(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2017 (13.04.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/061925 A1

(51) International Patent Classification:
H04W 12/02 (2009.01) *H04W 36/00* (2009.01)
H04W 12/04 (2009.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/SE2016/050880

(22) International Filing Date:
20 September 2016 (20.09.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/239,062 8 October 2015 (08.10.2015) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; 164 83 Stockholm (SE).

(72) Inventors: **AXÉN, Rasmus**; Jordbruksgatan 12, SE-583 36 Linköping (SE). **JOHANSSON, Stefan**; Åbylundsgatan 62, SE-582 36 Linköping (SE). **NORRMAN, Karl**; Stigbergsgatan 32A, SE-116 28 Stockholm (SE).

(74) Agent: **AYOUB, Nabil**; Ericsson AB, Patent Unit Kista RAN 2, 164 80 Stockholm (SE).

(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, 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: A RADIO ACCESS NODE AND A METHOD OF OPERATING THE SAME

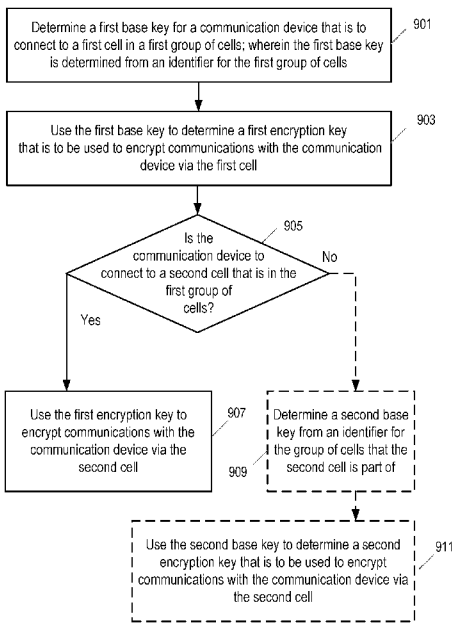

Figure 9

(57) Abstract: According to an aspect, there is provided a method of operating a first radio access node in a communication network, the first radio access node supporting a plurality of cells that are divided into one or more groups of cells, wherein at least a first group of cells comprises more than one cell, the method comprising determining (901) a first base key for a communication device that is to connect to the first radio access node via a first cell in the first group of cells; wherein the first base key is determined from an identifier for the first group of cells; using (903) the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells, using (907) the first encryption key to encrypt communications between the communication device and the first radio access node via the second cell.

WO 2017/061925 A1

A RADIO ACCESS NODE AND A METHOD OF OPERATING THE SAME

Technical Field

This disclosure relates to a radio access node in a communication network and a method of operating the same, and in particular relates to a radio access node that supports a plurality of cells.

Background

A trend in today's networks is for the operator to add more frequencies and reduce the size of cells to increase the capacity of mobile broadband. This leads to an increase in UE (User Equipment) reconfigurations and mobility actions. Examples of reconfigurations are when UEs are connected to multiple cells simultaneously, and the eNB (the node with which the UEs communicate over the air interface, and that controls a set of cells) may then enable and disable connectivity with the UE through the set of cells it controls.

The ability to quickly move or resume a UE session between cells becomes increasingly more important in order to fit the traffic patterns associated with short data bursts. A recent addition to the Long Term Evolution (LTE) standards is support for Multi Frequency Band Indicators (MFBI). MFBI has been introduced due to the fact that many LTE bands are partly or fully overlapping. MFBI provides the possibility that one cell can belong to multiple bands, even though it is only serving one physical frequency. Since the Evolved Absolute Radio Frequency Channel Number (EARFCN) of a cell is unique per band, this means that the EARFCN of the cell may differ, depending on which band the UE uses. MFBI has mainly been introduced to reduce the cost to the UEs. By only supporting a limited set of bands, the amount of conformance testing required can be significantly reduced.

The present disclosure relates to security when a UE connects to an eNB through one of a number of cells. In particular, the present disclosure relates to a problem during handover between cells that arises, for example, due to the way in which security of handovers in LTE is tied to the EARFCN. Outlines of security in LTE and handovers in LTE are presented below, however this disclosure should not be interpreted as only applying to LTE.

The communication between the UE and the eNB is encrypted and partially integrity protected. The integrity and encryption keys are derived from a common root key called the K_{eNB} which is shared between the UE and the eNB. The K_{eNB} can be said to be used to protect traffic, and this should be understood as meaning that the K_{eNB} is used to derive encryption and integrity keys that are used to encrypt and integrity protect traffic. Thus the integrity protection and encryption keys are derived from the K_{eNB} and an identifier for which integrity or encryption algorithm the key should be used with. The K_{eNB} is unique to the UE-eNB pair. That is, the same K_{eNB} is never used to protect the traffic between the UE and two different eNBs, and, likewise, the same K_{eNB} is not used to protect traffic between two different UEs and the network. The rationale behind this design is to prevent an attacker that has gained access to or knowledge of a K_{eNB} that is used between a UE and a first eNB to have any use for that K_{eNB} when attempting to break encryption or integrity on traffic between the UE and a physically different eNB.

To ensure that the K_{eNB} is unique per UE-eNB pair, K_{eNB} is changed during handover between two eNBs. For simplicity, K_{eNB} is actually changed on all intra-LTE handovers (e.g. handover between cells), even when the source eNB and target eNB is the same node.

The uniqueness of the UE-K_{eNB} pair during handover is achieved by the fact that the UE and source eNB derive a new K_{eNB} (denoted K_{eNB}*) from the current K_{eNB}, the Physical Cell Identifier (PCI) of the target primary cell (PCell) and the target physical cell downlink frequency. This is specified in clause 7.2.8 of 3GPP TS 33.401 “3GPP System Architecture Evolution (SAE); Security architecture”, version 12.14.0 (2015-03).

More specifically, the input to the key derivation function (KDF) to derive K_{eNB}* is:

- FC = 0x13
- P0 = PCI (target PCI)
- L0 = length of PCI (i.e. 0x00 0x02)
- P1 = EARFCN-DL (target physical cell downlink frequency)
- L1 length of EARFCN-DL (i.e. 0x00 0x02)

A handover between two eNBs without core network involvement, a so-called X2 handover, is described below with reference to Figure 1. Handovers can be performed after the UE has completed all necessary procedures to activate Radio Resource

Control (RRC) and Non-Access Stratum (NAS) security. The X2 handover is initiated by the source eNB 1 calculating a K_{eNB}^* key from the currently active K_{eNB}, shared between the source eNB 1 and the UE 2, and sending it together with the UE security capabilities to the target eNB 3 in a handover request message 4. The target eNB 3 replies with the required configuration information 5 for the UE connection. This information includes the chosen algorithms that the target eNB 3 and the UE 2 shall use. The source eNB 1 then forwards the reply to the UE 2 (signal 6), and the UE 2 confirms the handover with a completion message 7 to the target eNB 3. In the last step, the target eNB 3 retrieves a new key called the Next Hop key (NH) from a Mobility Management Entity (MME). The NH is derived from a key K_{ASME} (a base key that is shared by the UE and MME) and the NH is used as a basis for the calculation of K_{eNB}^* in the next handover event.

Five problems that relate to the K_{eNB} being bound to the Physical Cell Identifier (PCI) and EARFCN-DL of the primary cell (PCell) are outlined below.

The first of the problems is the prevention of the ability to quickly move or resume a UE session between cells. This is becoming increasingly important in order to fit with traffic patterns associated with short data bursts. The traffic bursts may be sent from the UE to the eNB over one of many cells controlled by the eNB. However, since the encryption is tied to the primary cell (via the use of the EARFCN-DL of the primary cell and the PCI in the derivation of the key K_{eNB}), each time the UE reconnects in another cell a key renegotiation must be performed before traffic can resume. This is where the first problem lies: re-negotiation of the K_{eNB} consumes considerable processor cycles and memory, and it implies that the encryption key also is modified leading to some already ciphered packets having to be buffered, deciphered using the old encryption key and then re-ciphered using the new encryption key. This adds delay that reduces the end-user experience. Moreover, it complicates the implementation of the eNB, leading to increased risk for implementation errors and increased cost for code maintenance. It should be noted that even though no handover is performed, the EARFCN-DL may have changed due to the fact that the UE connects in a different PCell for the same eNB.

Secondly, as discussed above, MFBI provides the possibility that one cell can belong to multiple bands, even though it is only serving one physical frequency. Since the EARFCN of a cell is unique per band, this means that the EARFCN-DL of the cell may

differ, depending on which band the UE uses. Consequently, if an eNB wants to enable and/or disable bearers on different frequencies an intra-eNB or intra-cell handover is required according to current standards, and hence the buffering and re-encryption issues remain.

Thirdly, the EARFCN-DL binding to K_{eNB} prevents multi-connectivity being used in a flexible way, e.g. switching freely between PCells without having to suspend all sessions and negotiate a new encryption key. Currently SCells can be reconfigured without suspending the user plane traffic, but when the PCell changes then all user plane traffic must be suspended (even for cells that have good connectivity).

An example is shown in Figure 2 where a UE 8 and radio access network, RAN (represented by eNB 9) performs key renegotiation when the UE 8 moves between cell 1 (10-1) and cell 2 (10-2), e.g. when the UE 8 is at location A. The eNB 9 and UE 8 first suspend all radio bearers in the session, then any already-ciphered Packet Data Convergence Protocol (PDCP) packets that are not confirmed as received by the UE must be de-ciphered and re-ciphered using the new encryption key. Once reconfiguration is complete the data session can be resumed.

In existing LTE systems the simultaneous use of multiple carriers is allowed (which is known as carrier aggregation, CA, or multicarrier), but the PCI and EARFCN-DL binding does not cause a problem here. Multicarrier means that a UE can be connected to more than one cell at the same time and use the combined bandwidth to schedule the UE. The UE must have one primary cell but can have several secondary cells. The Physical cell ID of the PCell is used as the input parameter for the K_{eNB} generation, and the EARFCN-DL is taken from the frequency of the PCell as well.

The fourth problem is illustrated with reference to Figure 3. Figure 3 shows an eNB 9 that is controlling four cells, 10-1, 10-2, 10-3 and 10-4. The Figure illustrates a handover-chain scenario with a UE 8 in three different locations, A, B and C where the binding of the K_{eNB} to the PCI and EARFCN-DL creates a highly inefficient process. At location A the UE 8 is connected to cell 1 (10-1) and 4 (10-4), at location B the UE 8 is connected to cell 1 (10-1), 3 (10-3) and 4 (10-4), and at location C the UE 8 is connected to cell 2 (10-2), 3 (10-3) and 4 (10-4).

During reconfiguration of a PCell all data sessions are suspended, regardless of cell quality or bandwidth, due to the K_{eNB} renegotiation. Depending on which cells are selected as the PCell for the UE 8, up to three different K_{eNB} renegotiations could occur when moving from point C to point A. During this time packets are buffered in the eNB 9, re-encrypted and sent out once the K_{eNB} renegotiation is complete. This adds delay to the ongoing data session.

The fifth problem is an additional problem that MFBI has introduced and results from the fact that carrier aggregation is only supported between a limited set of bands (also to reduce UE cost). Since the standard has defined that the UE should initially be configured with the EARFCN-DL of the primary band (if supported by the UE), it may prove that carrier aggregation between that band (of the PCell) and a potential SCell is not supported, but where one of the additional bands of the PCell can be combined with the potential SCell.

In order to provide the possibility of carrier aggregation, the EARFCN-DL of the PCell has to be changed. That is achieved by performing a procedure called intra-cell handover, and is the same mechanism that is used for key-change-on-the-fly to update the K_{eNB} and hence implicitly the encryption key. In terms of signalling this intra-cell handover looks like a handover, but no change of PCell has actually been made.

This, however, introduces the same problem as for normal handovers, where the data session has to be suspended during the intra-cell handover procedure and already ciphered data has to be de-ciphered and re-ciphered again, once the intra-cell handover is completed.

The five problems above are specific to the way security is handled in LTE, although some of the problems may also be evident in other types of communication networks. However, the need to optimise security processing is common to many different types of network.

Therefore there is a need for improvements in the way in which security is handled when a handover occurs between cells supported by the same eNB.

Summary

According to a first aspect, there is provided a method of operating a first radio access node in a communication network. The first radio access node supports a plurality of cells that are divided into one or more groups of cells, where at least a first group of cells comprises more than one cell. The method comprises determining a first base key for a communication device that is to connect to the first radio access node via a first cell in a first group of cells; wherein the first base key is determined from an identifier for the first group of cells; using the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells, using the first encryption key to encrypt communications between the communication device and the first radio access node via the second cell.

According to a second aspect, there is provided a first radio access node for use in a communication network. The first radio access node supports a plurality of cells that are divided into one or more groups of cells, where at least a first group of cells comprises more than one cell. The first radio access node is adapted or configured to (or comprises one or more modules configured to) determine a first base key for a communication device that is to connect to the first radio access node via a first cell in a first group of cells; wherein the first base key is determined from an identifier for the first group of cells; use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells.

According to a third aspect, there is provided a first radio access node for use in a communication network. The first radio access node comprises a processor and a memory, said memory containing instructions executable by said processor whereby said first radio access node is operative to perform the method according to the first aspect set out above.

According to a fourth aspect, there is provided a method of operating a communication device. The method comprises determining a first base key for a first cell in a first group of cells from an identifier for the first group of cells, the first group of cells being

supported by a first radio access node; using the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and, in the event that the communication device is to connect to a second cell in the first group of cells, using the first encryption key to encrypt communications between the communication device and the first radio access node via the second cell.

According to a fifth aspect, there is provided a communication device. The communication device is adapted or configured to (or comprises one or more modules configured to) determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, wherein the first group of cells are supported by a first radio access node; use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to a second cell in the first group of cells.

According to a sixth aspect, there is provided a communication device. The communication device comprises a processor and a memory, said memory containing instructions executable by said processor whereby said communication device is operative to perform the method according to the fourth aspect set out above.

According to a seventh aspect, there is provided a method of operating a node in a communication network. The method comprises determining a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells that are divided into one or more groups of cells, where at least the first group of cells comprises more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

According to an eighth aspect, there is provided a node for use in a communication network. The node is adapted or configured to (or comprises one or more modules configured to) determine a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells

that are divided into one or more groups of cells, where at least a first group of cells comprises more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

According to a ninth aspect, there is provided a node for use in a communication network. The node comprises a processor and a memory, said memory containing instructions executable by said processor whereby said node is operative to perform the method according to the seventh aspect set out above.

According to a tenth aspect, there is provided a computer program product comprising a non-transitory computer readable medium having computer readable code embodied therein. The computer readable code is configured such that, on execution by a suitable computer or processor, the computer or processor is caused to perform any of the method aspects set out above.

Particular embodiments may incorporate one or more of the aspects provided above and elements of certain aspects may be combined.

Brief Description of the Drawings

Certain embodiments of the techniques introduced in this document are described below with reference to the following figures, in which:

Figure 1 illustrates the signalling in a handover between a source eNB and a target eNB in an LTE network;

Figure 2 illustrates a UE moving between two cells;

Figure 3 illustrates a UE moving between four cells;

Figure 4 is a non-limiting example block diagram of a LTE cellular communications network;

Figure 5 is a block diagram of a communication device according to an embodiment;

Figure 6 is a block diagram of a radio access node according to an embodiment;

Figure 7 is a block diagram of a core network node according to an embodiment;

Figure 8 illustrates an exemplary grouping of cells into security areas according to an embodiment;

Figure 9 is a flow chart illustrating a method of operating a radio access node according to an embodiment;

Figure 10 is a flow chart illustrating a method of operating a communication device according to an embodiment;

Figure 11 is a flow chart illustrating a method of operating a node according to an embodiment;

Figure 12 is a block diagram of a first radio access node according to another embodiment;

Figure 13 is a block diagram of a communication device according to another embodiment;

Figure 14 is a block diagram of a node according to another embodiment;

Figure 15 is a block diagram of a first radio access node according to yet another embodiment;

Figure 16 is a block diagram of a communication device according to yet another embodiment; and

Figure 17 is a block diagram of a node according to yet another embodiment.

Detailed Description

The following sets forth specific details, such as particular embodiments for purposes of explanation and not limitation. But it will be appreciated by one skilled in the art that other embodiments may be employed apart from these specific details. In some instances, detailed descriptions of well-known methods, nodes, interfaces, circuits, and devices are omitted so as not obscure the description with unnecessary detail. Those

skilled in the art will appreciate that the functions described may be implemented in one or more nodes using hardware circuitry (e.g., analog and/or discrete logic gates interconnected to perform a specialized function, ASICs, PLAs, etc.) and/or using software programs and data in conjunction with one or more digital microprocessors or general purpose computers. Nodes that communicate using the air interface also have suitable radio communications circuitry. Moreover, where appropriate the technology can additionally be considered to be embodied entirely within any form of computer-readable memory, such as solid-state memory, magnetic disk, or optical disk containing an appropriate set of computer instructions that would cause a processor to carry out the techniques described herein.

Hardware implementation may include or encompass, without limitation, digital signal processor (DSP) hardware, a reduced instruction set processor, hardware (e.g., digital or analog) circuitry including but not limited to application specific integrated circuit(s) (ASIC) and/or field programmable gate array(s) (FPGA(s)), and (where appropriate) state machines capable of performing such functions.

In terms of computer implementation, a computer is generally understood to comprise one or more processors, one or more processing units, one or more processing modules or one or more controllers, and the terms computer, processor, processing unit, processing module and controller may be employed interchangeably. When provided by a computer, processor, processing unit, processing module or controller, the functions may be provided by a single dedicated computer, processor, processing unit, processing module or controller, by a single shared computer, processor, processing unit, processing module or controller, or by a plurality of individual computers, processors, processing units, processing modules or controllers, some of which may be shared or distributed. Moreover, these terms also refer to other hardware capable of performing such functions and/or executing software, such as the example hardware recited above.

Although in the description below the term user equipment (UE) is used, it should be understood by the skilled in the art that “UE” is a non-limiting term comprising any mobile device, communication device, wireless communication device, terminal device or node equipped with a radio interface allowing for at least one of: transmitting signals in uplink (UL) and receiving and/or measuring signals in downlink (DL). A UE herein may comprise a UE (in its general sense) capable of operating or at least performing

measurements in one or more frequencies, carrier frequencies, component carriers or frequency bands. It may be a "UE" operating in single- or multi-radio access technology (RAT) or multi-standard mode. As well as "UE", the general terms "terminal device", "communication device" and "wireless communication device" are used in the following description, and it will be appreciated that such a device may or may not be 'mobile' in the sense that it is carried by a user. Instead, the term "terminal device" (and the alternative general terms set out above) encompasses any device that is capable of communicating with communication networks that operate according to one or more mobile communication standards, such as the Global System for Mobile communications, GSM, UMTS, Long-Term Evolution, LTE, etc. A UE may comprise a Universal Subscription Identity Module (USIM) on a smart-card or implemented directly in the UE, e.g., as software or as an integrated circuit. The operations described herein may be partly or fully implemented in the USIM or outside of the USIM.

One or more cells are associated with a base station, where a base station comprises in a general sense any network node transmitting radio signals in the downlink and/or receiving radio signals in the uplink. Some example base stations, or terms used for describing base stations, are eNodeB, eNB, NodeB, macro/micro/pico/femto radio base station, home eNodeB (also known as femto base station), relay, repeater, sensor, transmitting-only radio nodes or receiving-only radio nodes. A base station may operate or at least perform measurements in one or more frequencies, carrier frequencies or frequency bands and may be capable of carrier aggregation. It may also be a single-radio access technology (RAT), multi-RAT, or multi-standard node, e.g., using the same or different base band modules for different RATs.

Unless otherwise indicated herein, the signalling described is either via direct links or logical links (e.g. via higher layer protocols and/or via one or more network nodes).

Figure 4 shows an example diagram of an evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (E-UTRAN) architecture as part of an LTE-based communications system 32 to which the techniques described herein can be applied. Nodes in a core network 34 part of the system 32 include one or more Mobility Management Entities (MMEs) 36, a key control node for the LTE access network, and one or more Serving Gateways (SGWs) 38 which route and forward user data packets while acting as a mobility anchor. They communicate with base stations or radio access nodes 40 referred to in LTE as eNBs,

over an interface, for example an S1 interface. The eNBs 40 can include the same or different categories of eNBs, e.g. macro eNBs, and/or micro/pico/femto eNBs. The eNBs 40 communicate with each other over an inter-node interface, for example an X2 interface. The S1 interface and X2 interface are defined in the LTE standard. A UE 42 is shown, and a UE 42 can receive downlink data from and send uplink data to one of the base stations 40, with that base station 40 being referred to as the serving base station of the UE 42.

Figure 5 shows a communication device/terminal device (UE) 42 that can be adapted or configured to operate according to one or more of the non-limiting example embodiments described. The UE 42 comprises a processor or processing unit 50 that controls the operation of the UE 42. The processing unit 50 is connected to a transceiver unit 52 (which comprises a receiver and a transmitter) with associated antenna(s) 54 which are used to transmit signals to and receive signals from a radio access node 40 in the network 32. The UE 42 also comprises a memory or memory unit 56 that is connected to the processing unit 50 and that contains instructions or computer code executable by the processing unit 50 and other information or data required for the operation of the UE 42.

Figure 6 shows a radio access node (for example a cellular network base station such as a NodeB or an eNodeB, eNB) that can be adapted or configured to operate according to the example embodiments described. The radio access node 40 comprises a processor or processing unit 60 that controls the operation of the radio access node 40. The processing unit 60 is connected to a transceiver unit 62 (which comprises a receiver and a transmitter) with associated antenna(s) 64 which are used to transmit signals to, and receive signals from, UEs 42 in the network 32. The radio access node 40 also comprises a memory or memory unit 66 that is connected to the processing unit 60 and that contains instructions or computer code executable by the processing unit 60 and other information or data required for the operation of the radio access node 40. The radio access node 40 also includes components and/or circuitry 68 for allowing the radio access node 40 to exchange information with another radio access node 40 (for example via an X2 interface), and/or with a core network node 36, 38 (for example via an S1 interface). It will be appreciated that base stations for use in other types of network (e.g. UTRAN or WCDMA RAN) will include similar components to those shown in Figure 6 and appropriate interface circuitry 68 for enabling communications with the other radio access nodes in those types of networks (e.g.

other base stations, mobility management nodes and/or nodes in the core network). It will be appreciated that a radio access node 40 can be implemented as a number of distributed functions in the radio access network (RAN).

Figure 7 shows a core network node 36, 38 that can be used in the example embodiments described. The node 36, 38 could be an MME 36, an SGW 38, or another type of core network node (e.g. a radio network controller, RNC). The node 36, 38 comprises a processing unit 70 that controls the operation of the node 36, 38. The processing unit 70 is connected to interface components and/or circuitry 72 for allowing the node 36, 38 to exchange information with network nodes in the radio access network (RAN), for example radio access nodes 40, which it is associated (which is typically via the S1 interface) and/or with other nodes in the core network part of the network. The node 36, 38 also comprises a memory unit 74 that is connected to the processing unit 70 and that stores program and other information and data required for the operation of the node 36, 38.

It will be appreciated that only the components of the UE 42, radio access node 40 and core network node 36, 38 discussed in the context of the embodiments presented herein are illustrated in Figures 5, 6 and 7.

Although the embodiments of the present disclosure will mainly be described in the context of LTE, it will be appreciated by those skilled in the art that the problems and solutions described herein are equally applicable to other types of wireless access networks and user equipments (UEs) implementing other access technologies and standards, and thus LTE (and the other LTE specific terminology used herein) should only be seen as examples of the technologies to which the techniques can be applied.

As noted above, there are several problems with the current handling of security in an LTE communication network, particularly relating to handling of security during the handover procedure between cells supported by the same radio base station (eNB). The techniques provided below therefore provide improvements in the way in which security is handled when a handover occurs between cells supported by the same eNB. In particular the techniques described herein provide a simple and fast way to allow a UE to enable and disable connectivity to an eNB through multiple cells (including PCells) that may have different EARFCN-DL, without having to reconfigure the encryption too frequently, for example in a deployment scenario where PDCP is

centralized or when several eNBs are allocated in the same hardware equipment. Currently such an action requires re-keying and hence causes significant processing delays and the need to storage packets in a buffer.

As part of the techniques described herein, for an eNB that supports a plurality of cells, the cells are grouped into one or more groups. These groups are referred to herein as "security areas", although this name should not be seen as limiting. Each group can comprise more than one cell, and it is possible for all of the cells of an eNB to be in the same group. At least a first group of cells comprises more than one cell, and in some embodiments, each group comprises at least two cells. Each of the security areas (groups) is given a respective identifier that is referred to herein as a "security area identifier". Thus, a "security area identifier" may be shared by two or more physical cells or beams.

The particular cells that belong to the same security area may be determined, e.g., based on whether the encryption of the traffic for the collection of cells is performed within the same secure environment. For example, an eNB may have a distributed architecture, where the encryption is performed in physically different hardware, and the main gain of changing K_{eNB} at a handover is, as pointed out above, to protect keys that are used in different physical eNBs (or physically different entities performing the functions of a distributed eNB implementation).

Within a security area, the techniques described herein provide that an Access Stratum (AS)-base key, for example K_{eNB} and encryption keys derived from it, for a particular communication device/terminal device (UE) can be reused by the UE in each of the cells of the security area (group). Put another way, the eNB 40, within a given security area, uses the same K_{eNB}, and encryption key derived from it, for a specific UE (and likewise the UE uses the same K_{eNB}, and encryption keys derived from it, for the different cells in the security area). It will be appreciated that if the same integrity or encryption algorithm is used and the K_{eNB} remains the same, then the encryption key and integrity key will also remain the same. This reuse of the keys enables the UE to move (e.g., handover) between cells in a group without the eNB 40 or UE 42 having to reconfigure the AS-base key, K_{eNB}, or an associated encryption key, and hence the eNB can seamlessly activate and deactivate cells for a UE inside the security area in a very fast and flexible way. If the UE moves (e.g., hands-over) to a cell that is in a different security area (e.g. a cell of the same eNB that is in a different group, or a cell

that is supported by a different eNB), then a new AS-base key (denoted K_{eNB}*) is derived by the relevant eNB 40 and the UE 42, along with a new encryption key, for use by the UE in that other security area. It will be appreciated that the UE and the eNB may share more than one K_{eNB} at any given time.

The following description indicates how to keep the K_{eNB} the same at different events relating to cell-change, and it will be understood by those skilled in the art that keeping the K_{eNB} the same will mean that the encryption key and integrity key will also remain the same provided that the same encryption/integrity protection algorithms are used.

It will be appreciated that with the above techniques the UE can reconnect to any cell within a particular security area and resume the current configuration, which comprises continuing to use the same K_{eNB} and encryption key. This reduces the setup delay considerably, thereby improving the end user experience and performance.

An exemplary grouping of cells into two groups for an eNB 40 is shown in Figure 8. In Figure 8, the eNB 40 has six cells, labelled Cell 1 to Cell 6. In this example, Cells 1-4 are grouped into one security area 80, and Cells 5 and 6 are grouped into a second security area 82.

It will be appreciated that although Cells 1-6 are shown as generally covering a respective geographical area, it is possible that two or more of the cells could substantially spatially overlap (for example if they use different frequencies).

The eNB 40 can inform the UE about which security area a certain cell belongs to, and the identifier for the security area. This information can be communicated to the UE in one of a number of ways, for example in system control information (e.g., in a System Information Block, SIB) or in dedicated UE signalling (e.g., Radio Resource Control (RRC), Radio Link Control (RLC), or Medium Access Control (MAC) signalling).

In some embodiments, the security configuration is, for all practical purposes, made distinct to the security area by making the AS-base key dependent on the security area itself. In particular, the AS-base key can be made dependent on the security area by deriving the AS-base key using the security area identifier as an input to the key-generation function. The AS-base key can be generated from different types of existing key material. For example, it can be generated from a previous AS-base key

(e.g., a K_{eNB}, and the new AS-base key would then correspond to the K_{eNB}*). It could also be generated from an NH value or K_{ASME}, as described above. The AS-base key can be derived from such previous keys using a Key Derivation Function (KDF), for example, HMAC-SHA256.

In conventional LTE, an eNB may prepare a number of potential target cells for handover. During the preparation, the eNB will provide the potential target cells with keying material to be used with the UE in case the UE is handed over to that particular target cell. To avoid an eNB of a potential target cell that is not selected for handover getting the keying material (e.g. K_{eNB}*) that is used between the actual target cell and the UE, the source eNB individually calculates the keying material for each potential target cell. Specifically, the source eNB includes the PCI and EARFCN-DL for the target cell in the key material calculation.

In contrast, by using the security area identifier in the derivation of the AS-base key, the result is that two or more prepared target cells that belong to different security areas will get different K_{eNB}*s. This ensures that if an attacker that gets hold of the K_{eNB}* of one of the prepared target cells, this will not jeopardise the security of the K_{eNB}*s of the other prepared target cells.

It is noted that this does not make the security model weaker. Even though there is a handover between two cells (within a security area), they are both controlled by the same eNB and hence an attacker that breaks into that eNB would, in the current security model in LTE, get the single K_{eNB} used for both cells. With the techniques described herein, the attacker would get both keys.

An example of generating a K_{eNB}* according to the above principle in the context of LTE is: AS-base key = KDF(K_{eNB}, S), where KDF is as defined in 3GPP TS 33.401 referenced above, K_{eNB} is the currently active K_{eNB}, and S is the set of parameters FC, P0, L0 encoded as defined in 3GPP TS 33.401, where FC is a functional code, P0 is an encoding of the security area identifier and L0 is the length of the encoding of the security area identifier in octets. It will be appreciated by those skilled in the art that other parameters can be included in the key derivation function call. Other derivation functions are also possible. The security area identifier may be encoded as an integer, a bit-string, an ASCII string or other representation. The important part is that the

same security area identifier is not used for two security areas that can be simultaneously prepared for handover of a UE, as described above.

The security area identifier is used to generate the AS-base key instead of a cell identity (e.g. the PCI) and frequency (e.g. the EARFCN-DL). By generating the AS-base key without using the PCI and EARFCN-DL of the PCell, the base key is not forced to be updated for each change in the PCell. It will be appreciated that in some embodiments the security area identifier might not be the only input to the AS-base key generation function, and it is possible for the AS-base key to be derived using other parameters in addition to the security area identifier.

The eNB 40 may establish a connection to the UE via one or more cells and release these connections using the same K_{eNB} (or at least the same encryption key) each time.

As noted above, an eNB 40 can be understood (and implemented) as a number of distributed functions, and the location of the security handling (i.e. PDCP and RRC) in the radio access network can decide how big the security areas can be without breaking any security principles.

An exemplary method of operating a radio access node (e.g. an eNB in an LTE network) 40 according to the techniques described herein is shown in Figure 9. The radio access node 40 (which is also referred to as the first radio access node below) supports a plurality of cells that are divided into one or more groups of cells. Each group may comprise more than one cell, with at least a first group of cells comprising more than one cell and each group has a respective identifier.

In a first step, step 901, the first radio access node 40 determines a first base key, referred to as a first AS-base key (e.g. a K_{eNB}) below for a communication device 42 that is to connect to the first radio access node 40 via a first cell in the first group of cells (e.g. via Cell 1 in security area 80 in Figure 8). In particular embodiments the first AS-base key is determined from an identifier for the first group of cells (i.e. the security area identifier described above). In these or further embodiments, the first AS-base key is determined without using an identifier that is unique to the first cell (e.g. a PCI) and/or an identifier of the frequency to be used in the first cell (e.g. an EARFCN-DL).

Next, in step 903, the first radio access node 40 uses the first AS-base key to determine a first encryption key that is to be used to encrypt communications between the communication device 42 and the first radio access node 40 via the first cell. The first encryption key can be used to encrypt communications, e.g. user plane data or control plane data, between the communication device 42 and the radio access node 40. It will be appreciated that respective encryption keys can be derived from the first AS-base key for encrypting each of user plane data and control plane data.

In step 905, which can be performed during a handover procedure to a second cell, it is determined whether the second cell that is in the first group of cells (e.g. one of Cells 2-4 in security area 80 in Figure 8).

If it is determined that the communication device 42 is to connect to a second cell that is in the first group of cells, then rather than determine a new base key (e.g. K_{eNB}*) and hence also a new encryption key as in a conventional system, the radio access node 40 uses the first encryption key to encrypt communications between the communication device 42 and the radio access node 40 via the second cell (step 907).

However, if at step 905 it is determined that the communication device 42 is to connect to a second cell that is not in the first group of cells then the first radio access node 40 (that is supporting the first cell) determines a second (AS-)base key for the communication device 42 for use with the second cell (step 909). In particular, the first radio access node 40 can determine the second base key from an identifier for the group of cells that the second cell is part of (e.g. from the identifier for security area 82 in Figure 8 if the second cell is Cell 5 or Cell 6) and the first AS-base key. It will be appreciated that in this case the second cell could be a cell in security area 82 in Figure 8 (i.e. a cell that also is supported by the first radio access node), or the second cell could be a cell that is supported by a different (second) radio access node.

Although not shown in Figure 9, just before or after step 909, the first radio access node 40 can determine whether the second cell is a cell that is supported by the first radio access node.

If the first radio access node 40 supports both the first cell and the second cell, then after step 909 the radio access node 40 uses the second base key to determine a second encryption key that is to be used to encrypt communications between the

communication device 42 and the first radio access node 40 via the second cell (step 911).

If the second cell is supported by a second radio access node, the second base key determined in step 909 is sent by the first radio access node to the second radio access node (i.e. step 911 as shown in Figure 9 is not performed in this case). The second radio access node then uses the received second base key to determine a second encryption key that is to be used to encrypt communications between the communication device 42 and the second radio access node via the second cell.

In some embodiments, the first radio access node can send an indication of the identifier for the first group of cells to the communication device 42 (so that the communication device 42 can also determine the first base key).

Figure 10 illustrates a method of operating a communication device (e.g. a UE) 42 according to the techniques presented herein. The communication device 42 is being served by a first radio access node 40 (e.g. an eNB) that supports a plurality of cells that are divided into one or more groups of cells. Each group may comprise more than one cell, with at least a first group of cells comprising more than one cell, and each group has a respective identifier.

When the communication device 42 connects to the first radio access node via a first cell (e.g. Cell 1 in security area 80 in Figure 8) in the first group of cells, the communication device 42 determines a first base key, referred to as a first AS-base key (e.g. K_{eNB}) below for the first cell (step 1001). In particular embodiments the first base key is determined from an identifier for the first group of cells (i.e. the security area identifier described above). In these or further embodiments, the first AS-base key is determined without using an identifier that is unique to the first cell (e.g. a PCI) and/or an identifier of the frequency to be used in the first cell (e.g. an EARFCN-DL).

Next, in step 1003, the communication device 42 uses the first AS-base key to determine a first encryption key that is to be used to encrypt communications between the communication device 42 and the first radio access node 40 via the first cell. The first encryption key can be used to encrypt communications, e.g. user plane data or control plane data, between the communication device 42 and the first radio access node 40 via the first cell. It will be appreciated that respective encryption keys can be

derived from the first AS-base key for encrypting each of user plane data and control plane data.

In step 1005, which can be performed during a handover procedure to a second cell, it is determined whether the second cell is in the first group of cells (e.g. one of Cells 2-4 in security area 80 in Figure 8).

If it is determined that the communication device 42 is to connect to a second cell that is in the first group of cells, then rather than determine a new AS-base key (e.g. K_{eNB}*) and hence also a new encryption key as in a conventional system, the communication device 42 uses the first encryption key to encrypt communications between the communication device 42 and the first radio access node 40 via the second cell (step 1007).

However, if at step 1005 it is determined that the communication device 42 is to connect to a second cell that is not in the first group of cells, then the communication device 42 determines a second AS-base key to use with that cell (step 1009). In particular, the communication device 42 can determine the second AS-base key from an identifier for the group of cells that the second cell is part of (e.g. from the identifier for security area 82 in Figure 8 if the second cell is Cell 5 or Cell 6) and the first AS-base key. It will be appreciated that in this case the second cell could be a cell in security area 82 in Figure 8 (i.e. a cell that also is supported by the first radio access node), or the second cell could be a cell that is supported by a different (second) radio access node.

The communication device 42 then uses the second AS-base key to determine a second encryption key that is to be used to encrypt communications via the second cell (step 1011). This second encryption key can then be used to encrypt communications via the second cell.

In some embodiments the communication device 42 can receive an indication of the identifier for the first group of cells from the first radio access node 40. In alternative embodiments, the communication device 42 can receive an indication of the identifier for the first group of cells from a node other than the first radio access node 40.

An exemplary method of operating a network node according to another embodiment of the techniques described herein is shown in Figure 11. This method relates to the operation of a node that is responsible for generating the base key from the security area identifier (if not the radio access node that is supporting the first cell that the communication device 42 is to communicate via), and thus could be a node in the core network part of the communication network (and for example the node could be an MME 36), or a node in the RAN of the communication network (e.g. an eNB 40, or a function or component that is part of a distributed eNB architecture).

Thus, in step 1101, for a communication device 42 that is to connect to a first radio access node 40 via a first cell in a group of cells supported by the first radio access node 40, the network node determines a first base key for use by the first radio access node and the communication device. The first base key is determined from an identifier for the first group of cells. The base key is to be used for determining an encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell.

Although not shown in Figure 11, the network node can send the first base key to the first radio access node via an inter-node interface (e.g. inter-node interface 68 or inter-node interface 72).

Figure 12 is a block diagram of a first radio access node 40 according to another embodiment. The first radio access node 40 is for use in a communication network 32, and supports a plurality of cells that are divided into one or more groups 80, 82 of cells, wherein at least a first group 80, 82 of cells comprises more than one cell. The first radio access node 40 comprises a processor 1201 and a memory 1202. The memory 1202 contains instructions executable by the processor 1201 such that the first radio access node 40 is operative to determine a first base key for a communication device 42 that is to connect to the first radio access node 40 via a first cell in the first group of cells, where the first base key is determined from an identifier for the first group of cells; use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device 42 and the first radio access node 40 via the first cell; and use the first encryption key to encrypt communications between the communication device 42 and the first radio access node 40 in the event that the communication device 42 is to connect to the first radio access node 40 via a second cell in the first group of cells.

Figure 13 is a block diagram of a communication device 42 according to another embodiment. The communication device 42 comprises a processor 1301 and a memory 1302. The memory 1302 contains instructions executable by the processor 1301 whereby the communication device 42 is operative to determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, where the first group of cells are supported by a first radio access node 40; use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device 42 and the first radio access node 40 via the first cell; and use the first encryption key to encrypt communications between the communication device 42 and the first radio access node 40 in the event that the communication device 42 is to connect to a second cell in the first group of cells.

Figure 14 is a block diagram of a node according to another embodiment. This node could be a node in the core network part of the communication network (and for example the node could be an MME 36), or a node in the RAN of the communication network (e.g. an eNB 40, or a function or component that is part of a distributed eNB architecture). The node 40 is for use in a communication network 32 and comprises a processor 1401 and a memory 1402. The memory 1402 contains instructions executable by the processor 1401 such that the node is operative to determine a first base key for use by a first radio access node 40 and a communication device 42 that is to connect to the first radio access node 40 via a first cell in a first group of cells, where the first radio access node 40 supports a plurality of cells that are divided into one or more groups of cells, with at least the first group of cells comprising more than one cell, and where the first base key is determined from an identifier for the first group of cells.

Figure 15 is a block diagram of a first radio access node 40 according to yet another embodiment. The first radio access node 40 is for use in a communication network 32, and supports a plurality of cells that are divided into one or more groups 80, 82 of cells, wherein at least a first group 80, 82 of cells comprises more than one cell. The first radio access node 40 comprises a determining module 1501 configured to determine a first base key for a communication device 42 that is to connect to the first radio access node 40 via a first cell in the first group of cells, where the first base key is determined from an identifier for the first group of cells; a first using module 1502 configured to use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device 42 and the first radio access node

40 via the first cell; and a second using module 1503 configured to use the first encryption key to encrypt communications between the communication device 42 and the first radio access node 40 in the event that the communication device 42 is to connect to the first radio access node 40 via a second cell in the first group of cells.

Figure 16 is a block diagram of a communication device 42 according to yet another embodiment. The communication device 42 comprises a determining module 1601 configured to determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, where the first group of cells are supported by a first radio access node 40; a first using module 1602 configured to use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device 42 and the first radio access node 40 via the first cell; and a second using module 1603 configured to use the first encryption key to encrypt communications between the communication device 42 and the first radio access node 40 in the event that the communication device 42 is to connect to a second cell in the first group of cells.

Figure 17 is a block diagram of a node according to yet another embodiment. This node could be a node in the core network part of the communication network (and for example the node could be an MME 36), or a node in the RAN of the communication network (e.g. an eNB 40, or a function or component that is part of a distributed eNB architecture). The node 40 is for use in a communication network 32 and comprises a determining module 1701 configured to determine a first base key for use by a first radio access node 40 and a communication device 42 that is to connect to the first radio access node 40 via a first cell in a first group of cells, where the first radio access node 40 supports a plurality of cells that are divided into one or more groups of cells, with at least the first group of cells comprising more than one cell, and where the first base key is determined from an identifier for the first group of cells.

Embodiments of the techniques described herein can provide a number of advantages. For example the techniques can provide the ability to combine several cells into a secure area within which the UE can securely move, switch or reconnect between the cells with minimum delay and low signalling cost. The techniques can also improve PDCP performance at packet forwarding (reduces processor requirements and buffering) since the same encryption key is used in the target and source cells. The techniques enable multi-connectivity in a more flexible way (UE and eNB can swap

between PCell and SCell without key reconfiguration). MFBI can be enhanced, where the EARFCN-DL of the PCell can be changed without requiring key reconfiguration. It is possible to reconnect fast even if the PCell is not the same as before. Support for centralised PDCP nodes can be improved since no re-keying is required at intra security area handover. The need to stall and synchronise component carriers other than the one that is actually being reconfigured is removed (this improves multi-connectivity handover where each component carrier could be configured individually). The techniques enable the possibility of using the already configured encryption in UE to send small data packets without having to go from IDLE to CONNECTED mode, still with the same level of security as CONNECTED. The network can be configured during cell planning so that the K_{eNB} is only changed when the risk level is too high. For example, there is no need to change the K_{eNB} for security purposes when performing a handover between two cells belonging to the same physical eNB. The techniques enable a simpler architecture that allows for a better split of user and control plane. Overall the techniques simplify key handling for the UE and RAN and reduces core network signalling at reconnect within the same security area.

Modifications and other variants of the described embodiment(s) will come to mind to one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the embodiment(s) is/are not to be limited to the specific examples disclosed and that modifications and other variants are intended to be included within the scope of this disclosure. Although specific terms may be employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Various embodiments are set out in the following statements:

1. A method of operating a first radio access node in a communication network, the first radio access node supporting a plurality of cells that are divided into one or more groups of cells, each group comprising more than one cell, the method comprising:

determining a first base key for a communication device that is to connect to the first radio access node via a first cell in a first group of cells; wherein the first base key is determined from an identifier for the first group of cells;

using the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells, using the first encryption key to encrypt communications between the terminal device and the first radio access node via the second cell.

2. A method as defined in statement 1, wherein the method further comprises the step of:

determining whether the communication device is to connect to a second cell in the first group of cells;

and wherein the step of using the first encryption key is performed if it is determined that the second cell is in the first group of cells.

3. A method as defined in statement 2, wherein if it is determined that the communication device is to connect to a second cell that is not in the first group of cells, the method further comprises the steps of:

determining a second base key for the communication device from an identifier for the group of cells that the second cell is part of.

4. A method as defined in statement 3, wherein the method further comprises the steps of:

determining whether the second cell is a cell that is supported by the first radio access node;

if the second cell is a cell that is supported by the first radio access node, using the second base key to determine a second encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the second cell, and using the second encryption key to encrypt communications between the terminal device and the first radio access node via the second cell; and

if the second cell is a cell that is not supported by the first radio access node, sending the second base key to the radio access node that is supporting the second cell.

5. A method as defined in any of statements 1-4, wherein the method further comprises the step of:

sending an indication of the identifier for the first group of cells to the communication device.

6. A method as defined in any of statements 1-5, wherein the first base key is an Access Stratum, AS, base key, K_{eNB}.

7. A method as defined in any of statements 1-6, wherein the first radio access node is an eNB in a Long Term Evolution, LTE, network.

8. A first radio access node for use in a communication network, the first radio access node supporting a plurality of cells that are divided into one or more groups of cells, each group comprising more than one cell, the first radio access node being adapted to:

determine a first base key for a communication device that is to connect to the first radio access node via a first cell in a first group of cells; wherein the first base key is determined from an identifier for the first group of cells;

use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell;

use the first encryption key to encrypt communications between the terminal device and the first radio access node in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells.

9. A method of operating a communication device, the method comprising:

determining a first base key for a first cell in a first group of cells from an identifier for the first group of cells, the first group of cells being supported by a first radio access node;

using the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

in the event that the communication device is to connect to a second cell in the first group of cells, using the first encryption key to encrypt communications between the communication device and the first radio access node via the second cell.

10. A method as defined in statement 9, wherein the method further comprises the step of:

determining whether the communication device is to connect to a second cell in the first group of cells;

and wherein the step of using the first encryption key is performed if it is determined that the second cell is in the first group of cells.

11. A method as defined in statement 10, wherein if it is determined that the communication device is to connect to a second cell that is not in the first group of cells, the method further comprises the steps of:

determining a second base key from an identifier for the group of cells that the second cell is part of;

using the second base key to determine a second encryption key; and

using the second encryption key to encrypt communications via the second cell.

12. A method as defined in any of statements 9-11, wherein the method further comprises the step of:

receiving an indication of the identifier for the first group of cells from the first radio access node.

13. A method as defined in any of statements 9-12, wherein the first base key is an Access Stratum, AS, base key, K_{eNB}.

14. A method as defined in any of statements 9-13, wherein the first radio access node is an eNB in a Long Term Evolution, LTE, network.

15. A communication device, the communication device being adapted to:

determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, wherein the first group of cells are supported by a first radio access node;

use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to a second cell in the first group of cells.

16. A method of operating a node in a communication network, the method comprising:

determining a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells that are divided into one or more groups of cells, each group comprising more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

17. A method as defined in statement 16, wherein the first base key is for determining a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell.

18. A method as defined in statement 16 or 17, wherein the method further comprises the step of:

sending the first base key to the first radio access node.

19. A method as defined in statement 16, 17 or 18, wherein the node is a node in a core network part of the communication network, or a node in a radio access part of the communication network.

20. A node for use in a communication network, the node being adapted to:

determine a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells that are divided into one or more groups of cells, each group comprising more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

21. A computer program product comprising a non-transitory computer readable medium having computer readable code embodied therein, the computer readable code being configured such that, on execution by a suitable computer or processor, the computer or processor is caused to perform the method of any of statements 1-7, 9-14 and 16-19.

Claims

1. A method of operating a first radio access node in a communication network, the first radio access node supporting a plurality of cells that are divided into one or more groups of cells, wherein at least a first group of cells comprises more than one cell, the method comprising:

determining (901) a first base key for a communication device that is to connect to the first radio access node via a first cell in the first group of cells; wherein the first base key is determined from an identifier for the first group of cells;

using (903) the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells, using (907) the first encryption key to encrypt communications between the communication device and the first radio access node via the second cell.

2. A method as defined in claim 1, wherein the method further comprises the step of:

determining (905) whether the communication device is to connect to a second cell in the first group of cells;

and wherein the step of using (907) the first encryption key is performed if it is determined that the second cell is in the first group of cells.

3. A method as defined in claim 2, wherein if it is determined that the communication device is to connect to a second cell that is not in the first group of cells, the method further comprises the steps of:

determining (909) a second base key for the communication device from an identifier for the group of cells that the second cell is part of.

4. A method as defined in claim 3, wherein the method further comprises the steps of:

determining whether the second cell is a cell that is supported by the first radio access node;

if the second cell is a cell that is supported by the first radio access node, using (911) the second base key to determine a second encryption key that is to be used to

encrypt communications between the communication device and the first radio access node via the second cell, and using the second encryption key to encrypt communications between the communication device and the first radio access node via the second cell; and

if the second cell is a cell that is not supported by the first radio access node, sending the second base key to the radio access node that is supporting the second cell.

5. A method as defined in any of claims 1-4, wherein the method further comprises the step of:

sending an indication of the identifier for the first group of cells to the communication device.

6. A method of operating a communication device, the method comprising:

determining (1001) a first base key for a first cell in a first group of cells from an identifier for the first group of cells, the first group of cells being supported by a first radio access node;

using (1003) the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

in the event that the communication device is to connect to a second cell in the first group of cells, using (1007) the first encryption key to encrypt communications between the communication device and the first radio access node via the second cell.

7. A method as defined in claim 6, wherein the method further comprises the step of:

determining (1005) whether the communication device is to connect to a second cell in the first group of cells;

and wherein the step of using (1007) the first encryption key is performed if it is determined that the second cell is in the first group of cells.

8. A method as defined in claim 7 wherein if it is determined that the communication device is to connect to a second cell that is not in the first group of cells, the method further comprises the steps of:

determining (1009) a second base key from an identifier for the group of cells that the second cell is part of;

using (1011) the second base key to determine a second encryption key; and

using the second encryption key to encrypt communications via the second cell.

9. A method as defined in any of claims 6-8, wherein the method further comprises the step of:

receiving an indication of the identifier for the first group of cells from the first radio access node.

10. A method of operating a node in a communication network, the method comprising:

determining (1101) a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells that are divided into one or more groups of cells, wherein at least the first group of cells comprises more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

11. A method as defined in claim 10, wherein the first base key is for determining a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell.

12. A method as defined in claim 10 or 11, wherein the method further comprises the step of:

sending the first base key to the first radio access node.

13. A method as defined in claim 10, 11 or 12, wherein the node is a node in a core network part of the communication network, or a node in a radio access part of the communication network.

14. A first radio access node (40) for use in a communication network (32), the first radio access node (40) supporting a plurality of cells that are divided into one or more groups of cells, wherein at least a first group of cells comprises more than one cell, the first radio access node (40) being adapted to:

determine a first base key for a communication device (42) that is to connect to the first radio access node (40) via a first cell in the first group of cells; wherein the first base key is determined from an identifier for the first group of cells;

use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device (42) and the first radio access node (40) via the first cell; and

use the first encryption key to encrypt communications between the communication device (42) and the first radio access node (40) in the event that the communication device (42) is to connect to the first radio access node (40) via a second cell in the first group of cells.

15. A first radio access node (40) as defined in claim 14, wherein the first radio access node (40) is further adapted to:

determine whether the communication device (42) is to connect to a second cell in the first group of cells;

and wherein the first radio access node (40) is adapted to use the first encryption key to encrypt communications between the communication device (42) and the first radio access node (40) if it is determined that the second cell is in the first group of cells.

16. A first radio access node (40) as defined in claim 15, wherein the first radio access node (40) is further adapted to:

determine a second base key for the communication device (42) from an identifier for the group of cells that the second cell is part of if it is determined that the communication device (42) is to connect to a second cell that is not in the first group of cells.

17. A first radio access node (40) as defined in claim 16, wherein the first radio access node (40) is further adapted to:

determine whether the second cell is a cell that is supported by the first radio access node (40);

use the second base key to determine a second encryption key that is to be used to encrypt communications between the communication device (42) and the first radio access node (40) via the second cell, and use the second encryption key to encrypt communications between the communication device (42) and the first radio access node (40) via the second cell if the second cell is a cell that is supported by the first radio access node (40); and

send the second base key to the radio access node (40) that is supporting the second cell if the second cell is a cell that is not supported by the first radio access node (40).

18. A first radio access node (40) as defined in any of claims 14-17, wherein the first radio access node (40) is further adapted to:

send an indication of the identifier for the first group of cells to the communication device (42).

19. A communication device (42), the communication device (42) being adapted to:

determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, wherein the first group of cells are supported by a first radio access node (40);

use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device (42) and the first radio access node (40) via the first cell; and

use the first encryption key to encrypt communications between the communication device (42) and the first radio access node (40) in the event that the communication device (42) is to connect to a second cell in the first group of cells.

20. A communication device (42) as defined in claim 19, wherein the communication device (42) is further adapted to:

determine whether the communication device (42) is to connect to a second cell in the first group of cells;

and wherein the communication device (42) is adapted to use the first encryption key to encrypt communications between the communication device (42) and the first radio access node (40) if it is determined that the second cell is in the first group of cells.

21. A communication device (42) as defined in claim 20 wherein the communication device (42) is further adapted to:

determine a second base key from an identifier for the group of cells that the second cell is part of if it is determined that the communication device (42) is to connect to a second cell that is not in the first group of cells;

use the second base key to determine a second encryption key; and

use the second encryption key to encrypt communications via the second cell.

22. A communication device (42) as defined in any of claims 19-21, wherein the communication device (42) is further adapted to:

receive an indication of the identifier for the first group of cells from the first radio access node (40).

23. A node (36; 38; 40) for use in a communication network (32), the node (36; 38; 40) being adapted to:

determine a first base key for use by a first radio access node (40) and a communication device (42) that is to connect to the first radio access node (40) via a first cell in a first group of cells, wherein the first radio access node (40) supports a plurality of cells that are divided into one or more groups of cells, wherein at least the first group of cells comprises more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

24. A node (36; 38; 40) as defined in claim 23, wherein the first base key is for determining a first encryption key that is to be used to encrypt communications between the communication device (42) and the first radio access node (40) via the first cell.

25. A node (36; 38; 40) as defined in claim 23 or 24, wherein the node (36; 38; 40) is further adapted to:

send the first base key to the first radio access node (40).

26. A node (36; 38; 40) as defined in claim 23, 24 or 25, wherein the node (36; 38; 40) is a node in a core network part of the communication network (32), or a node in a radio access part of the communication network (32).

27. A computer program product comprising a non-transitory computer readable medium having computer readable code embodied therein, the computer readable code being configured such that, on execution by a suitable computer or processor, the computer or processor is caused to perform the method of any of claims 1-13.

28. A first radio access node for use in a communication network, the first radio access node supporting a plurality of cells that are divided into one or more groups of cells, wherein at least a first group of cells comprises more than one cell, wherein the

first radio access node comprises a processor and a memory, said memory containing instructions executable by said processor whereby said first radio access node is operative to:

determine a first base key for a communication device that is to connect to the first radio access node via a first cell in the first group of cells; wherein the first base key is determined from an identifier for the first group of cells;

use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells.

29. A first radio access node as defined in claim 28, wherein the first radio access node is further operative to:

determine whether the communication device is to connect to a second cell in the first group of cells;

and wherein the first radio access node is operative to use the first encryption key to encrypt communications between the communication device and the first radio access node if it is determined that the second cell is in the first group of cells.

30. A first radio access node as defined in claim 29, wherein the first radio access node is further operative to:

determine a second base key for the communication device from an identifier for the group of cells that the second cell is part of if it is determined that the communication device is to connect to a second cell that is not in the first group of cells.

31. A first radio access node as defined in claim 30, wherein the first radio access node is further operative to:

determine whether the second cell is a cell that is supported by the first radio access node;

use the second base key to determine a second encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the second cell, and use the second encryption key to encrypt

communications between the communication device and the first radio access node via the second cell if the second cell is a cell that is supported by the first radio access node; and

send the second base key to the radio access node that is supporting the second cell if the second cell is a cell that is not supported by the first radio access node.

32. A first radio access node as defined in any of claims 28-31, wherein the first radio access node is further operative to:

send an indication of the identifier for the first group of cells to the communication device.

33. A communication device comprising a processor and a memory, said memory containing instructions executable by said processor whereby said communication device is operative to:

determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, wherein the first group of cells are supported by a first radio access node;

use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to a second cell in the first group of cells.

34. A communication device as defined in claim 33, wherein the communication device is further operative to:

determine whether the communication device is to connect to a second cell in the first group of cells;

and wherein the communication device is adapted to use the first encryption key to encrypt communications between the communication device and the first radio access node if it is determined that the second cell is in the first group of cells.

35. A communication device as defined in claim 34 wherein the communication device is further operative to:

determine a second base key from an identifier for the group of cells that the second cell is part of if it is determined that the communication device is to connect to a second cell that is not in the first group of cells;

use the second base key to determine a second encryption key; and

use the second encryption key to encrypt communications via the second cell.

36. A communication device as defined in any of claims 33-35, wherein the communication device is further operative to:

receive an indication of the identifier for the first group of cells from the first radio access node.

37. A node for use in a communication network, wherein the node comprises a processor and a memory, said memory containing instructions executable by said processor whereby said node is operative to:

determine a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells that are divided into one or more groups of cells, wherein at least the first group of cells comprises more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

38. A node as defined in claim 37, wherein the first base key is for determining a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell.

39. A node as defined in claim 37 or 38, wherein the node is further operative to:

send the first base key to the first radio access node.

40. A node as defined in claim 37, 38 or 39, wherein the node is a node in a core network part of the communication network, or a node in a radio access part of the communication network.

41. A first radio access node for use in a communication network, the first radio access node supporting a plurality of cells that are divided into one or more groups of cells, wherein at least a first group of cells comprises more than one cell, the first radio access node comprising:

a determining module configured to determine a first base key for a communication device that is to connect to the first radio access node via a first cell in the first group of cells; wherein the first base key is determined from an identifier for the first group of cells;

a first using module configured to use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

a second using module configured to use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to the first radio access node via a second cell in the first group of cells.

42. A first radio access node as defined in claim 41, wherein the first radio access node further comprises:

a second determining module configured to determine whether the communication device is to connect to a second cell in the first group of cells;

and wherein the second using module is configured to use the first encryption key to encrypt communications between the communication device and the first radio access node if the second determining module determines that the second cell is in the first group of cells.

43. A first radio access node as defined in claim 42, wherein the first radio access node further comprises:

a third determining module configured to determine a second base key for the communication device from an identifier for the group of cells that the second cell is part of if it is determined that the communication device is to connect to a second cell that is not in the first group of cells.

44. A first radio access node as defined in claim 43, wherein the first radio access node further comprises:

a fourth determining module configured to determine whether the second cell is a cell that is supported by the first radio access node;

a third using module configured to use the second base key to determine a second encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the second cell, and use the second encryption key to encrypt communications between the communication device

and the first radio access node via the second cell if the second cell is a cell that is supported by the first radio access node; and

a first sending module configured to send the second base key to the radio access node that is supporting the second cell if the second cell is a cell that is not supported by the first radio access node.

45. A first radio access node as defined in any of claims 41-44, wherein the first radio access node further comprises:

a second sending module configured to send an indication of the identifier for the first group of cells to the communication device.

46. A communication device, the communication device comprising:

a determining module configured to determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells, wherein the first group of cells are supported by a first radio access node;

a first using module configured to use the first base key to determine a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell; and

a second using module configured to use the first encryption key to encrypt communications between the communication device and the first radio access node in the event that the communication device is to connect to a second cell in the first group of cells.

47 A communication device as defined in claim 46, wherein the communication device further comprises:

a second determining module configured to determine whether the communication device is to connect to a second cell in the first group of cells;

and wherein the second using module is configured to use the first encryption key to encrypt communications between the communication device and the first radio access node if the second determining module determines that the second cell is in the first group of cells.

48. A communication device as defined in claim 47, wherein the communication device further comprises:

a third determining module configured to determine a second base key from an identifier for the group of cells that the second cell is part of if it is determined that the

communication device is to connect to a second cell that is not in the first group of cells;

a third using module configured to use the second base key to determine a second encryption key; and

a fourth using module configured to use the second encryption key to encrypt communications via the second cell.

49. A communication device as defined in any of claims 46-48, wherein the communication device further comprises:

a receiving module configured to receive an indication of the identifier for the first group of cells from the first radio access node.

50. A node for use in a communication network, the node comprising:

a determining module configured to determine a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells, wherein the first radio access node supports a plurality of cells that are divided into one or more groups of cells, wherein at least the first group of cells comprises more than one cell, and wherein the first base key is determined from an identifier for the first group of cells.

51. A node as defined in claim 50, wherein the first base key is for determining a first encryption key that is to be used to encrypt communications between the communication device and the first radio access node via the first cell.

52. A node as defined in claim 50 or 51, wherein the node further comprises:

a sending module configured to send the first base key to the first radio access node.

53. A node as defined in claim 50, 51 or 52, wherein the node is a node in a core network part of the communication network, or a node in a radio access part of the communication network.

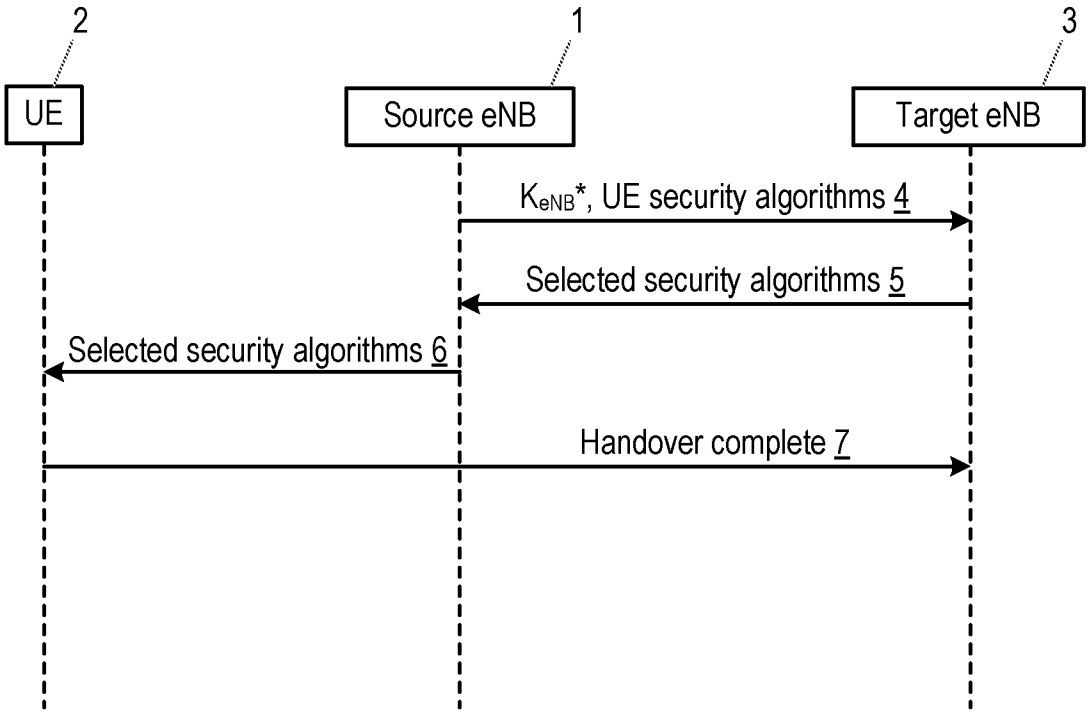
2
1
3
UE
Source eNB
Target eNB
K_{eNB}*, UE security algorithms 4
Selected security algorithms 5
Selected security algorithms 6
Handover complete 7

Figure 1

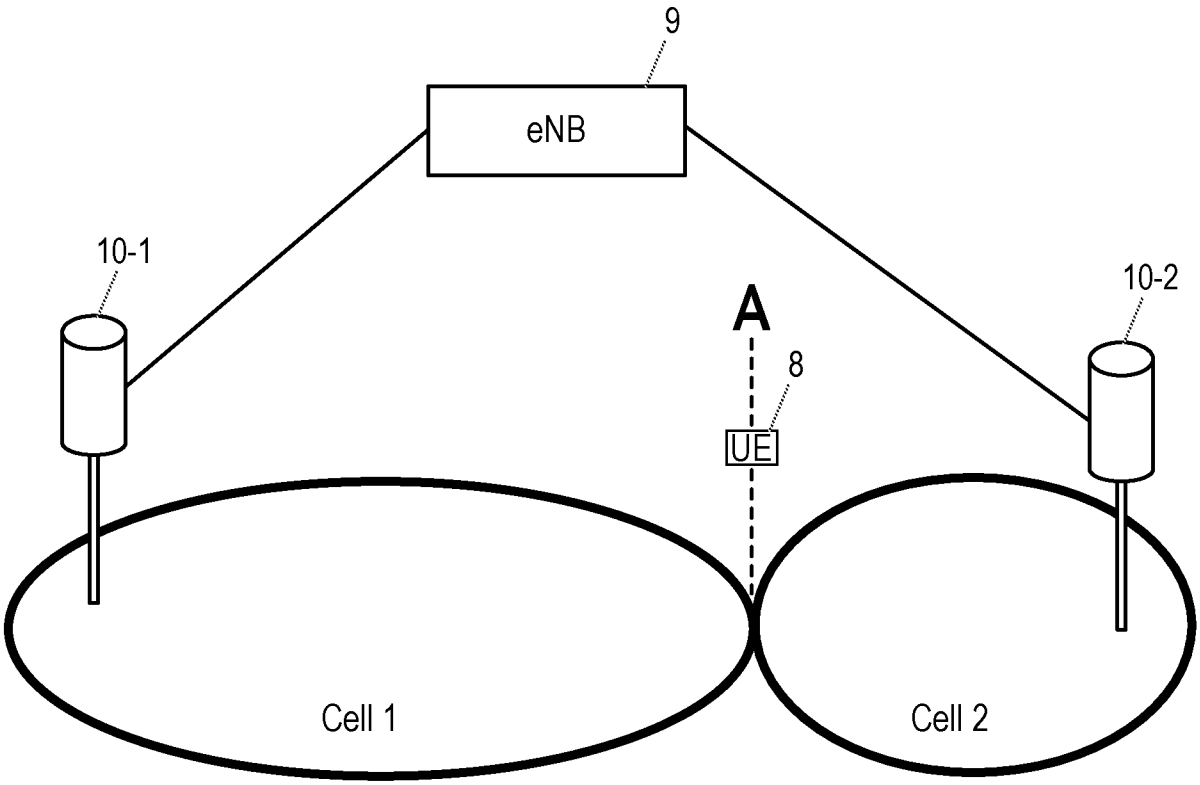

Figure 2

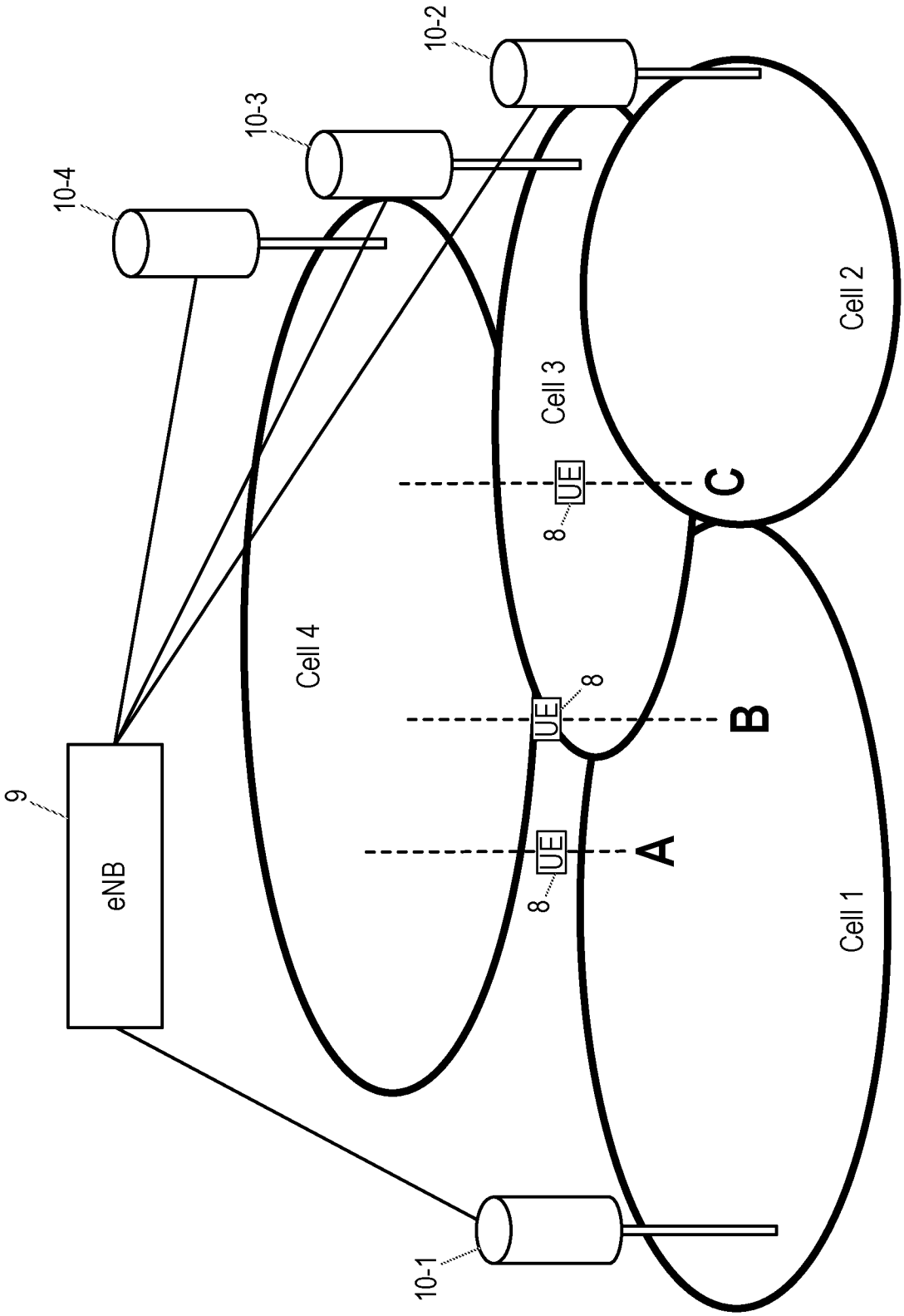

Figure 3

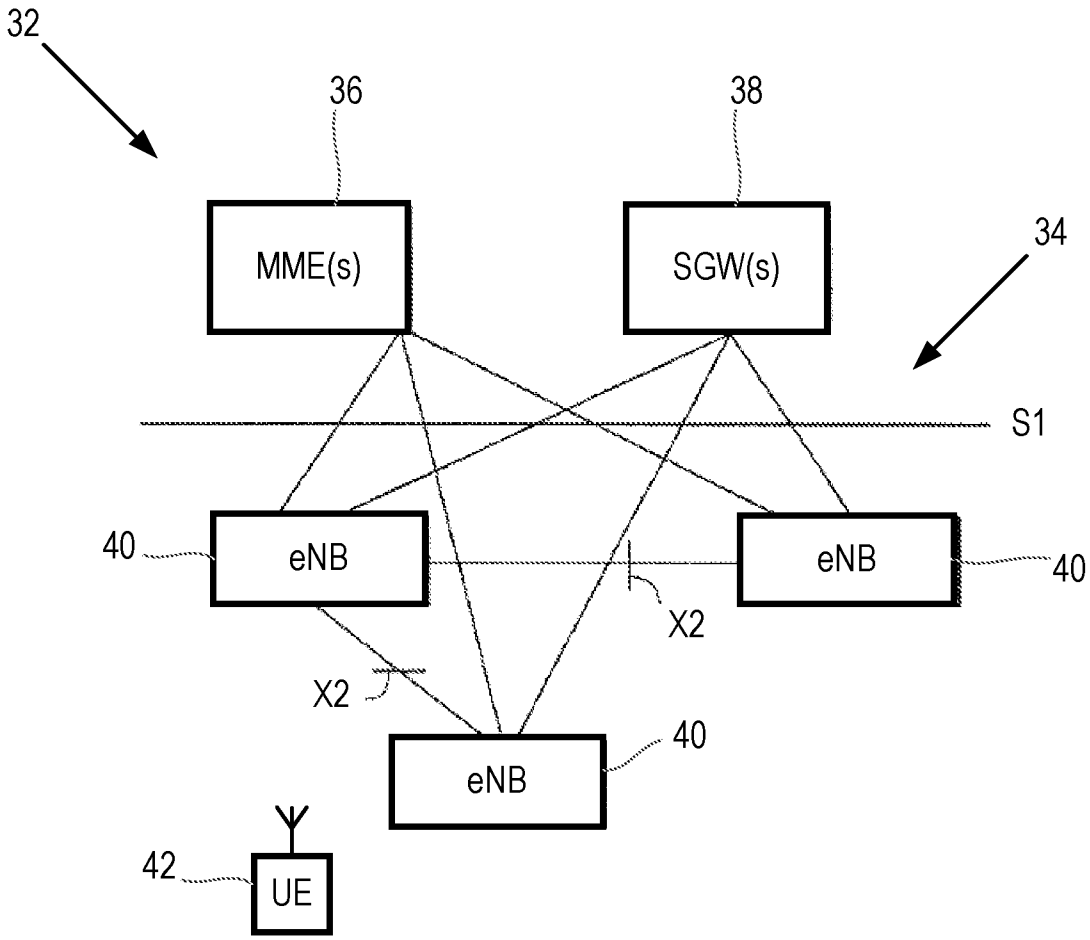

Figure 4

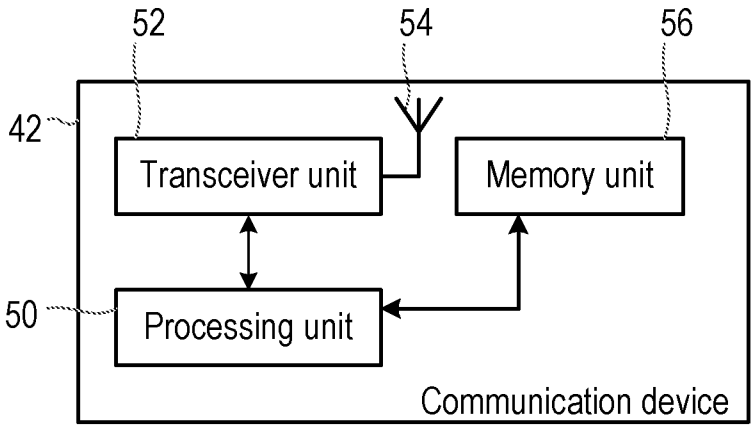

Figure 5

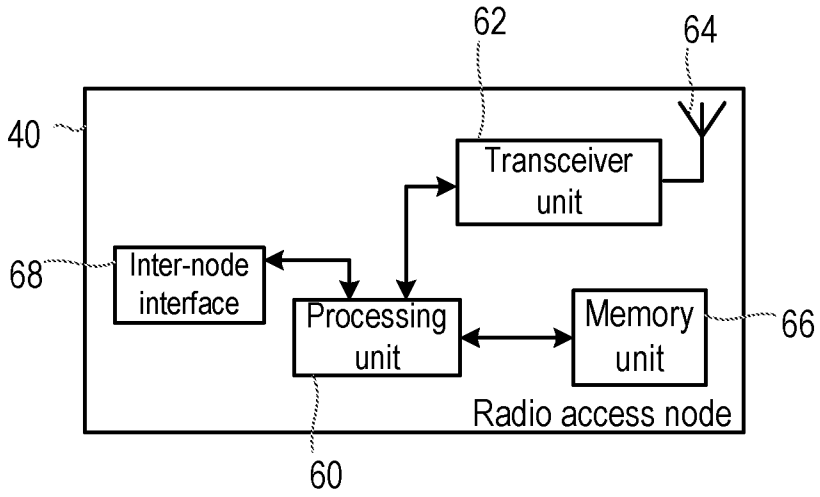

Figure 6

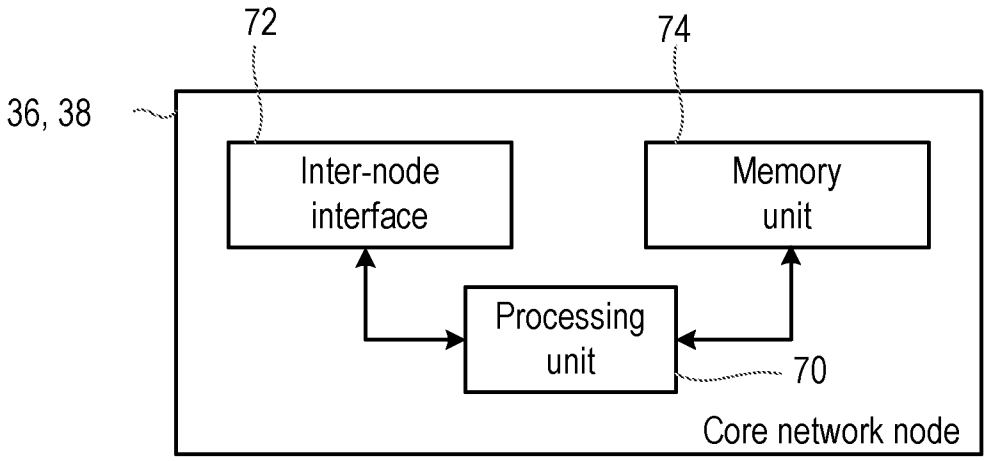

Figure 7

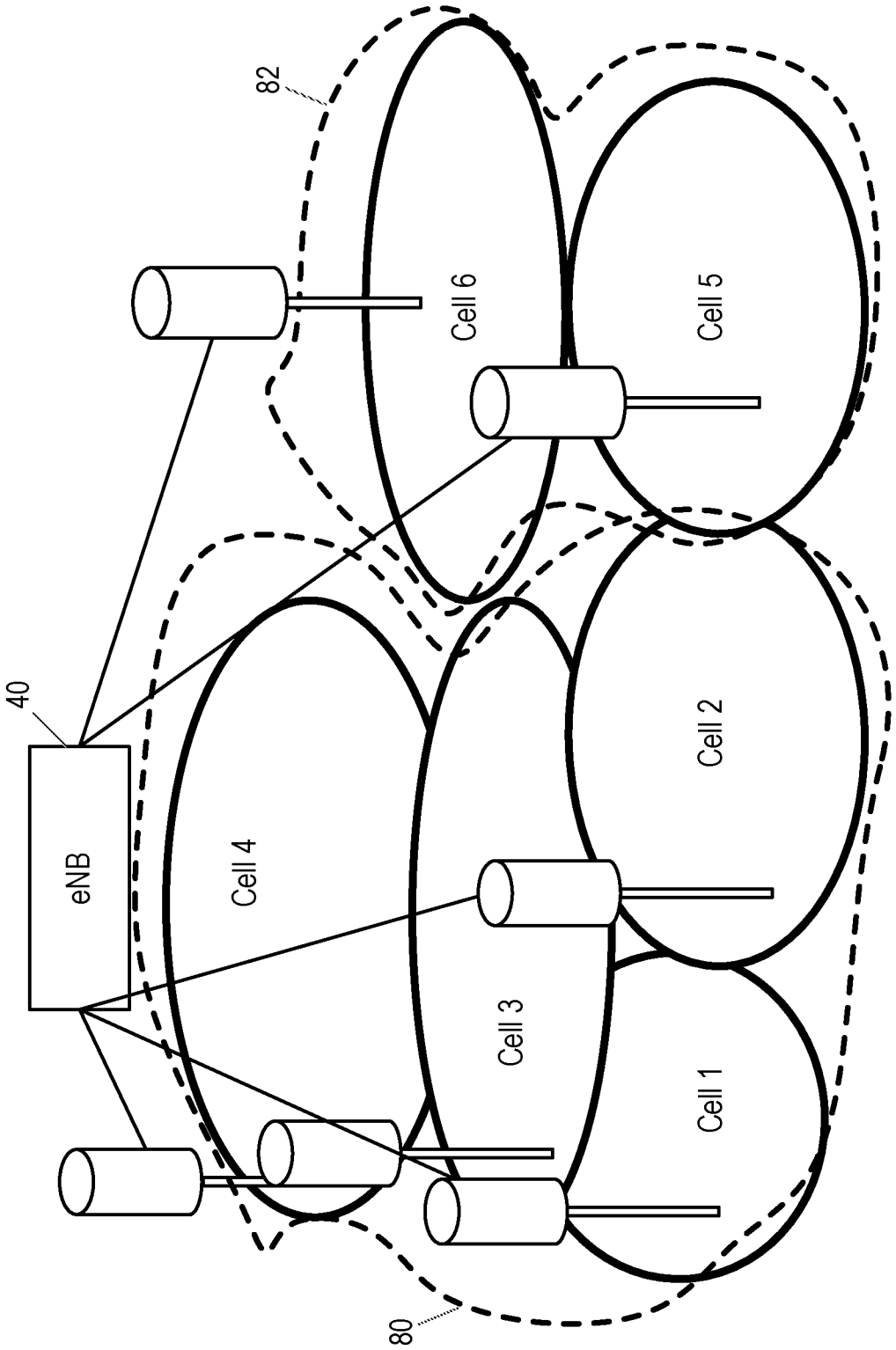

Figure 8

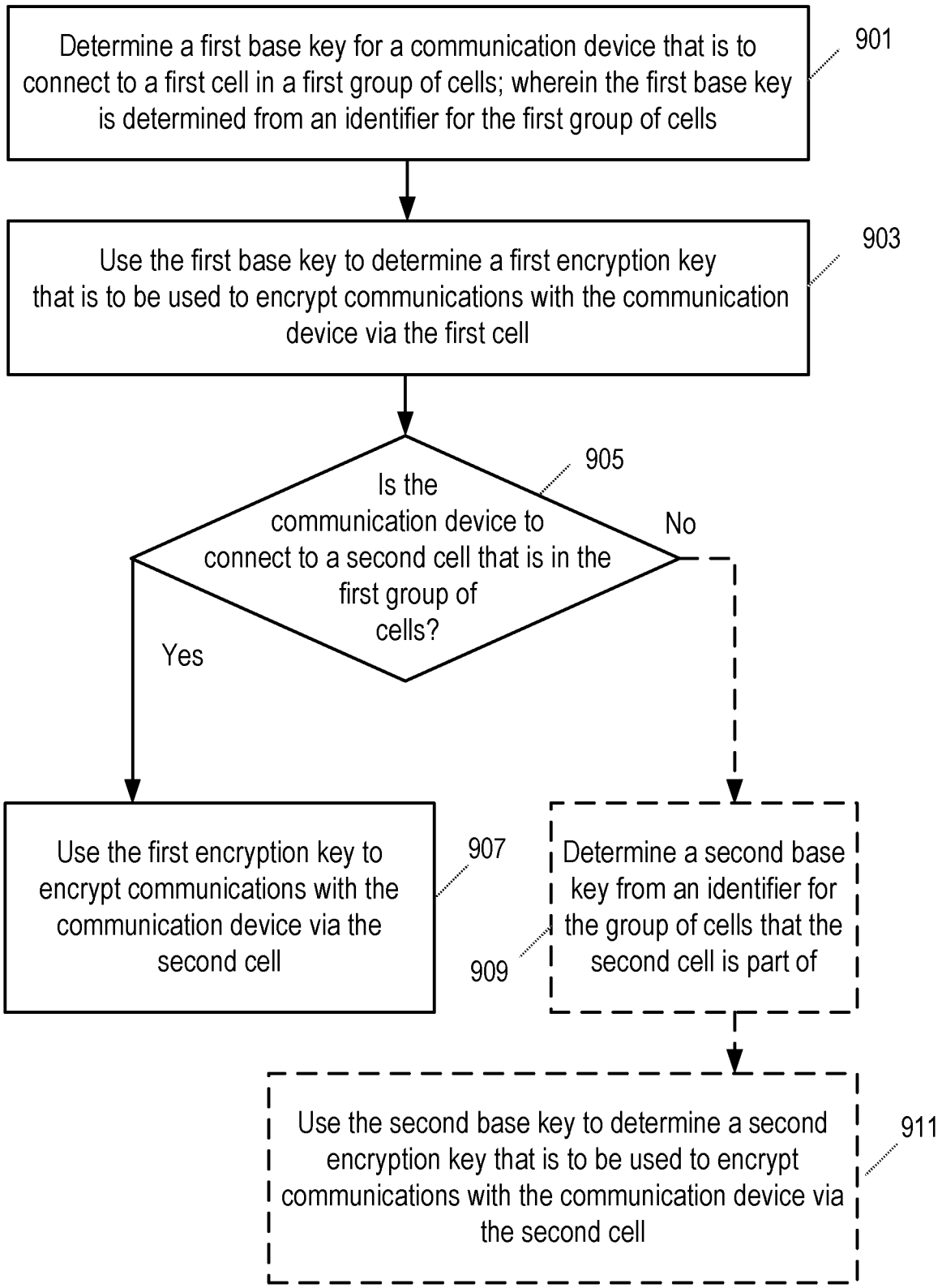
Determine a first base key for a communication device that is to connect to a first cell in a first group of cells; wherein the first base key is determined from an identifier for the first group of cells
901
Use the first base key to determine a first encryption key that is to be used to encrypt communications with the communication device via the first cell
903
Is the communication device to connect to a second cell that is in the first group of cells?
905
No
Yes
Use the first encryption key to encrypt communications with the communication device via the second cell
907
Determine a second base key from an identifier for the group of cells that the second cell is part of
909
Use the second base key to determine a second encryption key that is to be used to encrypt communications with the communication device via the second cell
911

Figure 9

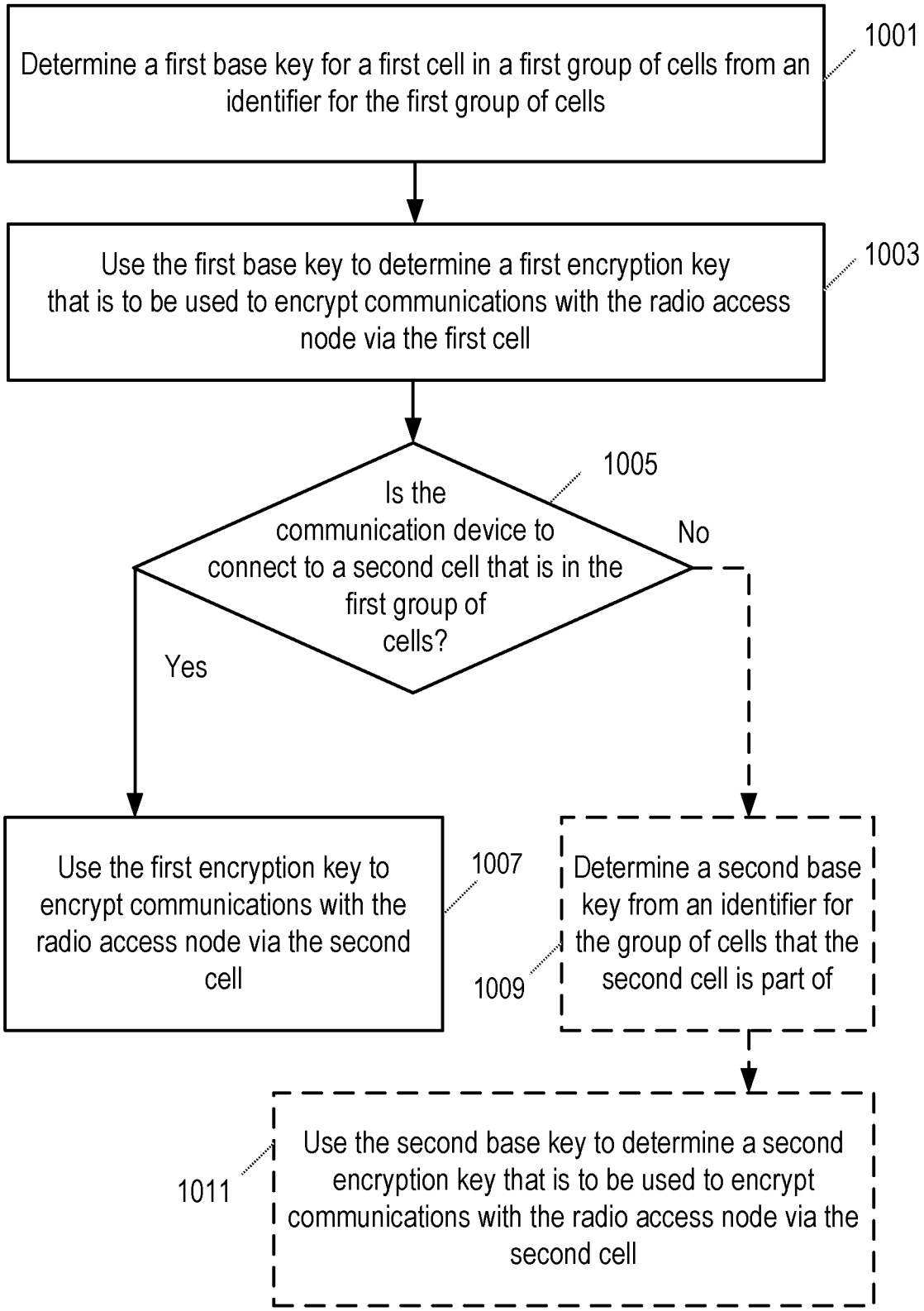
Determine a first base key for a first cell in a first group of cells from an identifier for the first group of cells
1001
Use the first base key to determine a first encryption key that is to be used to encrypt communications with the radio access node via the first cell
1003
Is the communication device to connect to a second cell that is in the first group of cells?
1005
No
Yes
Use the first encryption key to encrypt communications with the radio access node via the second cell
1007
Determine a second base key from an identifier for the group of cells that the second cell is part of
1009
Use the second base key to determine a second encryption key that is to be used to encrypt communications with the radio access node via the second cell
1011

Figure 10

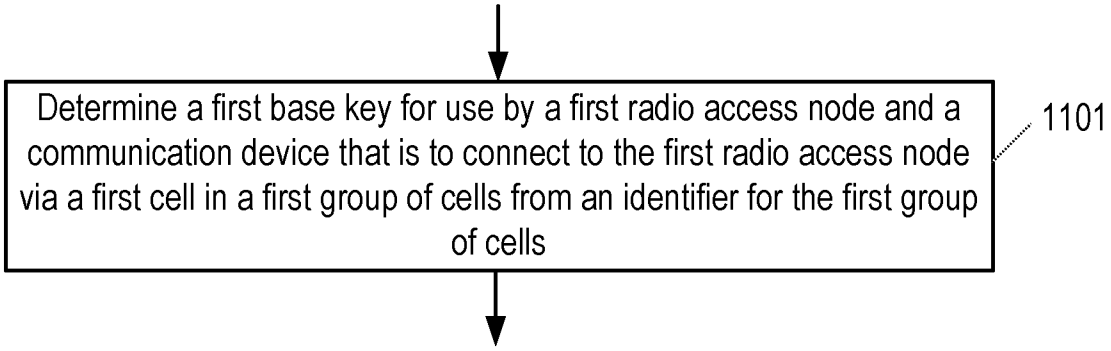
Determine a first base key for use by a first radio access node and a communication device that is to connect to the first radio access node via a first cell in a first group of cells from an identifier for the first group of cells
1101

Figure 11

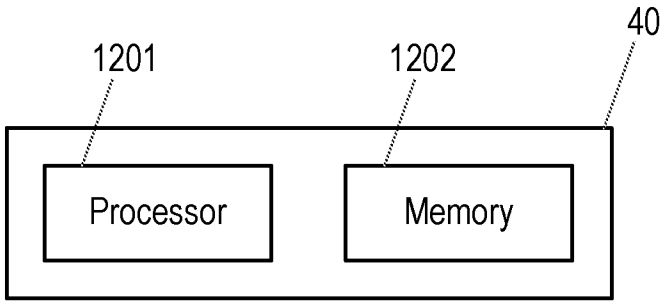

Figure 12

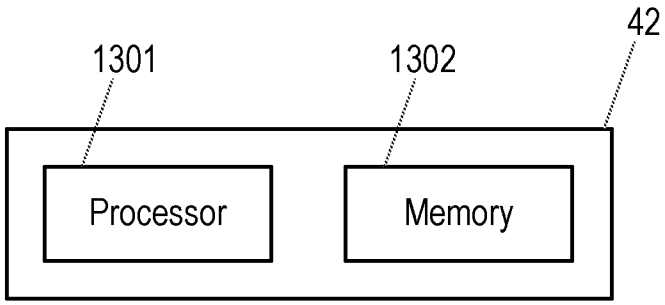

Figure 13

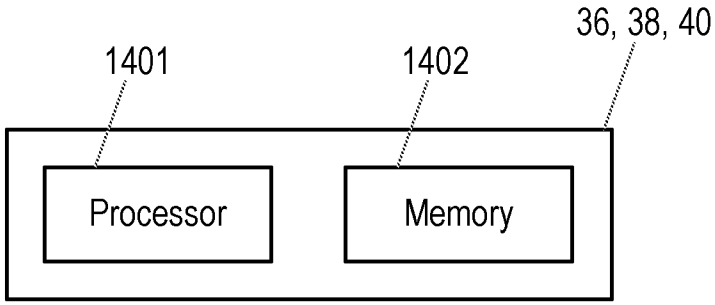

Figure 14

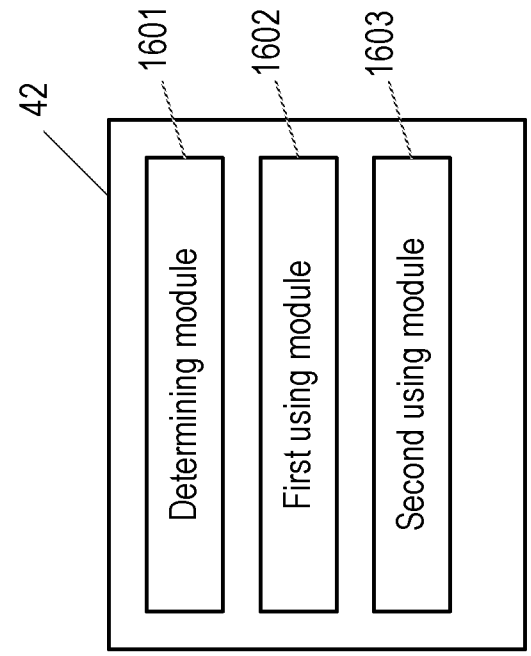

Figure 16

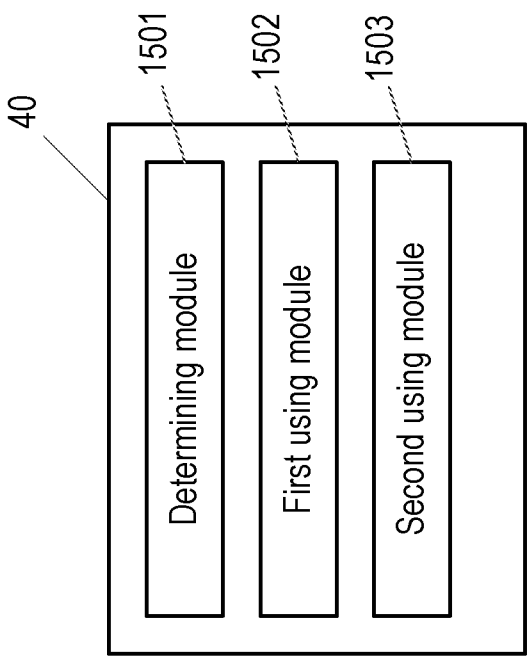

Figure 15

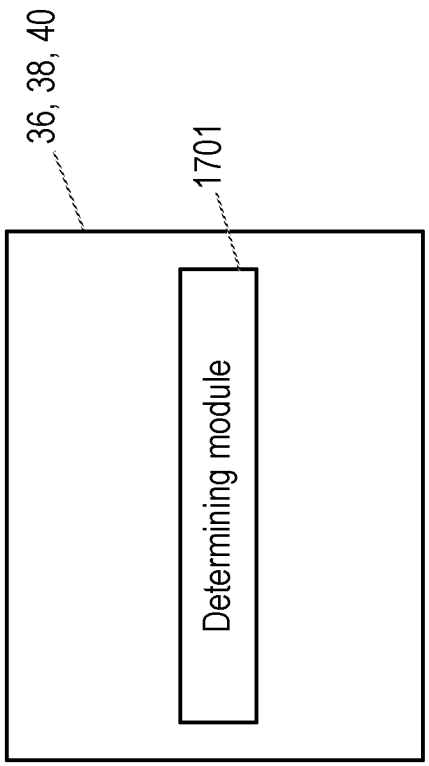

Figure 17

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2016/050880

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/02 H04W12/04 H04W36/00 H04L29/06
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 H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, COMPENDEX, INSPEC, IBM-TDB, 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	SAMSUNG: "Some security aspects of dual connectivity", 3GPP DRAFT; R2-141603_SCE_SECURITY_FINAL, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. RAN WG2, no. Valencia, Spain; 20140331 - 20140404 21 March 2014 (2014-03-21), XP050817589, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_85bis/Docs/ [retrieved on 2014-03-21] * section 2 * ----- -/--	1-53

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
3 November 2016	11/11/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Agudo Cortada, E

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2016/050880

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015/037926 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 19 March 2015 (2015-03-19) paragraphs [0003] - [0005], [0010] - [0015]	1-53
A	HUAWEI: "Security at RRC Connection Re-establishment", 3GPP DRAFT; R2-084309, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. Jeju; 20080812, 12 August 2008 (2008-08-12), XP050319389, [retrieved on 2008-08-12] * section 2 *	1-53

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/SE2016/050880

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2015037926 A1	19-03-2015	CN 105557007 A	04-05-2016
		EP 2965554 A1	13-01-2016
		US 2016029213 A1	28-01-2016
		US 2016044506 A1	11-02-2016
		US 2016205547 A1	14-07-2016
		WO 2015037926 A1	19-03-2015