message can be omitted.

[0057] Fig. 3b illustrates an example flow diagram of a method, according to one

20 embodiment. The method of Fig. 3b may be performed, for example, by a UE, mobile station, mobile device, IoT device, MTC device, or the like. As illustrated in Fig. 3b the method may include, at 350, receiving a new NCC in advance, for instance, during a previous RRC connection. For example, in certain embodiments, the new NCC may be received in a RRCConnectionReconfiguration message,

25 SecurityModeCommand message, RRCConnectionSetup message, or RRCConnectionResume message. In one embodiment, the method may also include, at 360, calculating or generating a new security key(s) based on the pre-provisioned new NCC and/or a cell ID of the cell that the UE is camped on. In an embodiment, the method may also include, at 370, applying the new security key(s),

30 for example, when the UE switches from an inactive state (e.g., RRC_INACTIVE

mode) to a connected state (e.g., RRC_CONNECTED mode), or when the UE transmits small data via ResumeRequest message in inactive mode without switching to a connected mode, or when the UE meets radio failures such as RLF or HO failure.

5 **[0058]** In view of the above, embodiments of the invention provide several technical effects and/or improvements and/or advantages. For example, certain embodiments can reduce latencies even in case of RLF, for example, by allowing for the omission of msg5. Also, according to certain embodiments, key refresh after the initial RRC messages is not required and data transmission can take place
10 immediately (even multiplexed with the first RRC message) by the UE. As a result, certain embodiments can improve performance and throughput of network nodes including, for example, base stations, eNBs, gNBs and/or UEs. Accordingly, the use of embodiments of the invention result in improved functioning of communications networks and their nodes.

15 **[0059]** In some embodiments, the functionality of any of the methods, processes, signaling diagrams, or flow charts described herein may be implemented by software and/or computer program code or portions of code stored in memory or other computer readable or tangible media, and executed by a processor.

20 **[0060]** In certain embodiments, an apparatus may be included or be associated with at least one software application, module, unit or entity configured as arithmetic operation(s), or as a program or portions of it (including an added or updated software routine), executed by at least one operation processor. Programs, also called computer program products or computer programs, including software routines, applets and macros, may be stored in any apparatus-readable data storage
25 medium and include program instructions to perform particular tasks.

30 **[0061]** A computer program product may comprise one or more computer-executable components which, when the program is run, are configured to carry out embodiments described herein. The one or more computer-executable components may include at least one software code or portions of code. Modifications and configurations required for implementing the functionality of an embodiment may

be performed as routine(s), which may be implemented as added or updated software routine(s). In some embodiments, software routine(s) may be downloaded into the apparatus.

[0062] Software or a computer program code or portions of code may be in a source code form, object code form, or in some intermediate form, and may be stored in some sort of carrier, distribution medium, or computer readable medium, which may be any entity or device capable of carrying the program. Such carriers include a record medium, computer memory, read-only memory, photoelectrical and/or electrical carrier signal, telecommunications signal, and/or software distribution package, for example. Depending on the processing power needed, the computer program may be executed in a single electronic digital device or it may be distributed amongst a number of devices or computers. The computer readable medium or computer readable storage medium may be a non-transitory medium.

[0063] In other embodiments, the functionality may be performed by hardware, for example through the use of an application specific integrated circuit (ASIC), a programmable gate array (PGA), a field programmable gate array (FPGA), or any other combination of hardware and software. In yet another embodiment, the functionality may be implemented as a signal, a non-tangible means that can be carried by an electromagnetic signal downloaded from the Internet or other network.

[0064] According to an embodiment, an apparatus, such as a node, device, or a corresponding component, may be configured as a computer or a microprocessor, such as single-chip computer element, or as a chipset, including at least a memory for providing storage capacity used for arithmetic operation(s) and an operation processor for executing the arithmetic operation.

[0065] One embodiment is directed to a method that may include a network node transmitting in advance, to one or more UEs, a new NCC. In one embodiment, the transmitting in advance may comprise transmitting the new NCC during a previous RRC connection. The method may also include using an integrity check to determine whether the UE(s) used a correct NCC.

[0066] Another embodiment is directed to an apparatus that may include at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus at least to transmit in advance, to one or more UEs, a new NCC. In one embodiment, the transmitting in advance may comprise transmitting the new NCC during a previous RRC connection. The at least one memory and the computer program code may be further configured, with the at least one processor, to cause the apparatus at least to use an integrity check to determine whether the UE(s) used a correct NCC.

[0067] Another embodiment is directed to a method that may include receiving, at a UE, a new NCC in advance, for example, during a previous RRC connection. The method may also include calculating or generating new security key(s) based on the new NCC and/or a cell ID of the cell that the UE is camped on, and applying the new security key(s), for example, when the UE switches from an inactive state to a connected state.

[0068] Another embodiment is directed to an apparatus that may include at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus at least to receive a new NCC in advance, for example, during a previous RRC connection, to calculate or generate new security key(s) based on the new NCC and/or a cell ID of the cell that the apparatus is camped on, and to apply the new security key(s), for example, when the apparatus switches from an inactive state to a connected state.

[0069] One having ordinary skill in the art will readily understand that the invention as discussed above may be practiced with steps in a different order, and/or with hardware elements in configurations which are different than those which are disclosed. Therefore, although the invention has been described based upon these preferred embodiments, it would be apparent to those of skill in the art that certain modifications, variations, and alternative constructions would be apparent, while remaining within the spirit and scope of the invention. In order to determine the

metes and bounds of example embodiments, reference should be made to the appended claims.

We Claim:

1. A method, comprising:

transmitting in advance, by a network node, a new parameter used to
5 generate security keys to at least one user equipment; and

performing an integrity check to determine whether the at least one user
equipment is using a correct parameter to generate the security keys.

2. The method according to claim 1, wherein the new parameter comprises a new
10 next hop chaining counter (NCC).

3. The method according to claims 1 or 2, wherein the transmitting in advance
comprises transmitting the new parameter during a previous radio resource control
(RRC) connection between the at least one user equipment and the network node.

15

4. The method according to claim 3, wherein the transmitting further comprises
immediately transmitting the new parameter when the at least one user equipment
moves to a connected state.

20 5. The method according to claims 1 or 2, wherein the performing comprises
performing the integrity check in a radio resource control (RRC) connection resume
message.

6. The method according to claims 1 or 2, wherein the transmitting in advance
25 comprises transmitting the new parameter in at least one of a
RRCConnectionReconfiguration message, a SecurityModeCommand message, or
RRCConnectionSetup messages.

7. An apparatus, comprising:

30 at least one processor; and

at least one memory comprising computer program code,
the at least one memory and computer program code configured, with the at least
one processor, to cause the apparatus at least to
transmit in advance a new parameter used to generate security keys to at least
5 one user equipment; and
perform an integrity check to determine whether the at least one user
equipment is using a correct parameter to generate the security keys.

8. The apparatus according to claim 7, wherein the new parameter comprises a new
10 next hop chaining counter (NCC).

9. The apparatus according to claims 7 or 8, wherein the at least one memory and
computer program code are further configured, with the at least one processor, to cause
the apparatus at least to transmit the new parameter during a previous radio resource
15 control (RRC) connection between the at least one user equipment and the
apparatus.

10. The apparatus according to claim 9, wherein the at least one memory and
computer program code are further configured, with the at least one processor, to cause
20 the apparatus at least to immediately transmit the new parameter when the at least
one user equipment moves to a connected state.

11. The apparatus according to claims 7 or 8, wherein the at least one memory and
computer program code are further configured, with the at least one processor, to cause
25 the apparatus at least to perform the integrity check in a radio resource control (RRC)
connection resume message.

12. The apparatus according to claims 7 or 8, wherein the at least one memory and
computer program code are further configured, with the at least one processor, to cause
30 the apparatus at least to transmit the new parameter in at least one of a

RRCCONNECTIONReconfiguration message, a SecurityModeCommand message, or RRCCONNECTIONSetup messages.

13. An apparatus, comprising:

5 transmitting means for transmitting in advance, by a network node, a new parameter used to generate security keys to at least one user equipment; and

 performing means for performing an integrity check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.

10

14. A non-transitory computer readable medium comprising program instructions stored thereon for performing at least the following:

 transmitting in advance, by a network node, a new parameter used to generate security keys to at least one user equipment; and

15 performing an integrity check to determine whether the at least one user equipment is using a correct parameter to generate the security keys.

15. A method, comprising:

20 receiving in advance, from a network node, a new parameter used to generate security keys for a user equipment; and

 generating, by the user equipment, new security keys based on at least one of the new parameter or a cell identifier of a cell that the user equipment is camped on.

25 16. The method according to claim 15, wherein the new parameter comprises a new next hop chaining counter (NCC).

17. The method according to claims 15 or 16, wherein the receiving in advance comprises receiving the new parameter during a previous radio resource control (RRC) connection between the user equipment and the network node.

30

18. The method according to claims 15 or 16, the method further comprising:

applying the new security keys when at least one of:

the user equipment switches from an inactive state to a connected state;

5 the user equipment transmits small data in the inactive state without switching to the connected state; or

radio link failure (RLF) or handover (HO) failure occurs.

19. An apparatus, comprising:

10 at least one processor; and

at least one memory comprising computer program code,

the at least one memory and computer program code configured, with the at least one processor, to cause the apparatus at least to

15 receive in advance, from a network node, a new parameter used to generate security keys for the apparatus; and

generate new security keys based on at least one of the new parameter or a cell identifier of a cell that the apparatus is camped on.

20. The apparatus according to claim 19, wherein the new parameter comprises a
20 new next hop chaining counter (NCC).

21. The apparatus according to claims 19 or 20, wherein the at least one memory and computer program code are further configured, with the at least one processor, to cause the apparatus at least to receive the new parameter during a previous radio resource control (RRC) connection between the apparatus and the network node.
25

22. The apparatus according to claims 19 or 20, wherein the at least one memory and computer program code are further configured, with the at least one processor, to cause the apparatus at least to:

30 apply the new security keys when at least one of:

the user equipment switches from an inactive state to a connected state;

the user equipment transmits small data in the inactive state without switching to the connected state; or

5 radio link failure (RLF) or handover (HO) failure occurs.

23. An apparatus, comprising:

receiving means for receiving in advance, from a network node, a new parameter used to generate security keys for the apparatus; and

10 generating means for generating new security keys based on at least one of the new parameter or a cell identifier of a cell that the apparatus is camped on.

24. A non-transitory computer readable medium comprising program instructions stored thereon for performing at least the following:

15 receiving in advance, from a network node, a new parameter used to generate security keys for a user equipment; and

generating, by the user equipment, new security keys based on at least one of the new parameter or a cell identifier of a cell that the user equipment is camped on.

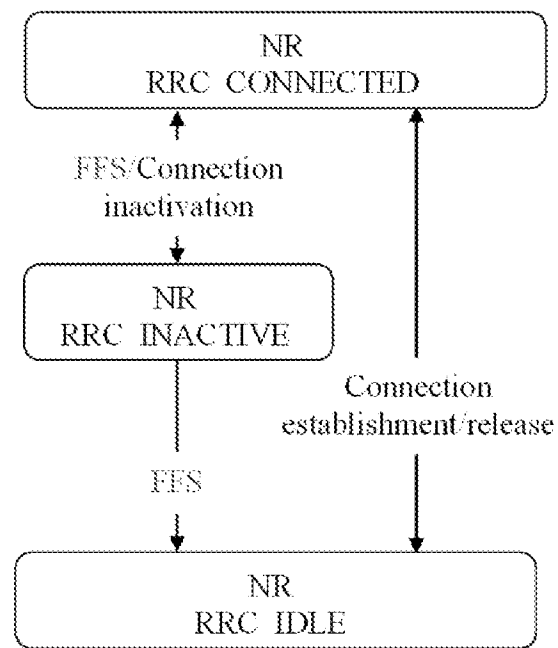


Fig. 1

2/3

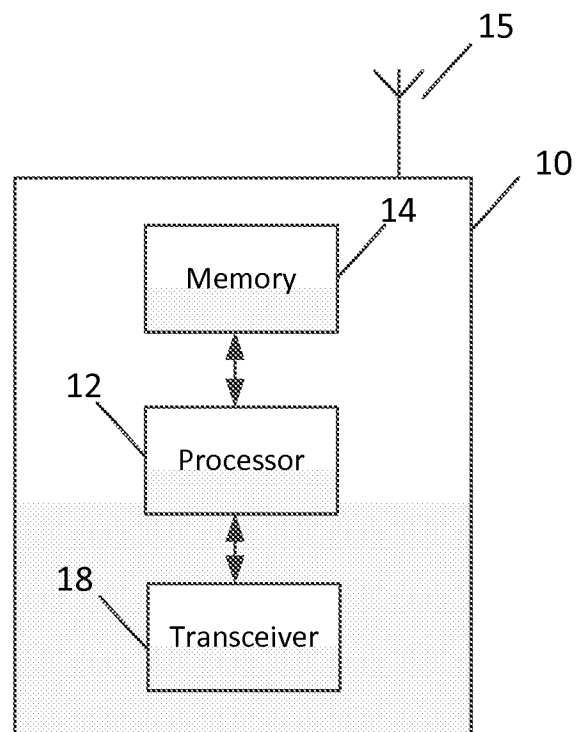


Fig. 2a

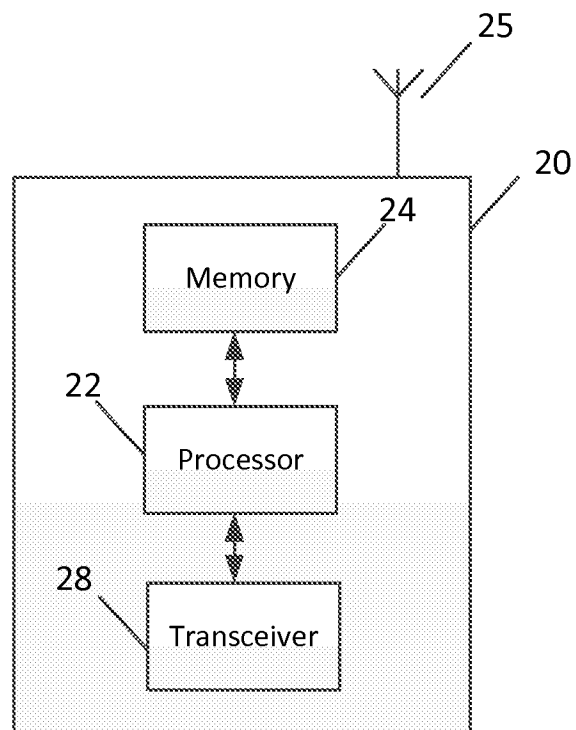


Fig. 2b

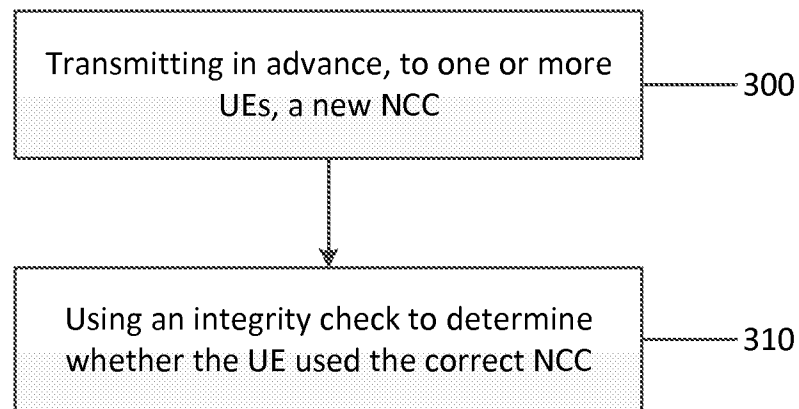


Fig. 3a

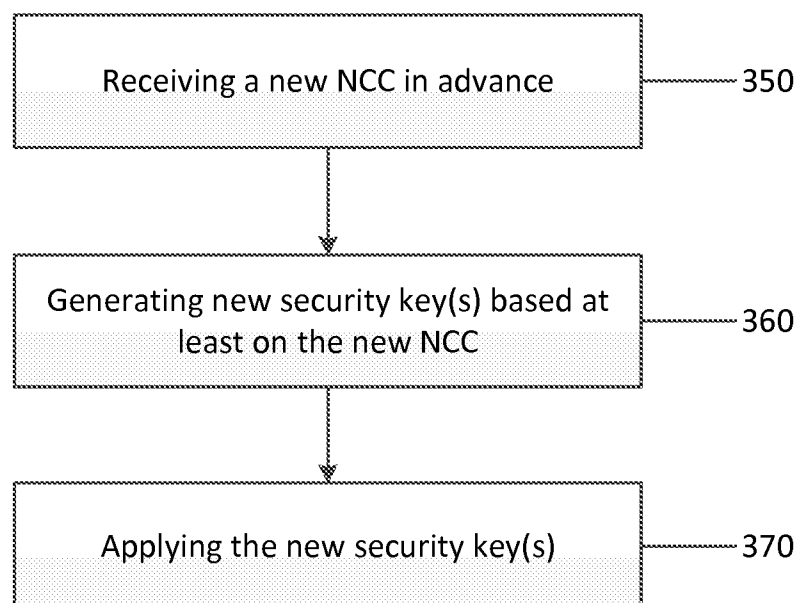


Fig. 3b

INTERNATIONAL SEARCH REPORT

International application No
PCT/FI2018/050290

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04W12/08
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)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NOKIA ET AL: "Principal signalling procedures for RRC connection control", 3GPP DRAFT; R2-1702762 PRINCIPAL SIGNALLING PROCEDURES FOR RRC CONNECTION CONTROL, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPO , vol. RAN WG2, no. Spokane, USA; 20170403 - 20170407 3 April 2017 (2017-04-03), XP051244750, Retrieved from the Internet: URL: http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/RAN2/Docs/ [retrieved on 2017-04-03] page 2 - page 6; figures 1-5 ----- -/-	1-24



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

14 June 2018

Date of mailing of the international search report

22/06/2018

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

Hou, Jie

INTERNATIONAL SEARCH REPORT

International application No
PCT/FI2018/050290

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ERICSSON: "Key refresh in NR", 3GPP DRAFT; R2-1702555 - KEY REFRESH IN NR, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG2, no. Spokane, USA; 20170403 - 20170407 3 April 2017 (2017-04-03), XP051244571, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_ SYNC/RAN2/Docs/ [retrieved on 2017-04-03] page 1 - page 3 -----	1-24
X	US 2010/042841 A1 (KING NEAL [DE] ET AL) 18 February 2010 (2010-02-18) paragraph [0036] - paragraph [0065]; figures 1-6 -----	1-24
X,P	NOKIA ET AL: "RRC connection establishment, re-establishment and resume", 3GPP DRAFT; R2-1705247 RRC CONNECTION ESTABLISHMENT, RE-ESTABLISHMENT, AND RESUME, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG2, no. Hangzhou, China; 20170515 - 20170519 14 May 2017 (2017-05-14), XP051275716, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_ SYNC/RAN2/Docs/ [retrieved on 2017-05-14] Section 2; figures 1-2 ----- -/--	1-24

INTERNATIONAL SEARCH REPORT

International application No

PCT/FI2018/050290

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	INTEL CORPORATION: "Security optimizations when resuming or re-establishing", 3GPP DRAFT; R2-1707040 NR RRC-SECURITY-OPTIM, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG2, no. Qingdao, China; 20170627 - 20170629 26 June 2017 (2017-06-26), XP051301536, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/RAN2/Docs/ [retrieved on 2017-06-26] Section 2; figures 1-2	1-24
X,P	----- INTEL CORPORATION: "Security handling for resumption, re-establishment and handover", 3GPP DRAFT; R2-1708803 NR RRC-SECURITY-OPTIM, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG2, no. Berlin, Germany; 20170821 - 20170825 20 August 2017 (2017-08-20), XP051318607, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/RAN2/Docs/ [retrieved on 2017-08-20] Section 2 and Section 5 -----	1-24

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FI2018/050290

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010042841 A1	18-02-2010	CN 101651539 A	17-02-2010
		DE 102009037469 A1	25-02-2010
		US 2010042841 A1	18-02-2010
