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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 September 2010 (16.09.2010)

PCT

(10) International Publication Number
WO 2010/104992 A1

(51) International Patent Classification:
H04W 36/00 (2009.01)

(21) International Application Number:
PCT/US2010/026883

(22) International Filing Date:
10 March 2010 (10.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/159,048 10 March 2009 (10.03.2009) US

(71) Applicant *(for all designated States except US)*: **KINETO WIRELESS INC.** [US/US]; 1601 Mccarthy Blvd., Milpitas, CA 95035 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KHETAWAT, Amit** [US/US]; 1931 Bright Willow Circle, San Jose, CA 95131 (US). **TAO, Patrick** [CA/US]; 2636 Mosswood Drive, San Jose, CA 95132 (US).

(74) Agent: **ADELI, Mani**; Adeli & Tollen LLP, 11940 San Vicente Blvd. Suite 100, Los Angeles, CA 90049 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title**: NETWORK TRIGGERED UE RIGISTRATION ON IUH INTERFACE

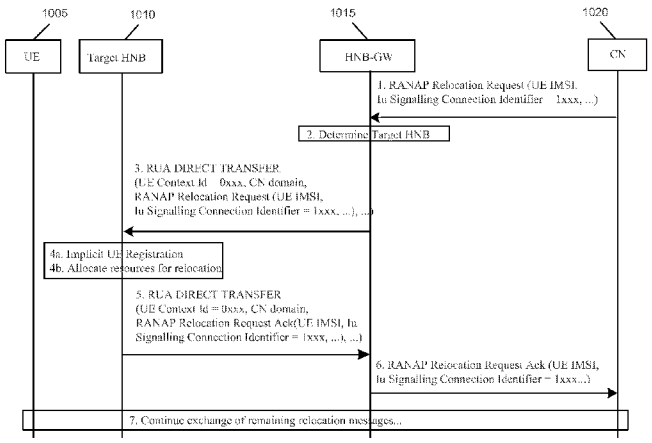

Figure 11

(57) **Abstract**: A method that receives, at a network controller, a handover message that includes a first connection identifier as an identifier for a signalling connection between the network controller and the core network. The method allocates, by the network controller, a different second connection identifier to identify a signalling connection between the network controller and an access point of a second wireless communication system communicatively connected to the network controller. The method sends the handover message and the second connection identifier to the access point. The method receives a reply message that includes the second connection identifier as the identifier for the signalling connection between the network controller and the core network. The method replaces, at the network controller, the second connection identifier in the reply message with the first connection identifier as the identifier for the signalling connection between the network controller and the core network.

WO 2010/104992 A1

NETWORK TRIGGERED UE REGISTRATION ON IUH INTERFACE

BACKGROUND

[0001] Licensed wireless systems provide mobile wireless communications to individuals using wireless transceivers. Licensed wireless systems refer to public cellular telephone systems and/or Personal Communication Services (PCS) telephone systems. Wireless transceivers, also referred to as user equipment (UE), include cellular telephones, PCS telephones, wireless-enabled personal digital assistants, wireless modems, and the like.

[0002] Licensed wireless systems utilize wireless signal frequencies that are licensed from governments. Large fees are paid for access to these frequencies. Expensive base station (BS) equipment is used to support communications on licensed frequencies. Base stations are typically installed approximately a mile apart from one another (e.g., cellular towers in a cellular network). In a Universal Mobile Telecommunications System (UMTS), these base stations are system provider controlled and include Node-Bs which are high power and long range radio frequency transmitters and receivers used to directly connect with the user equipment. The wireless transport mechanisms and frequencies employed by typical licensed wireless systems limit both data transfer rates and range.

[0003] Licensed wireless systems continually upgrade their networks and equipment in an effort to deliver greater data transfer rates and range. However, with each upgrade iteration (e.g., 3G to 4G), the licensed wireless system providers incur substantial costs from licensing additional bandwidth spectrum to upgrading the existing radio network equipment or core network equipment. To offset these costs, the licensed wireless system providers pass down the costs to the user through the licensed wireless service fees. Users also incur equipment costs with each iterative upgrade of the licensed wireless network as new user equipment is needed to take advantage of the new services or improved services of the upgraded network.

[0004] Landline (wired) connections are extensively deployed and generally perform at a lower cost with higher quality voice and higher speed data services than the licensed wireless systems. The problem with landline connections is that they constrain the mobility of a user. Traditionally, a physical connection to the landline was required.

[0005] Home Node Bs (HNBs) emerged as one solution to lower costs associated with the licensed wireless systems while maintaining user wireless mobility and taking advantage of the higher quality voice and higher speed data services of the landline connections. HNB allows users the ability to seamlessly and wirelessly roam in and out of Node B service regions and HNB service regions where the HNB systems facilitate mobile access to the landline-based networks. The mobility range associated with such HNB systems is typically on the order of 100 meters or less. A typical HNB communication system includes a base station comprising a wireless access point (AP) with a physical connection (e.g., coaxial, twisted pair, or optical cable) to a landline-based network. The AP has an RF transceiver to facilitate communication with a wireless handset that is operative within a modest distance of the AP.

[0006] HNB communication systems allow users to purchase ordinary off-the-shelf access points in order to deploy a HNB service region that allows for access to HNB service. In this manner, HNB is able to provide higher quality services at a lower cost than the licensed wireless macro cell.

[0007] Accordingly, HNBs are low cost versions of the expensive Base Stations that comprise the mobile network that still use the operator's licensed spectrum for communication with licensed devices. The use of regular landlines required the HNBs to adopt proprietary messaging and signaling standards that were different than those used by the licensed wireless systems for the expensive Base Stations.

[0008] Accordingly, there is a need in the art to develop a simplified integrated system that leverages the mobility provided by licensed wireless systems while maintaining the quality of service and data transfer rates of landline connections. Such a simplified integrated system needs to reduce adoption costs for both the individual user and the system provider that deploys such a system.

BRIEF SUMMARY

[0009] In 3GPP Standard, an Iu signalling connection identifier uniquely identifies an Iu signalling connection between a given radio network controller (RNC) and a given core network (CN). Furthermore, it is also described that the most significant bit (MSB) of an Iu signalling connection identifier of a Radio Access Network Application Part (RANAP) message indicates the node that has assigned a value to the identifier. When the value is assigned to the identifier by the CN, the MSB of the identifier has to be 1 and when it is assigned by RNC or HNB-GW the MSB has to be 0.

[0010] A UE Context Id is also a unique identifier allocated by the HNB gateway (HNB-GW) for a particular UE, as described in 3GPP Standard. Also, as described in 3GPP Standard, a user equipment (UE) Context Id can be utilized as an Iu signalling connection identifier value for use in the RANAP messages exchanged by a HNB and the HNB-GW. The HNB-GW must take into account the rules described above when allocating UE Context Ids. Therefore, when a UE Context Id allocated by a HNB-GW is utilized as Iu signalling connection identifier value, the MSB of the UE Context Id must be a 0 because it is the HNB-GW that assigned a value to the Iu signalling connection identifier and RANAP messages which are initiated by the radio access network shall have MSB of Iu signalling connection identifier set to value 0.

[0011] The above rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value pose a problem when applied during a handover procedure from a macro network cell to a target HNB. Specifically, the RANAP messages (for example, RANAP Relocation Request message) which are initiated from the CN and which trigger the creation of UE registration by the HNB-GW, carry the Iu signalling connection identifier allocated by the CN. These same messages will also result in creation of UE associated signalling connection over the Iuh interface. This will require the HNB-GW to allocate a context Id for the UE registration. However, the context Id which the HNB-GW allocated must have the MSB set to 0 and hence cannot have the same value as that assigned to the "Iu signalling connection identifier" IE in the corresponding RANAP message triggered by the CN which must have the MSB set to 1. A handover message from the core network includes a connection identifier which includes information indicating the core network assigned a value to the connection identifier. It is a rule that a message constructed by an access

point must include a connection identifier that includes information indicating the network controller assigned a value to the connection identifier. Even when an access point constructs a message in response to the handover message from the core network, the access point must follow the rule. However, if the access point follows the rule and uses a connection identifier that includes information indicating the network controller assigned a value to the connection identifier for the reply message, the core network would not be able to recognize that the reply message is in response to the handover message because the reply message would have a connection identifier different from the connection identifier included in the handover message.

[0012] Some embodiments provide a first solution to the above mentioned problem. In the first solution, the access point uses the connection identifier of the handover message as the connection identifier of the reply message in response to the handover message. For other messages the access point constructs, the access point uses a connection identifier that includes information indicating the network controller assigned a value to the connection identifier.

[0013] Some embodiments provide a second solution. In the second solution, the access point uses a connection identifier that includes information indicating the network controller assigned a value to the connection identifier, for all messages it constructs. The network controller ensures that, for the messages that are in response to the messages from the core network, a connection identifier that includes information indicating the core network controller assigned a value to the connection identifier.

[0014] Some embodiments are implemented in a communication system that includes a first wireless communication system that includes a licensed wireless radio access network and a core network and a second wireless communications system that includes several unplanned and user deployed access points for establishing service regions of the second network using short-range licensed wireless frequencies and a network controller for communicatively coupling a user equipment (UE) operating in the service regions to the core network.

[0015] Some embodiments provide a method of handling a handover of an ongoing session of a user equipment (UE) in a communication system. The method receives, at the network controller, a message from the core network. The message includes a first connection identifier as an identifier for a signalling connection associated with the UE between the network controller and the core network. The method also allocates, by the network controller, a second

connection identifier to identify a signalling connection associated with the UE between the network controller and an access point of the second wireless communication system communicatively connected to the network controller. The second connection identifier is different than the first connection identifier. The method also sends the message and the second connection identifier from the network controller to the access point. The method also receives a reply message from the access point in response to the message. The reply message includes the second connection identifier as the identifier for the signalling connection associated with the UE between the network controller and the core network. The method also replaces, at the network controller, the second connection identifier in the reply message with the first connection identifier as the identifier for the signalling connection associated with the UE between the network controller and the core network. The method sends the reply message from the network controller to the core network. In some embodiments, the first and second identifiers indicate the communication system node (e.g., CN, RNC, HNB-GW) that has assigned the value to the identifier. In some embodiments, the first and second identifiers indicate the communication system node (e.g., CN, RNC, HNB-GW) that has assigned the identifier. In some embodiments, the first and second identifiers indicate the communication system node (e.g., CN, RNC, HNB-GW) that has assigned the signalling connection.

[0016] Some embodiments provide a computer readable medium of the network controller that stores a computer program. The computer program includes instructions that are executable by one or more processors. In some embodiments, the computer program includes a set of instruction for receiving a message from the core network. The message includes a first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for allocating a second connection identifier to identify a connection associated with the UE between the network controller and an access point of the second wireless communication system communicatively connected to the network controller. The second connection identifier is different than the first connection identifier. The computer program also includes a set of instructions for sending the message and the second connection identifier to the access point. The computer program also includes a set of instructions for receiving a reply message from the access point in response to the message. The reply message includes the second connection identifier as the identifier for the connection associated with the UE between

the network controller and the core network. The computer program also includes a set of instructions for replacing the second connection identifier in the reply message with the first connection identifier as the identifier for the connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for sending the reply message to the core network.

[0017] Some embodiments provide a method of handling a handover of an ongoing session of a user equipment (UE) in a communication system. The method receives a message at an access point of the plurality of access points from the network controller. The message includes (i) a first connection identifier as an identifier for a first connection associated with the UE between the network controller and a first node of the communication system and (ii) a second connection identifier allocated by the network controller. The second connection identifier is to identify a second connection associated with the UE between the network controller and the access point. The second connection identifier is different than the first connection identifier. The method also determines whether the first connection identifier identifies the first connection as a connection between the network controller and the core network. When the first connection identifier identifies the first connection as a connection between the network controller and the core network, the method sends a reply message from the access point to the network controller. The reply message includes the first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network. When the first connection identifier identifies the first connection as a connection between the network controller and a node of the communication system other than the core network, the method sends a reply message from the access point to the network controller. The reply message includes the second connection identifier as an identifier for a connection associated with the UE between the network controller and the node of the communication system.

[0018] Some embodiments provide a computer readable medium of an access point that stores a computer program. The computer program includes instruction that are executable by one or more processors. In some embodiments, the computer program includes a set of instructions for receiving a message from the network controller. The message includes (i) a first connection identifier as an identifier for a first connection associated with the UE between the

network controller and a first node of the communication system and (ii) a second connection identifier allocated by the network controller. The second connection identifier is to identify a second connection associated with the UE between the network controller and the access point. The second connection identifier is different than the first connection identifier. The computer program also includes a set of instructions for determining whether the first connection identifier identifies the first connection as a connection between the network controller and the core network. The computer program also includes a set of instructions for, when the first connection identifier identifies the first connection as a connection between the network controller and the core network, sending a reply message to the network controller. The reply message includes the first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for, when the first connection identifier identifies the first connection as a connection between the network controller and a node of the communication system other than the core network, sending a reply message to the network controller. The reply message includes the second connection identifier as an identifier for a connection associated with the UE between the network controller and the node of the communication system.

[0019] The preceding Summary is intended to serve as a brief introduction to some embodiments of the invention. It is not meant to be an introduction or overview of all inventive subject matter disclosed in this document. The Detailed Description that follows and the Drawings that are referred to in the Detailed Description will further describe the embodiments described in the Summary as well as other embodiments. Accordingly, to understand all the embodiments described by this document, a full review of the Summary, Detailed Description and the Drawings is needed. Moreover, the claimed subject matters are not to be limited by the illustrative details in the Summary, Detailed Description and the Drawing, but rather are to be defined by the appended claims, because the claimed subject matters can be embodied in other specific forms without departing from the spirit of the subject matters.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The novel features of the invention are set forth in the appended claims. However, for purpose of explanation, several embodiments of the invention are set forth in the following figures.

[0021] **Figure 1** illustrates a system architecture for 3G HNB deployments in accordance with some embodiments of the invention.

[0022] **Figure 2** illustrates elements of the HNB Access Network (HNB-AN) sub-system architecture in accordance with some embodiments.

[0023] **Figure 3** illustrates the Home Node-B (HNB) system architecture including the HNB-AN of some embodiments integrated with a core network of a second communication system that includes a licensed wireless radio access network.

[0024] **Figure 4** illustrates some of the various devices that may be used in some embodiments in order to access services of the HNB-AN or HNB system.

[0025] **Figure 5** illustrates the protocol architecture supporting the HNB Application Part (HNBAP) over the Iuh interface, in some embodiments.

[0026] **Figure 6** illustrates the protocol architecture in support of the HNB control plane (i.e., for both the CS and PS domain), in some embodiments.

[0027] **Figure 7** illustrates UE registration with the HNB in some embodiments.

[0028] **Figure 8** illustrates a procedure for the HNB-GW to allow UE registration using temporary identity in some embodiments.

[0029] **Figure 9** illustrates implicit UE registration in some embodiments.

[0030] **Figure 10** illustrates the CS or PS Handover from a macro network cell to HNB procedure in some embodiments.

[0031] **Figure 11** illustrates the CS or PS Handover from a macro network cell to HNB procedure in some embodiments.

[0032] **Figure 12** illustrates the CS or PS Handover from a macro network cell to HNB procedure in some embodiments.

[0033] **Figure 13** illustrates the CS or PS Handover from one HNB to another HNB procedure in some embodiments.

[0034] **Figure 14** illustrates the CS or PS Handover from one HNB to another HNB procedure in some embodiments.

[0035] **Figure 15** illustrates the CS or PS Handover from one HNB to another HNB procedure in some embodiments.

[0036] **Figure 16** illustrates an explicit UE registration in some embodiments.

[0037] **Figure 17** illustrates the CS or PS Handover from macro network to HNB procedure in some embodiments.

[0038] **Figure 18** illustrates the CS or PS Handover from one HNB to another HNB procedure in some embodiments.

[0039] **Figure 19** conceptually illustrates a computer system with which some embodiments are implemented.

DETAILED DESCRIPTION

[0040] In the following detailed description of the invention, numerous details, examples, and embodiments of the invention are set forth and described. However, it will be clear and apparent to one skilled in the art that the invention is not limited to the embodiments set forth and that the invention may be practiced without some of the specific details and examples discussed.

[0041] Throughout the following description, acronyms commonly used in the telecommunications industry for wireless services are utilized along with acronyms specific to the present invention. A table of acronyms used in this application is included in Section V.

[0042] Some embodiments provide a first solution to the above mentioned problem. In the first solution, the access point uses the connection identifier of the message as the connection identifier of the reply message in response to the message. For other messages the access point constructs, the access point uses a connection identifier that includes information indicating the network controller assigned a value to the connection identifier.

[0043] Some embodiments provide a second solution. In the second solution, the access point uses a connection identifier that includes information indicating the network controller assigned a value to the connection identifier, for all messages it constructs. The network controller ensures that, for the messages that are in response to the messages from the core network, a connection identifier that includes information indicating the core network controller assigned a value to the connection identifier.

[0044] Some embodiments are implemented in a communication system that includes a first wireless communication system that includes a licensed wireless radio access network and a core network and a second wireless communications system that includes several unplanned and user deployed access points for establishing service regions of the second network using short-range licensed wireless frequencies and a network controller for communicatively coupling a user equipment (UE) operating in the service regions to the core network.

[0045] Some embodiments provide a method of handling a handover of an ongoing session of a user equipment (UE) in a communication system. The method receives, at the network controller, a message from the core network. The message includes a first connection

identifier as an identifier for a signalling connection associated with the UE between the network controller and the core network. The method also allocates, by the network controller, a second connection identifier to identify a signalling connection associated with the UE between the network controller and an access point of the second wireless communication system communicatively connected to the network controller. The second connection identifier is different than the first connection identifier. The method also sends the message and the second connection identifier from the network controller to the access point. The method also receives a reply message from the access point in response to the message. The reply message includes the second connection identifier as the identifier for the signalling connection associated with the UE between the network controller and the core network. The method also replaces, at the network controller, the second connection identifier in the reply message with the first connection identifier as the identifier for the signalling connection associated with the UE between the network controller and the core network. The method sends the reply message from the network controller to the core network. In some embodiments, the first and second identifiers indicate the communication system node (e.g., CN, RNC, HNB-GW) that has assigned the value to the identifier. In some embodiments, the first and second identifiers indicate the communication system node (e.g., CN, RNC, HNB-GW) that has assigned the identifier. In some embodiments, the first and second identifiers indicate the communication system node (e.g., CN, RNC, HNB-GW) that has assigned the signalling connection.

[0046] Some embodiments provide a computer readable medium of the network controller that operates in a communication system comprising (i) a first wireless communications system comprising a licensed wireless radio access network and a core network and (ii) a second wireless communications system comprising a plurality of short range access points for establishing service regions of the second wireless communications system using licensed wireless frequencies and the network controller for communicatively coupling a user equipment (UE) operating in the service regions to the core network. The computer readable medium stores a computer program for execution by at least one processing unit. The computer program includes a set of instruction for receiving a message from the core network. The message includes a first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for allocating a second connection identifier to identify a connection

associated with the UE between the network controller and an access point of the second wireless communication system communicatively connected to the network controller. The second connection identifier is different than the first connection identifier. The computer program also includes a set of instructions for sending the message and the second connection identifier to the access point. The computer program also includes a set of instructions for receiving a reply message from the access point in response to the message. The reply message includes the second connection identifier as the identifier for the connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for replacing the second connection identifier in the reply message with the first connection identifier as the identifier for the connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for sending the reply message to the core network.

[0047] Some embodiments provide a method of handling a handover of an ongoing session of a user equipment (UE) in a communication system. The method receives a message at an access point of the plurality of access points from the network controller. The message includes (i) a first connection identifier as an identifier for a first connection associated with the UE between the network controller and a first node of the communication system and (ii) a second connection identifier allocated by the network controller. The second connection identifier is to identify a second connection associated with the UE between the network controller and the access point. The second connection identifier is different than the first connection identifier. The method also determines whether the first connection identifier identifies the first connection as a connection between the network controller and the core network. When the first connection identifier identifies the first connection as a connection between the network controller and the core network, the method sends a reply message from the access point to the network controller. The reply message includes the first connection identifier as the identifier for the connection associated with the UE between the network controller and the core network. When the first connection identifier identifies the first connection as a connection between the network controller and a node of the communication system other than the core network, the method sends a reply message from the access point to the network controller. The reply message includes the second connection identifier as the identifier for the

connection associated with the UE between the network controller and the node of the communication system.

[0048] Some embodiments provide a computer readable medium of an access point of a group of short range access points that operate in a communication system comprising (i) a first wireless communications system comprising a licensed wireless radio access network and a core network and (ii) a second wireless communications system comprising the plurality of short range access points for establishing service regions of the second wireless communications system using licensed wireless frequencies and a network controller for communicatively coupling a user equipment (UE) operating in the service regions to the core network. The computer readable medium stores a computer program for execution by at least one processing unit. The computer program includes a set of instructions for receiving a message from the network controller. The message includes (i) a first connection identifier as an identifier for a first connection associated with the UE between the network controller and a first node of the communication system and (ii) a second connection identifier allocated by the network controller. The second connection identifier is to identify a second connection associated with the UE between the network controller and the access point. The second connection identifier is different than the first connection identifier. The computer program also includes a set of instructions for determining whether the first connection identifier identifies the first connection as a connection between the network controller and the core network. The computer program also includes a set of instructions for, when the first connection identifier identifies the first connection as a connection between the network controller and the core network, sending a reply message to the network controller. The reply message includes the first connection identifier as the identifier for the connection associated with the UE between the network controller and the core network. The computer program also includes a set of instructions for, when the first connection identifier identifies the first connection as a connection between the network controller and a node of the communication system other than the core network, sending a reply message to the network controller. The reply message includes the second connection identifier as the identifier for the connection associated with the UE between the network controller and the node of the communication system.

[0049] Several more detailed embodiments of the invention are described in sections below. Specifically, Section I discusses the HNB system architecture. Section II describes various protocol architectures of the HNB system, including protocol architectures for the Home Node-B Application Part (HNBAP) and the Radio Access Network Application Part (RANAP) User Adaption (RUA) layer. Section III discusses mobility management within the HNB system, including mobility management scenarios and relocation.

[0050] Section IV provides a description of a computer system with which some embodiments of the invention are implemented. Lastly, Section V lists the abbreviations and provides definitions for terms found herein.

I. HNB SYSTEM ARCHITECTURE

[0051] **Figure 1** illustrates a system architecture for 3G HNB deployments in accordance with some embodiments of the invention. As shown, the system includes a HNB access network (HNB-AN or HNB system) 110. The key features of the 3G HNB system architecture include (a) support for a standard User Equipment (UE) 105 as defined in the 3GPP technical specification TS 23.101 entitled "General UMTS architecture" which is incorporated herein by reference and (b) co-existence with the UMTS Terrestrial Radio Access Network (UTRAN) and interconnection with the existing Core Network (CN) 115 via the standardized interfaces defined for UTRAN.

[0052] In some embodiments, the standardized interfaces include (a) the Iu-cs interface for circuit switched services as overviewed in the 3GPP technical specification (TS) 25.410 entitled "UTRAN Iu Interface: general aspects and principles" which is incorporated herein by reference, (b) the Iu-ps interface for packet switched services as overviewed in the 3GPP TS 25.410, (c) the Iu-pc interface for supporting location services as described in the 3GPP TS 25.450 entitled "UTRAN Iupc interface general aspects and principles" which is incorporated herein by reference, and (d) the Iu-bc interface for supporting cell broadcast services as described in the 3GPP TS 25.419 entitled "UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)" which is incorporated herein by reference. However, it should be apparent to one of ordinary skill in the art that other interfaces may be implemented by the HNB-AN. For instance, the A/Gb interfaces of standard Global System for Mobile (GSM) communications systems can be implemented by a HNB-AN to support 2G or GSM/GPRS air interface.

[0053] To address specific 3G HNB applications, some embodiments utilize existing Iu and Uu interfaces within the HNB-AN 110. The HNB-AN 110 addresses some of the key issues in the deployment of 3G HNB applications, such as the ad-hoc and large scale deployment of 3G HNBs using public infrastructure such as the Internet.

[0054] **Figure 2** illustrates elements of the HNB Access Network (HNB-AN) 200 architecture in accordance with some embodiments. This figure includes (3G) HNB 205, Generic IP Access Network 210, HNB-GW 215, HNB Management System 220, Iuh interface 225 that is established between the Generic IP Access Network 210 and the HNB-GW 215, and an interface 230 between the HNB-GW 215 and the HNB Management System 220. In some embodiments, the interface 230 is based on the 3GPP TR-069 family of standards. In some other embodiments, the interface 230 is the Iuhm interface. These elements are described in further detail below with reference to **Figure 3**.

[0055] **Figure 2** and other figures below illustrate a single access point (e.g., HNB 205) communicatively coupled to a network controller (e.g., HNB-GW 215). However, it should be apparent to one of ordinary skill in the art that the network controller (e.g., HNB-GW 215) of some embodiments is communicatively coupled to several HNBs and the network controller communicatively couples all such HNBs to the core network. Also, the HNB of some embodiments is communicatively coupled to several UEs. The figures merely illustrate a single HNB communicatively coupled to the HNB-GW for purposes of simplifying the discussion to interactions between a single access point and a single network controller. However, the same network controller may have several of the same interactions with several different access points.

[0056] **Figure 3** illustrates the HNB-AN system architecture of some embodiments integrated with a core network of a second communication system that includes a licensed wireless radio access network. The HNB system includes (1) Home Node-B (HNB) 305, (2) Home Node-B Gateway (HNB-GW) 315, (3) Broadband IP Network 320, (4) Security Gateway (SeGW) 325, and (6) HNB Management System 330. The licensed wireless radio access network of the second communication system includes UTRAN 385 which is comprised of a Node-B 380 and a Radio Network Controller 375 of a UMTS. The core network of the second communication system includes Mobile Switching Center (MSC) 365, Serving GPRS Support Node (SGSN) 370, Authorization, Authentication, and Accounting server 355, and Home

Location Register 360. Additionally, Service Mobile Location Center (SMLC) 340 and Cell Broadcast Center (CBC) 345 may be components of the core network.

A. User Equipment (UE)

[0057] In some embodiments, UE 310 is used to access services of the HNB-AN and also access services of the licensed wireless radio access network 385 of a cellular provider. In some such embodiments, the UE seamlessly transitions from the HNB-AN to the cellular provider and vice versa without loss of connectivity. In some embodiments, the UE 310 is thus a standard device operating over licensed spectrum of a licensed wireless system provider. Accordingly, the UE 310 wirelessly connects to the HNB 305 using the same signalling and messaging interfaces as it would when connecting to a base station, such as a base transceiver station (BTS) in GSM, or the Node-B 380 of a Universal Mobile Telecommunications System (UMTS).

[0058] **Figure 4** illustrates some of the various devices that may be used in some embodiments in order to access services of the HNB-AN or HNB system. In some embodiments, the devices include (1) standard licensed wireless handsets 405 and wireless enabled computers 410 that connect through HNBs 415, (2) dual mode handsets with WiMAX capabilities 420 that connect through WiMAX access points 425, (3) devices such as wired telephones 430 and faxes 435 that connect through terminal adapters 440, and (4) softmobile enabled devices 445.

1. Licensed Wireless Handsets

[0059] In some embodiments, the UE 310 includes cellular telephones 405, smartphones, PDAs, and modem like devices some of which are shown in **Figure 4**. These devices include any device that wirelessly communicates with a licensed wireless service provider using existing licensed wireless technologies, such as Global System for Mobile (GSM) communications, UMTS, etc.

2. Terminal Adaptors

[0060] In some embodiments, the UE 310 includes a terminal adaptor device (such as 440 of **Figure 4**) that allows incorporating fixed-terminal devices such as telephones, faxes, and other equipments that are not wirelessly enabled within the HNB-AN. As far as the subscriber is concerned, the service behaves as a standard analog fixed telephone line. The service is delivered

in a manner similar to other fixed line VoIP services, where a UE is connected to the subscriber's existing broadband (e.g., Internet) service.

3. WiMAX

[0061] In some embodiments, the UE 310 includes a dual mode cellular/WiMAX UE (such as 420 of **Figure 4**) that enables a subscriber to seamlessly transition between a cellular network and a WiMAX network through a WiMAX access point (such as 425 of **Figure 4**).

4. SoftMobiles

[0062] Connecting laptops to broadband access at hotels and Wi-Fi hot spots has become popular, particularly for international business travelers. In addition, many travelers are beginning to utilize their laptops and broadband connections for the purpose of voice communications. Rather than using mobile phones to make calls and pay significant roaming fees, they utilize SoftMobiles (or SoftPhones) such as 445 of **Figure 4** and VoIP services when making long distance calls. Accordingly, the UE 310 of some embodiments includes SoftMobile like devices.

[0063] To use a SoftMobile service, a subscriber would place a USB memory stick with an embedded SIM into a USB port of their laptop. A SoftMobile client would automatically launch and connect over IP to the mobile service provider. From that point on, the subscriber would be able to make and receive mobile calls as if she was in her home calling area.

B. HNB

[0064] The Home Node-B (HNB) 305 is an access point that offers a standard radio interface (Uu) for user equipment (UE) connectivity using short range licensed wireless frequencies. The HNB 305 provides the radio access network connectivity to the UE using the Iuh interface towards the HNB-GW 315.

[0065] The HNB 305 differs from the UMTS Node-B in that the range of wireless connectivity supported by the HNB 305 (e.g., tens of meters) is much less than the range supported by the UMTS Node-B (e.g., hundreds or thousands of meters). This is because the HNB 305 is a low power and a short range device similar to wireless access points found within a user's home. The low power and short range requirement ensures that the HNB 305 does not interfere with the service regions of the licensed wireless system providers (e.g., cellular

networks) that are established using the wireless frequencies that the licensed wireless system providers licensed from the government at great expense. Moreover, the low power requirement enables the HNB 305 to operate using standard electrical outlets of a user's home or office. In some embodiments, the low power and short range requirement further facilitates the small scale of the HNB device relative to the radio access network Node-B devices. Unlike the Node-B, which is housed in one or more racks and cabinets and the antennas for its radios are mounted on a tower reaching several meters in height, the HNB is a much smaller device often the size of 802.11 wireless routers commonly found within a user's home.

[0066] Conversely, the Node-B is network equipment of a UMTS Terrestrial Radio Access Network (UTRAN). The Node-B is managed and operated by a licensed wireless system provider. The Node-B of the licensed wireless system has to provide service to many more users than the HNB 305 and must do so without loss of connectivity over vast regions (e.g., states and countries). Accordingly, the licensed wireless service provider deploys several Node-Bs that are adjacent to one another in order to create an uninterrupted region of coverage. Conversely, an HNB service region established by a first HNB does not need to be adjacent to any other HNB service region and need not offer uninterrupted service between HNB service regions.

[0067] In some embodiments, the HNB 305 is user hosted as opposed to the Node-B that is hosted by the licensed wireless system. A user hosted HNB allows a user to specify the location of the HNB, provide the connectivity between HNB and the HNB network or HNB-GW (e.g., the broadband connection), control operation of the HNB, for example, by providing power to the HNB. All such control over the Node-B is tightly managed by the licensed wireless system provider. In other words, the HNB is customer premise equipment (CPE) that a user is able to purchase from an electronics store or from the HNB-AN provider, whereas the Node-B is network equipment that is impractical for a single user to purchase, operate, and maintain.

[0068] Additionally, a key characteristic of the HNB architecture of some embodiments is that there are no permanent pre-configured peer adjacencies between HNB and HNB-GW. Instead, there are ad-hoc adjacencies that are initiated from the HNB (as it is usually behind a NAT/firewall, and does not have a permanent IP address in the carrier network). The HNB system therefore offers flexibility in deploying service. The HNBs of an HNB system may be

deployed on an ad hoc basis as opposed to the regimented deployment structure of the licensed wireless system.

[0069] Accordingly, in some embodiments, the HNB 305 supports enhancements for operating in an ad-hoc environment and the Node-B does not. The ad hoc system allows for individual users to establish HNB service regions based on each user's needs. In some embodiments, each user purchases an HNB and each of the HNBs may be purchased from different vendors with different HNB implementations. In this manner, the ad hoc HNB system creates several individual local coverage areas based on user deployment of each HNB whereas the licensed wireless system deploys its Node-Bs in an effort to provide regional coverage area that is uninterrupted across large areas (e.g., hundreds of miles).

[0070] It should be apparent to one of ordinary skill in the art that in some embodiments the HNB system provider deploys the HNBs rather than the users. In some such embodiments, the system remains ad hoc by virtue of the discontinuous nature of the separate and local HNB service regions. Additionally, in some such embodiments, the HNBs remain user hosted since power and broadband connectivity is provided by the user even though the system provider more closely regulates the HNB equipment that is deployed.

[0071] The ad hoc nature of the HNB system also allows the system to grow and shrink as its user base grows and shrinks. For example, whenever a new user desires to utilize the HNB service, the user purchases and hosts a HNB at a home or office location. The user hosted HNB provides the user with a HNB-AN service region from which the user access HNB system services. Conversely, the licensed wireless system provider must first deploy several Node-Bs in order to provide extensive large scale regional coverage. Once the service regions are established at great expense to the licensed wireless system provider, users then activate service with the licensed wireless system provider. Accordingly, the HNB system is an unplanned system whereas the licensed wireless system is a planned system. In other words, the HNB system does not need an existing access point infrastructure in order to operate. Rather, the infrastructure is unplanned whereby the infrastructure is built upon with every new user that is added to the system. This is opposite to the planned licensed wireless system. The licensed wireless system requires that there be an existing infrastructure before new users can be added. The infrastructure

of the licensed wireless system is planned in the sense that the infrastructure is built first in a particular region and then the service is marketed to that region after the infrastructure is built.

[0072] The HNB 305 also differs from generic access points used in UMA systems. Specifically, in a UMA system the access points act as transparent base stations. In other words, the user equipment and the network controller directly communicate. In the HNB system, however, the HNB 305 includes various Radio Network Controller (RNC) functionality. In some such embodiments, the HNB 305 initiates various messaging procedures and maintains state information regarding user equipment operating within the service region associated with the HNB 305. The HNB 305 is equipped with either a standard 3G Universal Subscriber Identity Module (USIM) or a 2G SIM. The (U)SIM provides the HNB 305 with a unique subscriber identity and allows the HNB 305 to utilize the existing subscriber management infrastructure of an operator. It should be apparent to one of ordinary skill in the art that some embodiments of the HNB system utilize a different identification mechanism for the HNB than the (U)SIM. For example, the HNB identity of some embodiments is based on Media Access Control (MAC) address of the HNB or any other globally unique identifier such as the combination of vendor identity and serial number from that vendor.

[0073] The access points of some embodiments include circuits for receiving, transmitting, generating, and processing the various messages that cause various physical transformations within the HNB-AN, core network, and licensed wireless radio access network. In some embodiments, the circuits of the access points include processing units (e.g., one or more processors), memory, receiver, and transceiver. In some embodiments, the receiver and/or the transceiver are wireless interfaces that operate using short range licensed wireless frequencies. In some other embodiments, the receiver and/or the transceiver are wired interfaces (e.g., DSL, cable, etc.). These circuits perform various physical transformations on the access point as well as other elements within the HNB-AN, licensed wireless radio access network, and core network. For example, the processor in conjunction with the memory generate a paging message that when sent to a UE using the transceiver causes the UE to prompt the user of an incoming call. As another example, the access point registers a UE by generating a registration message that is sent to the network controller using the transceiver when the access point detects that the UE has camped on the service region of the access point based on a location update

message received by the access point on its receiver. These and other physical components of the access points of some embodiments are described with further detail in **Figure 19** below.

[0074] It should be apparent to one of ordinary skill in the art that the HNB is one implementation of an access point that operates using short range licensed wireless frequencies. Some embodiments allow for any access point that operates using short range licensed wireless frequencies to be used in place of or in conjunction with the HNBs. For example, a Femtocell access point is a different implementation of an access point that provides short range licensed wireless frequencies in order to establish a service region of a Femtocell system that is similar to the HNB system described in relation to some embodiments of the invention.

C. Broadband IP Network

[0075] The HNB 305 provides radio access network connectivity for the UE 310. The HNB 305 then communicatively couples the UE to the HNB-GW 315 using the Iuh interface that exists between the HNB 305 and the HNB-GW 315. As shown in **Figure 3**, the Iuh interface is established over a broadband Internet Protocol (IP) network 320 where, in some embodiments, a customer's broadband connection is utilized. The broadband IP Network 320 represents all the elements that collectively, support IP connectivity between the HNB-GW 315 and the HNB 305. The IP network 320 is assumed to be an untrusted public IP network without any Asynchronous Transfer Mode (ATM) or Signaling System 7 (SS7) infrastructure.

[0076] In some embodiments, the broadband IP network 320 includes (1) other Customer premise equipment (e.g., Digital Subscriber Line (DSL)/cable modem, Wireless Local Area Network (WLAN) switch, residential gateways/routers, switches, hubs, WLAN access points), (2) network systems specific to the broadband access technology (e.g., DSL Access Multiplexer (DSLAM) or Cable Modem Termination System (CMTS)), (3) Internet Service Provider (ISP) IP network systems (edge routers, core routers, firewalls), (4) wireless service provider (WSP) IP network systems (edge routers, core routers, firewalls) and Network address translation (NAT) functions, either standalone or integrated into one or more of the above systems.

D. HNB-GW

[0077] The HNB-GW 315 is a network controller that provides network connectivity of the HNB 305 to the existing core network (CN) 335. The HNB-GW 315 entity appears as a

legacy RNC to the existing CN 335. Specifically, the HNB-GW 315 uses existing Iu interfaces (e.g., Iu-cs and Iu-ps) for CN connectivity. In this manner, the HNB system may be integrated into the existing CN 335 with no change to the CN 335. This allows the licensed wireless system providers the ability to provide HNB system functionality to their users with no change to their existing network.

[0078] As noted above, the HNB-GW 315 connects to the HNB 305 using the Iuh interface. Additional interfaces of the HNB-GW 315 include the Iu-pc interface to the Service Mobile Location Center (SMLC) 340, the Iu-bc interface to the Cell Broadcast Center (CBC) 345, the Wm interface to the Authorization, Authentication, and Accounting (AAA) server 355, and an interface that is based on the 3GPP TR-069 family of standards, as specified by the DSL Forum technical specifications, to the HNB management system 330. In some embodiments, the interface to the HNB management system 330 is the Iuhm interface. In some such embodiments, the Iuhm interface carries information related to customer premise equipment (CPE) device management functionality between the HNB and HNB Mgmt System. It should be apparent to one of ordinary skill in the art that other interfaces may be used instead of or in addition to the above enumerated interfaces.

[0079] In some embodiments, the HNB-GW 315 connects to several different HNBs and services each of the corresponding service regions of each of the several HNBs. In this manner, a single HNB-GW, such as the HNB-GW 315, communicatively couples multiple HNB service regions to the CN 335. Accordingly, the HNB-GW 315 provides call management functionality, mobility management functionality, security functionality, etc. as will be described in greater detail below. The HNB-GW 315 also performs key functionalities, such as the management of the legacy UTRAN identifiers (Location Area Identifiers (LAI), Service Area Identifiers (SAI), RND-Id, etc.) towards the CN 335, and Iuh interface management.

[0080] In some embodiments, the HNB-GW 315 includes various software module sub-components and/or various hardware module sub-components that perform some of the above mentioned functionality. For example, the Security Gateway (SeGW) 325 is a logical entity within the HNB-GW 315. The SeGW 325 provides the security functions including termination of secure access tunnels from the HNB 305, mutual authentication, encryption and data integrity

for signaling, voice and data traffic. In other embodiments, SeGW is an standalone entity and is not an entity within the HNB-GW.

[0081] The HNB Management System 330 provides centralized Customer Premise Equipment (CPE) device management for the HNB 305 and communicates with the HNB 305 via the security gateway logical entity. This system is used to manage a large number of HNBs including configuration, failure management, diagnostics, monitoring and software upgrades. In some embodiments, the HNB Management System 330 utilizes existing CPE device management techniques such as those described in the DSL Forum technical specifications TR-069.

[0082] The network controller of some embodiments includes circuits for receiving, transmitting, generating, and processing the various messages that cause various physical transformations within the HNB-AN, core network, and licensed wireless radio access network. In some embodiments, the circuits of the network controller include a processor, memory, receiver, and transceiver. These circuits perform various physical transformations on the network controller as well as other elements within the HNB-AN, licensed wireless radio access network, and core network. For example, the processor in conjunction with the memory generate context identifiers that when sent to a UE using the transceiver provide the UE with a unique identifier when operating within the HNB-AN. These and other physical components of the network controller of some embodiments are described with further detail in **Figure 19** below.

E. Core Network (CN) and Other Network Elements

[0083] As mentioned above, the HNB-GW 315 provides network connectivity of the HNB 305 to the existing CN 335. The CN 335 includes one or more HLRs 360 and AAA servers 355 for subscriber authentication and authorization. Once authorized, the UE may access the voice and data services of the CN 335 through the HNB system. To provide such services, the CN 335 includes a Mobile Switching Center (MSC) 365 to provide circuit switched services (i.e., voice). The CN also includes a Serving GPRS Support Node (SGSN) 370 to provide packet switched services. Though not shown in **Figure 3**, the SGSN operates in a conjunction with a Gateway GPRS Support Node (GGSN) in order to provide the packet switched services.

[0084] The SGSN 370 is typically responsible for delivering data packets from and to the GGSN and the UE within the geographical service area of the SGSN 370. Additionally, the SGSN 370 may perform functionality such as mobility management, storing user profiles, and storing location information. However, the actual interface from the CN 335 to various external data packet services networks (e.g., public Internet) is facilitated by the GGSN. As the data packets originating from the UE typically are not structured in the format with which to access the external data networks, it is the role of the GGSN to act as the gateway into such packet services networks. In this manner, the GGSN provides addressing for data packets passing to and from the UE and the external packet services networks (not shown). Moreover, as the user equipment of a licensed wireless network traverses multiple service regions and thus multiple SGSNs, it is the role of the GGSN to provide a static gateway into the external data networks.

[0085] Location services are provided by the SMLC 340. The CBC 345 provides support for cell broadcast services.

[0086] These and other elements of the CN 335 are primarily intended for use with the licensed wireless systems. In the description below, the licensed wireless system will be described with reference to the UTRAN of a UMTS. However, it should be apparent to one of ordinary skill in the art that any licensed wireless system, such as a GSM/EDGE Radio Access Network (GERAN) may be used to reference the licensed wireless system.

[0087] Elements common to a UTRAN based cellular network include multiple base stations referred to as Node-Bs that facilitate wireless communication services for various UE via respective licensed radio links (e.g., radio links employing radio frequencies within a licensed bandwidth). The licensed wireless channel may comprise any licensed wireless service having a defined UTRAN or GERAN interface protocol (e.g., Iu-cs and Iu-ps interfaces for UTRAN or A and Gb interfaces for GERAN) for a voice/data network. The UTRAN 385 typically includes at least one Node-B 380 and a Radio Network Controller (RNC) 375 for managing the set of Node-Bs. Typically, the multiple Node-Bs are configured in a cellular configuration (one per each cell) that covers a wide service area. A licensed wireless cell is sometimes referred to as a macro cell which is a logical term used to reference, e.g., the UMTS radio cell (i.e., 3G cell) under Node-B/RNC which is used to provide coverage typically in the

range of tens of kilometers. Also, the UTRAN or GERAN is sometimes referred to as a macro network.

[0088] Each RNC communicates with components of the core network through the above described standard radio network controller interface such as the Iu-cs and Iu-ps interfaces. For example, a RNC communicates with MSC via the UTRAN Iu-cs interface for circuit switched services. Additionally, the RNC communicates with SGSN via the UTRAN Iu-ps interface for packet switched services through GGSN. It is through the use of these standardized network interfaces that the HNB system, more particularly the HNB-GW, may be seamlessly integrated to leverage services of the CN and emulate functionality of a legacy RNC of the licensed wireless system.

II. PROTOCOL ARCHITECTURES OF THE HNB SYSTEM

[0089] Functionality provided by each of the HNB and the HNB-GW are defined within various protocol stacks. In some embodiments, the protocol stacks include software layers that are stored to the memory of the HNB and HNB-GW and that are executed by a processing unit of the HNB and HNB-GW. In some embodiments, the protocol stacks are implemented as hardware modules within the HNB and HNB-GW. Additional hardware components of the HNB and HNB-GW are described below in Section IV, "Computer System".

[0090] In some embodiments, the HNB system separates management functions from control plane functions into two separate protocol stacks. The HNB Application Part (HNBAP) protocol architecture implements the management functions for the HNB system and the RANAP User Adaptation (RUA) protocol architecture implements the control functions for the HNB system. As will be described below, additional protocol architectures are specified for providing other functionality such as user plane functionality. However, it should be apparent to one of ordinary skill in the art that other protocol architectures may be integrated into the components of the HNB system and that the functionality of each of the protocol architectures is scalable to provide more or less functionality than described below.

A. Protocol Architecture over the Iuh Interface

1. HNB Application Part (HNBAP) Protocol Architecture

[0091] As noted above, the HNBAP protocol architecture supports management functions between the HNB and HNB-GW including, but not limited to, the management of the underlying transport (i.e., the SCTP connection), HNB and UE registration procedures. **Figure 5** illustrates the HNBAP protocol architecture in accordance with some embodiments. This figure illustrates (1) HNB 505, (2) HNB-GW 515, and (3) HNBAP protocol stacks of each of the HNB 505 and the HNB-GW 515. The HNBAP protocol stacks include (1) access layers 510, (2) transport IP layer 520, (3) IP Security (IPSec) ESP layer 525, (4) remote IP layer 540, (5) Stream Control Transmission Protocol layer (SCTP) 530, and (6) a HNBAP protocol layer 545.

[0092] The underlying Access Layers 510 and "Transport IP" layer 520 (i.e., the "outer" IP layer associated with IPSec tunnel mode) provide the generic connectivity between the HNB 505 and the HNB-GW 515. The IPSec layer 525 operates in tunnel mode and provides encryption and data integrity for communications and data that are passed using the upper layers (530, 540, and 545).

[0093] SCTP 530 provides reliable transport between the HNB 505 and the HNB-GW 515. SCTP 530 is transported using the "Remote IP" layer 540 (i.e., the "inner" IP layer associated with IPSec tunnel mode). In some embodiments, the SCTP 530 establishes a single SCTP association between the HNB 505 and HNB-GW 515. The same SCTP association is used for the transport of both the HNBAP messages as well as the RANAP messages (using RUA protocol), described in further detail below, over the Iuh interface 535. The SCTP Payload Protocol Identifier (PPI) value is used to identify the protocol being transported in the SCTP data chunk (e.g., HNBAP or RUA). The PPI value used for HNBAP transport is coordinated between the HNB 505 and the HNB-GW 515 (e.g., the HNBAP PPI value should be registered with the Internet Assigned Numbers Authority (IANA)). Each SCTP association contains a number of "streams" which are used to support multiple flows across the Iuh interface. In some embodiments, a dedicated SCTP stream (i.e., stream id 0 of the underlying SCTP transport association) is used for the transport of HNBAP messages across the Iuh interface.

[0094] It should be apparent to one of ordinary skill in the art that other reliable transport protocol layers may be used instead of SCTP 530 to facilitate reliable transport of communications and data between the HNB 505 and the HNB-GW 515. For example, some embodiments use the Transmission Control Protocol (TCP) for reliably transporting messages between the HNB 505 and the HNB-GW 515.

[0095] In some embodiments, the HNBAP protocol 545 provides a resource management layer, registration of the HNB and UE with the HNB-GW, registration updates with the HNB-GW, and support for the identification of the HNB being used for HNB access. It should be apparent to one of ordinary skill in the art that the HNBAP protocol layer of some embodiments implements additional resource management functionality and that the above enumerated list is an exemplary set of such functionality.

2. HNB Control Plane Architecture (RUA)

[0096] After performing the management functions defined by the HNBAP protocol, the HNB and HNB-GW utilize a different protocol architecture that specifies the control plane in the HNB system. **Figure 6** illustrates the protocol architecture in support of the HNB control plane (i.e., for both the CS and PS domain) in accordance with some embodiments.

[0097] **Figure 6** includes (1) HNB 605, (2) HNB-GW 615, (3) CN 640, (4) UE 650, and (5) control plane protocol stacks of each of the HNB 605, the HNB-GW 615, the CN 640, and the UE 650. The control plane protocol stacks of the HNB 605 and the HNB-GW 615 include (1) access layers 610, (2) transport IP layer 620, (3) IPSec layer 625, (4) remote IP layer 640, (5) SCTP 630, (6) RANAP user adaptation (RUA) layer 635, and (7) interworking functionality (IWF) 645. The control plane protocol stack of the CN 640 includes signaling transport layers defined according to the 3GPP technical specification TS 25.412, "UTRAN Iu Interface Signaling Transport", herein incorporated by reference, a RANAP layer, and a Non Access Stratum (NAS) layer 665 that performs various call management, mobility management, General Packet Radio Service (GPRS) mobility management and session management, and short message services (SMS). The control plane protocol stack of the UE 650 includes a layer 1 signaling transport layer, a Media Access Control (MAC) layer, a Radio Link Control (RLC) layer, a Radio Resource Control (RRC) layer, and the NAS layer 665.

[0098] As described above, the underlying Access Layers 610 and "Transport IP" layer 620 provide the generic connectivity between the HNB 605 and the HNB-GW 615. The IPSec layer 625 provides encryption and data integrity for communications and data that are passed using the upper layers. SCTP 630 provides reliable transport for the RANAP User Adaptation (RUA) layer 635 between the HNB 605 and the HNB-GW 615.

[0099] The RANAP protocol is used for CS/PS signaling between the HNB 605 and the CN 640. RANAP, as is well known in the art, is an established protocol used for UMTS signaling between the CN and the UTRAN of a licensed wireless radio access network. Accordingly, the use of RANAP messages within the control plane of the HNB system, allows for the HNB system to support many of the UTRAN functions in the HNB system. These functions include: Radio Access Bearer (RAB) management, Radio Resource Management (RRM), Iu link management, Iu U-plane (RNL) management, mobility management, security, service and network access, and Iu coordination.

[00100] The HNB-GW 615 relays the RANAP messages between the HNB 605 and the CN 640. In some embodiments, the HNB-GW 615 terminates and re-originates some RANAP messages. For example, the HNB-GW 615 terminates and re-originates connection-less RANAP messages.

[00101] To perform the transparent transfer of RANAP messages, the HNB control plane protocol stacks of the HNB 605 and the HNB-GW 615 include the RUA layer 635. The RUA layer 635 provides a lightweight mechanism to transport RANAP messages 660 and control functions between the HNB 605 and the HNB-GW 615. Specifically, the RUA layer 635 encapsulates the RANAP messages 660 in an RUA layer header for transport between the HNB 605 and the HNB-GW 615. Therefore, through the use of the RUA 635 layer, no changes are made to the RANAP message definitions. Rather, all necessary changes are contained in the RUA header.

[00102] It should be apparent to one of ordinary skill in the art to reference the RUA layer with other terminologies such as RANAP Adaptation Layer (RAL) or RANAP Transport Adaptation (RTA), etc. However, the key function of this adaptation layer is to provide the functionality, over the Iuh interface, of transferring RANAP messages as defined in the 3GPP technical specification TS 25.413 entitled "UTRAN Iu interface Radio Access Network

Application Part (RANAP) signaling" which is incorporated herein by reference, and will be referred to as TS 25.413.

[00103] Through the RUA header and the encapsulation of the RANAP message, the RUA adaptation layer of some embodiments enables: (1) transport of RANAP messages using SCTP over the Iuh interface between the HNB and HNB-GW, (2) support for associating and identifying UE specific logical connections (i.e., identifying the RANAP messages belonging to a specific UE via the concept of UE context identifiers), (3) support for routing the establishment of a signalling connection to a CN node within a CN domain (i.e., support for Iu-flex at the HNB-GW), (4) support for indicating the cause for establishing the UE specific logical connection (e.g., for emergency session establishment, etc.), (5) providing a mechanism to transparently relay the RANAP messages from the HNB to CN without the need to decode the encapsulated RANAP message, and (6) support for the indication of service domain (CS or PS) for the RANAP messaging.

[00104] The RUA layer 635 minimizes the decoding and processing of RANAP messages 660 at the HNB-GW 615. Specifically, the HNB-GW 615, in many instances, no longer must decode and process the RANAP message 660. Instead, the HNB-GW 615 processes information within the RUA header information in order to determine a destination within the core network to receive a RANAP message 660 sent from a UE operating from a HNB service region communicatively coupled by the HNB-GW 615. The RUA layer 635 also eliminates the need for the HNB-GW 615 to process and decode the NAS layer 665.

[00105] In some embodiments, the RUA layer 635 does not duplicate existing RANAP procedures. Accordingly, RUA procedures are minimized. As will be described in further detail below, the HNB control plane protocol architecture of some embodiments simplifies context-ID allocation and associated functional overhead.

[00106] The RUA 635 utilizes the same underlying transport (i.e., SCTP connection) as HNBAP. It should be apparent to one of ordinary skill in the art that it is also possible to use TCP as a reliable transport layer instead of SCTP. The SCTP PPI value used for RUA transport is coordinated between the HNB 605 and the HNB-GW 615 (e.g., the RUA PPI value should be registered with IANA).

[00107] In some embodiments, a dedicated SCTP stream (e.g., stream id 0 of the underlying SCTP transport association) is used for the transport of connectionless RANAP messages 660 between the HNB 605 and the HNB-GW 615. For the connection oriented messages, the number of SCTP streams to be established at SCTP connection setup and the mapping of UE transactions to the specific SCTP streams is an implementation choice. The use of UE Context-Id allows multiple UE transactions to be multiplexed over the same SCTP stream.

[00108] The Inter-working Functionality (IWF) 645 in the HNB-GW 615 switches the RANAP messages 660 between the Iuh interface and the corresponding domain specific (CS/PS) Iu interface. It should be noted that the IWF 645 is a logical entity in the RUA protocol stack. As mentioned above, some RANAP messages 660 are terminated and re-originated in the HNB-GW 615 (e.g., connection-less RANAP messages) and some are modified in the HNB-GW 615 to adapt to the underlying transport towards the CN 640 (e.g., when using ATM interfaces towards the CN 640). Additionally, NAS protocol messages 655 (e.g., CC/MM/SMS, etc) are carried transparently between the UE 650 and the CN 640.

[00109] In some embodiments, the relay of RANAP messages 660 between the HNB 605 and the CN by the HNB-GW 615 is achieved using a direct transfer mechanism over the Iuh interface. This direct transfer mechanism involves encapsulation of the RANAP messages 660 in a DIRECT TRANSFER message exchanged between the HNB 605 and HNB-GW 615 over the Iuh interface. In some embodiments, this message is referred to as a RUA DIRECT TRANSFER message. In some embodiments, this message is referred to as a HNBAP DIRECT TRANSFER message. In some embodiments, the direct transfer mechanism is used to relay messages from CBC (Iu-bc) (not shown) and SMLC (Iu-pc) (not shown) to HNB 605 and vice-versa via the HNB-GW 615.

[00110] The architecture of **Figure 6** also supports transfer of the RANAP "Initial UE Message" and support for Iu-flex. Iu-flex functionality is defined in 3GPP TS 23.236, "Intra-Domain Connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes", hereinafter, TS 23.236, with additional functionality such as messaging, etc., described in TS 25.331. Specifically, Iu-flex covers details for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes for GSM and UMTS systems. The first RANAP message (i.e., the RANAP "Initial UE Message") is carried from the HNB 605 in the INITIAL DIRECT

TRANSFER message over the Iuh interface. The INITIAL DIRECT TRANSFER message also carries information used to route the establishment of a signalling connection from HNB-GW 615 to a CN node within a CN domain (i.e. support for Iu-flex).

[00111] Many of the common or connection-less RANAP messages are terminated and processed in the HNB-GW 615. When there is a need to relay specific connectionless message (e.g. Paging), then the DIRECT TRANSFER message is used to relay the specific connection-less message.

[00112] In some embodiments, the direct transfer mechanism for relaying RANAP messages provides a single protocol over the Iuh interface (i.e., clean architecture) whereby a single interface between HNB and HNB-GW functional entity is used. The direct transfer mechanism of some embodiments eliminates changes to the RANAP specifications for use over the Iuh interface. If RANAP were to be used directly over the Iuh interface, then all the specifications which reference RANAP would need to be updated to describe the applicability of existing RANAP messages between the two new nodes (e.g., HNB and the HNB-GW). In some embodiments, the direct transfer mechanism eliminates the need for "RNC-ID" and "Iu signalling connection identifier" attributes on a per HNB basis, carried in the RANAP messages. The "RNC-ID" and "Iu-signalling connection identifier" carried in the downlink RANAP messages are processed by the HNB-GW and can be ignored by the HNB. Similarly, in the uplink RANAP messages, the usage of the RNC-ID and Iu signalling connection identifier attributes can be implementation specific with no impact on the Iuh interface. Additionally, by carrying the RANAP messages in a container, the overhead (management and runtime) of the underlying transport layers of RANAP such as SCCP/M3UA are eliminated as well.

III. MOBILITY MANAGEMENT

A. Mobility Management Scenarios

1. HNB Initiated UE Registration

[00113] After an HNB is registered with a HNB-GW, the HNB establishes a short range licensed wireless service region of the HNB system. When UEs enter the service region, the HNB performs a registration procedure to authorize the UE for HNB service for the service region of a particular HNB. UE registration first determines whether the HNB is permitted to access services of the HNB system through the particular service region associated with the HNB

on which the UE is camped. In some embodiment, the UE registration also serves to determine what services the UE is authorized to access from that particular service region. Similar to the HNB registration, UE registration is performed through the HNB-GW.

[00114] Based on the service policy of the HNB system provider, UEs may be restricted to service through certain HNBs i.e. the HNBs may have a closed subscriber group (CSG) for allowing access through the particular HNB. In some embodiments, the UE is allowed service through an HNB that is associated with the user's home location. In some embodiments, the UE is allowed HNB service through certain HNB hotspots. By providing registration through the HNB-GW, some embodiments provide a central location whereby access to the HNB services can be controlled

[00115] **Figure 7** illustrates UE registration with the HNB, in some embodiments. Here, the HNB 705 registers a specific UE 710 with the HNB-GW 715. The registration is triggered when the UE 710 attempts to access the HNB 705 for the first time via an initial NAS message (e.g. Location Updating Request).

[00116] In the example of **Figure 7**, upon camping on the HNB 705, the UE 710 initiates (at step 1a) a Location Update procedure by establishing an RRC connection with the HNB 705 (it can be assumed that the HNB 705 has a location area that is distinct from its neighboring HNB and macro cells to trigger an initial message upon camping on the HNB 705). The UE 710 then transmits (at step 1b) a NAS message carrying the Location Updating Request message with some form of identity (IMSI/TMSI). If the (P)TMSI of the UE 710 (provided during RRC Connection Establishment) is unknown at the HNB being accessed (e.g., first access attempt by this specific UE using the (P)TMSI, the HNB requests (at step 1c) the IMSI of the UE and the UE replies at step 1d. In some embodiments where the networks support network mode 1, the UE could trigger a combined Routing Area and Location Area update request instead of the initial LU request. The HNB may also optionally perform local access control for faster rejection of those UEs not authorized to access the particular HNB. If the HNB performs the local access control, then unauthorized UEs are not attempted to be registered with the HNB-GW.

[00117] The HNB 705 attempts (at step 2) to register the UE 710 on the HNB-GW 715 over the UE specific transport session by transmitting the HNBAP UE REGISTER REQUEST. The message contains location information and the UE identity such as the IMSI of the (U)SIM

associated with the UE. The HNB identity over which the UE is attempting access can be inferred or derived by the HNB-GW based on HNB registration and the associated transport session (e.g. SCTP session) since the UE registration is also attempted (by the HNB) using the same transport session.

[00118] The HNB-GW 715 performs access control for the particular UE 710 attempting to utilize the specific HNB 705. If the HNB-GW 715 accepts the registration attempt, it responds (at step 3) with a HNBAP UE REGISTER ACCEPT message back to the HNB 705. In some embodiments, the HNB-GW 715 also assigns information specific to the UE 710 such as SAI specific to the registered UE, UE Context Id (for use in the RUA layer), etc. The UE Context Id provides a unique identifier for each UE within a particular HNB-GW. The UE Context Id is used to identify a logical Iuh signalling connection for a given UE. Additionally, since the UE Context Id is unique within the HNB-GW, it is also used (e.g. by the HNB) as the "Iu signalling connection identifier" in corresponding RANAP messages for that particular UE.

[00119] The HNB 705 performs (at step 4) a NAS relay of the Location Updating Request message from the UE 710 to the HNB-GW 715 via the use of RANAP Initial UE Message. The RANAP Initial UE Message is encapsulated in the RUA message header with additional necessary information which enables the HNB-GW 715 to relay RANAP message towards the appropriate CN entity.

[00120] The HNB-GW 715 establishes (at step 5) an SCCP connection to the CN 720 and forwards the Location Update request (or the combined RA/LA update request) NAS PDU to the CN 720 using the RANAP Initial UE Message. Subsequent NAS messages between the UE 710 and core network 720 will be sent between the HNB 705/HNB-GW 715 and the CN 720 using the RANAP Direct Transfer message encapsulated in the RUA header.

[00121] The CN 720 authenticates (at step 6) the UE 710 using standard authentication procedures. The CN 720 also initiates the Security Mode Control procedure. The NAS messages are relayed transparently by the HNB-GW 715 and the HNB 705 between the UE 710 and the CN 720. The CN 720 indicates (at step 7) it has received the location update and it will accept the location update using the Location Update Accept message to the HNB-GW 715. The HNB-GW 715 relays (at step 8) the LU Accept NAS message to the HNB 705 via the use of RANAP

Direct Transfer message encapsulated in the RUA header. The HNB 705 relays (at step 9) the LU Accept over the air interface to the UE 710 and the procedure is completed.

[00122] In some embodiments, the HNB has a location area that is distinct from its neighboring HNB and macro cells in order to trigger an initial message from a UE upon the UE camping on the HNB. The uniqueness of location is with respect to neighbors of a given HNB, which includes other surrounding HNBs and macro cells. It is neither required nor feasible to have a system-wide (i.e., across PLMN) unique location area for each HNB. Multiple HNBs are able to re-use the location area with the above consideration (i.e., non-conflicting with other neighbors). This unique location area is required to trigger an initial UE message and serves to perform access control and rejection of unauthorized UEs upon initial cell reselection and camping on the HNB; and, to track authorized UEs, in order to minimize the impact of paging at the HNB-GW as well as the HNB (via UE registration).

[00123] Once the UE has successfully registered with the HNB-GW and performed a successful location update, the HNB may expect a periodic LU for that UE (the enabling and the periodicity of the LU is controlled by the HNB via System Information broadcast from the HNB to the UE). This exchange will serve as a keep-alive between the HNB and the UE and will help the HNB detect idle UEs moving away from the camped HNB without explicit disconnect from the network.

a) **Abnormal Cases**

[00124] When the unauthorized UE is not allowed to camp on the HNB, the HNB-GW responds to the UE registration with a HNBAP REGISTRATION REJECT message to the HNB. The HNB is then expected to reject the corresponding UE using appropriate reject mechanisms. For example, some rejection mechanisms include RRC rejection or redirection to another cell or reject the LU with cause such as "Location Area not allowed", etc.

[00125] When the unauthorized UE is allowed to camp in idle mode only, the HNB-GW responds to the UE registration with a HNBAP REGISTRATION ACCEPT message to the HNB and also includes a cause code indicating the limited camping of the UE (i.e., idle mode only). The HNB continues with the Location Update NAS message processing. At the completion of a successful location update procedure, if this unauthorized UE now attempts a subsequent L3

transaction (e.g., a mobile originated service request), the HNB will use the appropriate mechanisms (e.g., RRC redirection or relocation) to redirect the UE to another macro cell for the active call.

b) **Iuh Registration and Paging Optimization for CSG UEs**

[00126] A HNB can be deployed in multiple access modes. When the HNBs are deployed in closed access mode (meaning only a certain group of users are allowed access), a mechanism for access control is implemented via enforcement in the network (either the radio access network or the core network). As a result, the network must reject un-authorized UEs (i.e. UEs not subscribing to a particular HNB). The allowed CSG list stored on the UE or in the subscriber database record (such as in the HLR or HSS) is also known as the white-list.

[00127] The CSG capable HNB broadcasts a CSG-Id over the air interface. In some embodiments, the CSG-Id refers to a single cell, and in other embodiments, the CSG-Id may be shared by multiple CSG cells. Additionally, the HNB may also include an indication on whether the cell belongs to a closed subscriber group. The CN elements (MSC/VLR/SGSN) are assumed to be CSG capable i.e. they are able to access the allowed CSG list (i.e. white-list) of a particular UE (i.e. subscriber) and to enforce access control for each subscriber.

[00128] Subscribers can be equipped with either a legacy UE or a CSG capable UE. The legacy UE's decision to select a particular HNB may be based on macro NCL (e.g. if moving from macro coverage into HNB coverage area in idle mode) or based on full scan of all available cells for a particular operator PLMN (e.g. if there is no macro coverage in idle mode). CSG capable UEs do not need the macro NCL assistance and are capable of selecting the HNB autonomously based on the White-List on the (U)SIM or manual selection using the CSG-Id/ "HNB Display Identity" broadcast by the HNB. However, if macro NCL includes HNB neighbors, then a CSG capable UE may use that information for initial scanning of the HNB but the eventual decision to select the particular HNB is based on the white-list or manual selection decision.

[00129] The following sub-sections describe CSG UE registration over the Iuh interface as well as the various mechanisms which would allow Page messages from the CN to be filtered at the HNB-GW (i.e. send the Page message to the specific HNB where the UE is camped) without

any dependency or need for specific co-relation between the CSG-Id and Location area of the HNBs (or with the macro LA).

i. UE Registration

[00130] Use of UE registration for CSG UEs over Iuh interface requires the HNB to trigger UE registration upon HNB cell selection. The HNB can rely upon an initial L3 transaction (e.g. LAU or Paging Response) to perform UE registration (similar to UE registration supported for legacy i.e. pre-CSG systems). For the CSG systems case, since the access control is performed in the CN, the HNB must also monitor for successful confirmation of the initial L3 transaction (e.g. LAU Accept). If the HNB detects failure in the L3 procedure, the HNB must trigger deregistration of the CSG UE. The UE registration procedure as defined for legacy systems requires the HNB to know the permanent identity (IMSI) of the UE and the IMSI is obtained via identity request procedure which is considered a breach of the current user confidentiality assumptions in macro networks. The following describes a solution, in some embodiments, which avoids the need for issuing an identity request (over the air interface) for CSG UEs Registration procedure.

1. Resolving identity issues for UE registration

[00131] The UE permanent identity is required in legacy (i.e. pre-CSG) environments to perform access control and to perform paging filtering (in the HNB-GW) using the IMSI. In the CSG environment, the access control is performed by the CN using CSG-id and the white-list on the UE. This leaves the problem of paging filtering. The paging filtering using UE registration, in the legacy system (i.e. pre-CSG UE/HNB), is triggered by HNB using the IMSI as the identity. Some embodiments modify the UE registration to allow UE registration using the {TMSI/P-TMSI, LAC} as temporary UE identity (Note: LAC is required since TMSI is unique within given LAC only and 2 simultaneous UE registration must be handled). The NAS message triggering UE registration (LAU or CSG Update) will result in the RANAP Common-Id procedure being sent by the CN towards the HNB-GW and will include the IMSI. This allows the HNB-GW to associate the UE context (created at UE registration using a temporary identity, such as (P)TMSI, with the particular IMSI. Subsequent paging can be filtered at the HNB-GW using the IMSI stored in the UE context.

[00132] **Figure 8** illustrates a procedure for the HNB-GW to allow UE registration using temporary identity (e.g. TMSI or PTMSI) in some embodiments. The HNB-GW subsequently receives the permanent identity from the core network (CN) and associates the above said UE registration with the permanent identity i.e. IMSI of the UE.

[00133] As shown, UE 805 selects (at step 1) and camps on the HNB 810 using its white-list (or allowed CSG list) and CSG information broadcast by the HNB 810. The UE 805 then sends (at step 2) an initial NAS (L3) message towards the HNB 810 (e.g. LAU request or Page response) containing only a temporary UE identity such as the TMSI (CS domain) or PTMSI (PS domain). The HNB 810 initiates (at step 3) a UE registration towards the HNB-GW 815 with this temporary UE identity without any further identity request from the UE 805 over the air interface. The HNB-GW 815 accepts (at step 4) the UE registration using the temporary identity and includes a unique context id in the UE registration accept message. The initial NAS message is forwarded (at steps 5-8) towards the CN 820 followed by authentication and other normative procedures. The CN 820 then sends (at step 9) the RANAP Common Id message containing the UE's permanent identity i.e. IMSI. The HNB-GW 815 then associates (at step 10) the existing UE registration and context Id with the IMSI obtained in this manner.

[00134] It should be noted that if the RRC "cell update" (or equivalent) procedure is used instead of NAS level messaging for indication of HNB selection by the CSG UE, then IMSI cannot be obtained from the CN. This would then require that the HNB perform an identity request or require that the CSG UE include the IMSI in the RRC "cell update" (or equivalent) procedure.

2. Inclusion of CSG-id in the page message from CN

[00135] As described above, the CN is able to access the allowed CSG list (i.e. white-list) of a particular UE (i.e. subscriber). By including target CSG-Id (i.e., the Allowed CSG list, white-list, CSG identity, etc.) in the Page message from the CN, the HNB-GW can send the page to the correct HNB, and IMSI becomes a non-issue. However, this mechanism does require modification to existing RANAP Page messages from the CN. Additionally, the CN may be required to include the CSG-Id conditionally towards the HNB-GW and never towards a macro RNC.

2. Relocation

[00136] The above registration scenarios do not account for scenarios covering (1) connected mode mobility (i.e., handover or relocation) from macro network to a HNB and (2) connected mode mobility (i.e., handover or relocation) from one HNB to another HNB. Specifically, the UE registration procedure, as described above and as described in 3GPP Technical Specification 25.467 entitled "UTRAN architecture for 3G Home NodeB; Stage 2" and 3GPP Technical Specification 25.469 entitled "UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling," hereinafter "TS 25.467" and "TS 25.469," which are incorporated herein by reference, is triggered upon an initial message from a UE to a given HNB.

[00137] Furthermore, as described above and as described in 3GPP Technical Specification 25.468 entitled "UTRAN Iuh Interface RANAP User Adaption (RUA) signalling," hereinafter "TS 25.468," which is herein incorporated by reference, a UE Context Id which is part of the "UE-associated Signalling Connection" over Iuh interface is setup as part of UE registration only. In some embodiments, the UE Context Id, which is used to identify a logical Iuh signalling connection for a given UE, is set up via a UE registration procedure only. In supporting the above two scenarios, UE associated Signalling Connection over Iuh interface may be established and may not be based on initial message from the UE. For instance, the connection may be established based on CN initiated or HNB-GW initiated messages. Several embodiments for network triggered setup of UE-associated Signalling Connection over Iuh covering the above scenarios are described in the following sections.

a) Implicit UE Registration

[00138] **Figure 9** illustrates a network-triggered UE registration in some embodiments. As shown, HNB-GW 910 receives (at step 0) a relocation trigger from the CN or a HNB (not shown). In some embodiments, the relocation trigger is a handover message which initiates an inbound relocation of a UE to the HNB-GW 910. Next, HNB_GW 910 determines (at step 1) the target HNB. HNB-GW 910 then allocates a UE Context Id and sends (at step 2) a RANAP message encapsulated in the RUA header of a RUA message to the target HNB 910. The RUA message includes the UE Context Id and the CN domain identification. In some embodiments, the RANAP message is a RANAP Relocation Request message. In some embodiments, the

RUA message is a RUA Direct Transfer message which contains the UE Context Id allocated by HNB-GW 910. In some embodiments, the RUA message is a RUA Connect message which contains the UE context Id allocated by the HNB-GW.

[00139] The RUA message with the new UE Context Id acts (at step 3a) as an implicit register request to the target HNB 905. The RUA message is implicit because the RUA message is not an explicit command to register the UE (e.g. a HNBAP UE Register Command) from HNB-GW 910. Instead, the RUA message causes the target HNB 905 to allocate resources for the UE relocation. Upon receiving the RUA message from HNB-GW 910, the target HNB 905 inspects the encapsulated RANAP message to extract other necessary information (e.g. UE IMSI) to create appropriate UE registration at the target HNB 905.

[00140] Upon a successful creation of UE registration, the target HNB 905 sends (at step 5) to HNB-GW 910 a RUA message encapsulating a RANAP message, indicating the successful creation of UE registration as well as a successful handling of the RANAP message encapsulated in the RUA message received (at step 2) from HNB-GW 910. In some embodiments, the RUA message sent (at step 5) to HNB-GW 910 from the target HNB 905 is an RUA Direct Transfer message and the RANAP message encapsulated in this RUA message is a RANAP Relocation Request Ack message. This network-triggered UE registration is described in detail further below.

[00141] As defined in TS 25.413, an Iu signalling connection identifier is a 24-bit IE which uniquely identifies an Iu signalling connection between a given RNC (or a given HNB-GW) and a given CN. Furthermore, it is also described that the most significant bit (MSB) of an Iu signalling connection identifier of a RANAP message indicates the node that has assigned a value to the identifier. When the value is assigned to the identifier by the CN, the MSB of the identifier has to be 1 and when it is assigned by RNC or HNB-GW the MSB has to be 0.

[00142] A UE Context Id is also a 24-bit IE in some embodiments and is a unique identifier allocated by the HNB-GW for a particular UE, as described in TS 25.467. Also, as described in TS 25.468, a UE Context Id can be utilized as an Iu signalling connection identifier value for use in the RANAP messages exchanged by a HNB and the HNB-GW to which the HNB is communicatively connected for a given UE. The HNB-GW must take into account the rules described in the previous paragraph when allocating UE Context Ids. Therefore, when a UE

Context Id allocated by a HNB-GW is utilized as Iu signalling connection identifier value, the MSB of the UE Context Id must be a 0 because it is the HNB-GW that assigned a value to the Iu signalling connection identifier and RANAP messages which are initiated by the radio access network shall have MSB of Iu signalling connection identifier set to value 0.

[00143] The above rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value pose a problem when they are applied during a handover procedure from a macro network cell to a target HNB. Specifically, the RANAP messages (for example, RANAP Relocation Request message) which are initiated from the CN and which trigger the creation of UE registration by the HNB-GW, carry the Iu signalling connection identifier allocated by the CN. These same messages will also result in creation of UE associated signalling connection over the Iuh interface. This will require the HNB-GW to allocate a context Id for the UE registration. However, the context Id which the HNB-GW allocated must have the MSB set to 0 and hence cannot have the same value as that assigned to the "Iu signalling connection identifier" IE in the corresponding RANAP message triggered by the CN which must have the MSB set to 1.

[00144] **Figure 10** illustrates problems associated with handling of UE Context Id and Iu signalling connection identifier. Specifically, **Figure 10** illustrates a CS/PS handover from a macro network cell to a HNB (i.e. from the macro network via the CN to the HNB) in some embodiments. In some embodiments, this procedure is performed when the UE 1005 is on an active CS/PS session (i.e., a communication session exchanging voice, data, or both) on the macro network cell (not shown) and has been commanded (e.g. by a source RNC, not shown) to make measurements on neighboring HNBs.

[00145] In some embodiments, the source RNC is able to provide information on neighboring cells such that one of the cells in the neighbor list matches the cell associated with the target HNB 1010. Also, HNB-GW 1015 is able to determine the target HNB based on the information contained in the handover message received from the source RNC (i.e. via CN 1020). An example of a mechanism to determine a target HNB is described in United States Patent Application 11/933,347, entitled "Method and Apparatus to Enable Hand-in for Femtocells", filed on April 17, 2009, which is incorporated herein by reference.

[00146] As shown in **Figure 10**, CN 1020 sends (at step 1) a message which triggers an inbound relocation of UE 1005 to HNB-GW 1015. In some embodiments, the relocation message is a RANAP message, e.g., a RANAP Relocation Request message for relocating an ongoing CS/PS session on UE 1005 to HNB-GW 1015. The RANAP message includes the UE IMSI. The RANAP message also includes Iu signalling connection identifier. The MSB of the Iu signalling connection identifier value of the RANAP message is a 1 because CN 1020 assigned the value to the Iu signalling connection identifier. This is symbolically shown as a value of 1xxx which denotes a 24-bit value with a 0 as the MSB. This notation is used in **Figure 10** and other figures in the following sections.

[00147] Next, HNB-GW 1015 determines (at step 2) the target HNB based on the information contained in the handover message from CN 1020. HNB-GW 1015 then allocates a UE Context Id and sends (at step 3) the RANAP Relocation Request message encapsulated in the RUA header of a RUA message to the target HNB 1010. The RUA message includes the UE Context Id and the CN domain identification. The UE Context Id has a 0 as its MSB because it is allocated by HNB-GW 1015 and is going to be used as the Iu signalling connection identifier value of the RANAP messages constructed by HNB-GW 1015 or the target HNB 1010. However, as described in step 1, above, this RANAP message is constructed by and originated from CN 1020. Therefore, the MSB of the Iu signalling connection identifier value of the RANAP message is 1, as shown in step 3. In some embodiments, the RUA message is a RUA Direct Transfer message that contains the UE Context Id allocated by HNB-GW 1015.

[00148] The RUA message with the UE Context Id acts (at step 4a) as an implicit register request to the target HNB 1010. As described above, the RUA message is implicit because the RUA message is not an explicit command to register the UE (e.g. a HNBAP UE Register Command) from HNB-GW 1015. Instead, the RUA message causes the target HNB 1005 to allocate resources for the UE registration. Upon receiving the RUA message from HNB-GW 1015, the target HNB 1010 inspects the encapsulated RANAP Relocation Request message to extract other necessary information (e.g. UE IMSI) to create appropriate UE registration at the target HNB 1010.

[00149] Upon a successful creation of UE registration, the target HNB 1010 sends (at step 5) to HNB-GW 1015 a RUA message encapsulating a RANAP message, indicating the

successful creation of UE registration as well as a successful handling of the RANAP message encapsulated in the RUA message received (at step 3) from HNB-GW 1015. In some embodiments, the RUA message sent (at step 5) to HNB-GW 1015 from the target HNB 1010 is an RUA Direct Transfer message and the RANAP message encapsulated in this RUA message is a RANAP Relocation Request Ack message. The MSB of the Iu signalling connection identifier value of the RANAP message constructed by the target HNB 1010 is 0 because the target HNB 1010 is to use the UE Context Id, which has a 0 as its MSB, as the Iu signalling connection identifier value for the RANAP messages the HNB 1010 constructs, as shown in step 5.

[00150] The target HNB 1010 sends (at step 5) the RANAP message to HNB-GW 1015 encapsulated in the RUA message which also includes the UE Context Id and the CN domain identification. HNB-GW 1015 relays (at step 6) this RANAP message to CN 1020. Since this RANAP message is a response by HNB-GW 1015 to the RANAP message received (at step 1) from CN 1020, the response RANAP message must have the same Iu signalling connection identifier value as the Iu signalling connection identifier value of the RANAP message sent (at step 1) to HNB-GW 1015. Otherwise, CN 1020 would not be able to recognize the response RANAP message as the response to its RANAP message sent (at step 1) to HNB-GW 1015. However, the response RANAP message already has a different Iu signalling connection identifier value (with a 0 as its MSB) as shown in steps 5 and 6.

[00151] In order to solve the problems described above (such as handling scenarios where the Context Id and the Iu signalling connection identifier are not the same), several examples are described in the following sections. These examples use the MSB of UE Context Id and/or the MSB of Iu signalling connection identifier to identify the node that has assigned a value to the identifier. It would be apparent to a person of ordinary skill in the art that other portions of these identifier, other flags or information elements, or other techniques known in the art can be used to identify the node that has initiated the message that triggers relocation without deviating from the teaching of the invention.

[00152] Accordingly, in order to simplify the description of embodiments described in **Figures 10** to **18**, reference has been made to specific examples such as the value of the "MSB" bit of certain values, UE Context Id, Iu signalling connection identifier, Iu signalling connection, Iu, RANAP, RUA, CN, HNB-GW, HNB, RNC, and several other terms. However, the invention

is not intended to be limited to these narrow definitions and examples. Specifically, instead of the value of an MSB bit, any other value, flag, or indicator being single bit or multiple bit can be used as an identifier. Instead of Iu signalling connection identifier and UE Context Id any first and second identifiers can be used. Instead of Iu signalling connection, any other connections between two nodes of the communication system that are capable to carrying a voice session, a data session, or both for a user equipment can be used. Instead of the Iu interface any other interface capable of supporting such voice and/or data sessions for a user equipment can be used. Furthermore, RANAP and RUA are just examples of messaging protocols used in communication systems. Any other suitable protocols can be used. The specific type of messages such as relocation request, direct transfer, relocation request ack, etc. are examples of the messages that can be used to perform the specific actions disclosed in **Figures 10** to **18**. Furthermore, CN, HNB-GW, HNB, and RNC are examples of nodes in a communication system. Other type of nodes such as network controllers, access points, gateways, and radio controllers can be used. The above generalization applies to individual description and drawings for **Figures 10** to **18** and is not repeated during description of each individual figure in order to enhance the readability of the disclosure. It will be clear and apparent to one skilled in the art that the invention is not limited to specific narrow examples set forth and that the invention may be practiced without the use of the specific details and examples discussed.

[00153] In some of the solutions described in the following sections, a HNB is disclosed that is able to determine and distinguish UE-associated signalling connections which are triggered by the network and UE-associated signalling connections that are triggered by the HNB. In other solutions described in the following paragraphs, a HNB-GW is disclosed that is able to determine and distinguish UE-associated signalling connection which are triggered by the network and UE-associated signalling connections that are triggered by the HNB.

i. Relocation from Macro Network Cell to Target HNB

[00154] **Figure 11** illustrates a first solution in some embodiments. Steps 1-4b are the same as steps 1-4b described above in **Figure 10**. In this embodiment, the target HNB 1010 determines whether the encapsulated RANAP message (received at step 3) is initiated from CN 1020 (i.e. whether the MSB of the Iu signalling connection identifier value of the RANAP message coming to the HNB 1010 is 1). When the RANAP message is initiated from the CN, the

target HNB 1010 instead of using the UE Context Id allocated by HNB-GW 1015, uses the Iu signalling connection identifier value of the encapsulated RANAP message from the HNB-GW 1015 for the entire duration of Iu signalling connection associated with UE 1005 (i.e. for the duration of the ongoing CS/PS session, until the signalling connection over the Iuh interface ends).

[00155] In some embodiments, the HNB 1010 uses the Iu signalling connection identifier value of the RANAP message initiated from CN 1020 when the HNB 1010 constructs a response RANAP message. Then, as shown in steps 1 and 5, the RANAP message constructed and sent (at step 5) by the target HNB 1010 to HNB-GW 1020 has the same Iu signalling connection identifier value as that of the RANAP message initiated (at step 1) from CN 1020. The MSB of this Iu signalling connection identifier value would be 1 because the RANAP Relocation Request message was initiated (at step 1) from CN 1020.

[00156] Upon receiving (at step 5) the RUA message encapsulating the RANAP message, HNB-GW 1015 relays (at step 6) to CN 1020 the RANAP message without inspecting it because HNB-GW 1015 is able to find out that the RANAP message is a response message to the RANAP message initiated (at step 1) from CN 1020, for instance, by looking at the UE Context Id contained in the RUA message. CN 1020 would recognize that the RANAP message received from (at step 5) from HNB-GW1015 is a response to its RANAP message sent (at step 1) to HNB-GW 1015 because the Iu signalling connection identifier value of the RANAP message received (at step 6) is the same as the Iu signalling connection identifier value of the RANAP Relocation Request message sent (at step 1) to HNB-GW 1015, as shown in steps 1 and 6. The remaining exchange of relocation messages continues (at step 7) among UE 1005, the target HNB 1010, HNB-GW 1015, and CN 1020.

[00157] The advantage of this solution is that a HNB-GW does not have to intercept and process the RANAP messages coming to the HNB-GW for manipulation of the Iu signalling connection identifier and thus can function as transparent as possible to the RANAP messages.

[00158] **Figure 12** illustrates a second solution in some embodiments. Steps 1-4b are the same as steps 1-4b described above in **Figure 10**. In this embodiment, the target HNB 1010 keeps using the UE Context Id allocated by HNB-GW 1015 as the Iu signalling connection identifier values of the RANAP messages that the target HNB 1010 constructs, regardless of the

kind of the node that the RANAP messages the HNB 1010 receives are initiated from. However, HNB-GW 1015 determines whether the RANAP messages coming from the target HNB 1010 (at step 5) are responses to the RANAP messages initiated (at step 1) from the CN 1020. In some embodiments, HNB-GW 1015 keeps a mapping that associates the UE Context Ids with the Iu signalling connection identifier values of the RANAP messages received from CN 1020 and relayed to the target HNB 1010 so that HNB-GW 1015 is able to determine whether the RANAP messages coming from the target HNB 1010 are responses to the RANAP messages that HNB-GW 1015 received from CN 1020 and relayed to the HNB 1015.

[00159] In some embodiments, as shown in step 5, the RANAP message encapsulated in the RUA message sent (at step 5) by the target HNB 1010 to HNB-GW 1015 has the UE Context Id (with 0 as the MSB) allocated by HNB-GW 1015 as the Iu signalling connection identifier value. However, upon receiving the RUA message from the target HNB 1010, HNB-GW 1015 determines that the RANAP message encapsulated in the RUA header is a response to the RANAP message HNB-GW 1015 received (at step 1) from the CN 1020. In some embodiments, the HNB-GW maintains the state of the UE sessions and from the state of the UE sessions is able to determine that a particular message is a response to a particular message from the CN.

[00160] Once HNB-GW 1015 determines that the RANAP message received (at step 5) is a response to the RANAP message received (at step 1) from CN 1020, HNB-GW 1015 inspects the RANAP message and replaces the Iu signalling connection identifier value of the RANAP message with the Iu signalling connection identifier value of the RANAP message received (at step 1) from CN 1020. As shown in steps 1 and 6, the RANAP message that is being sent (at step 6) to CN 1020 will have the same Iu signalling connection identifier value as that of the RANAP message that HNB-GW 1015 received (at step 1) from CN 1015. Then CN 1015 would be able to recognize that this RANAP message is a response to the RANAP message CN 1015 sent (at step 1) to HNB-GW 1015. The remaining exchange of relocation messages continues (at step 7) among UE 1005, the target HNB 1010, HNB-GW 1015, and CN 1020.

[00161] The advantage of the second solution is that a UE Context Id can be utilized as the Iu signalling connection identifier value for use in RANAP messages exchanged by a HNB and the HNB-GW that the HNB is communicatively connected to. Therefore, a HNB can follow the

rule for using a UE Context Id as the Iu signalling connection identifier of the RANAP messages that it constructs.

ii. Relocation from one HNB to another HNB

[00162] Unlike the handover procedures for an ongoing CS/PS session from the macro network to a target HNB described above, a handover procedure for an ongoing CS/PS session from a HNB to another HNB does not have a problem with applying the rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value. The RANAP messages (for example, RANAP Relocation Required message) which are initiated from one HNB and which trigger the creation of UE registration by the HNB-GW, carry the Iu signalling connection identifier previously allocated by the HNB-GW which must have the MSB set to 0. Therefore, the context Id which the HNB-GW allocated can have the MSB set to 0 in accordance with the rule.

[00163] For setup of UE associated signalling connection initiated by the UE, for instance, by an initial message of a UE in an attempt to register with the HNB-GW, the HNB uses the UE Context ID as the Iu signalling connection identifier in corresponding RANAP messages for the entire duration of that UE-associated signalling connection in some embodiments.

[00164] **Figure 13** illustrates a network-triggered UE registration in some embodiments. Specifically, **Figure 13** illustrates a CS/PS handover from one HNB to another HNB both of which are communicatively connected to the same HNB-GW. In some embodiments, this procedure is performed when the UE 1305 is on an active CS/PS session on the source HNB 1320 and has been commanded (by the source HNB 1320) to make measurements on neighboring HNBs.

[00165] In some embodiments, the source HNB 1320 is able to provide information on neighboring HNBs such that one of the HNBs in the neighbor list matches the target HNB 1310. Also, HNB-GW 1315 is able to determine the target HNB based on the information in the handover message received from the source HNB 1320. An example of a mechanism to determine a target HNB is described in the above mentioned United States Patent Application 11/933,347.

[00166] As shown in **Figure 13**, the source HNB 1320 sends (at step 1) a handover message which triggers an inbound relocation of UE 1305 from the source HNB 1320 to the target HNB 1310. In some embodiments, the handover message is a RANAP message, for instance, a RANAP Relocation Required message for an ongoing CS/PS session on UE 1005 to HNB-GW 1315. Next, HNB-GW 1315 determines (at step 2) the target HNB based on the information contained in the handover message from the source HNB 1320.

[00167] In some embodiments, HNB-GW 1315 then allocates a new UE Context Id so as to uniquely identify the UE 1305 over the Iuh interface within the target HNB 1310 and HNB-GW 1315. In some embodiments, for the messages exchanged between the HNB-GW 1315 and the HNB 1305, the HNB-GW 1315 can use the same UE Context Id received (at step 1) from the source HNB 1320 instead of allocating a new UE Context Id because a UE Context Id is allocated by a given HGW-GW and is unique among the HNBs communicatively connected to the HGW-GW.

[00168] The HNB-GW 1315 then constructs (at step 3) a RANAP message and sends it to the target HNB 1310 using a RUA message encapsulating the RANAP message. In some embodiments, the RANAP message is a RANAP Registration Request message. In some embodiments, the RUA message is a RUA Direct Transfer message that also contains the UE Context Id and the CN domain identification.

[00169] The RUA message with the UE Context Id acts (at step 4a) as an implicit register request to the target HNB 1310. As described above, the RUA message implicit because the RUA message is not an explicit command to register the UE (e.g. a HNBAP UE Register Command) from HNB-GW 1315. Instead, the RUA message causes the target HNB 1305 to allocate resources for the UE registration. Upon receiving the RUA message from HNB-GW 1315, the target HNB 1310 inspects the encapsulated RANAP Relocation Request message to extract other necessary information (e.g. UE IMSI) to create appropriate UE registration at the target HNB 1310.

[00170] Upon a successful creation of UE registration, the target HNB 1310 constructs a RANAP message and sends (at step 5) to the HNB-GW 1315 using a RUA message encapsulating the RANAP message. In some embodiments, the RUA message is a RUA Direct Transfer message. In some embodiments, the encapsulated RANAP message is a RANAP

Relocation Request Ack message, indicating the successful creation of UE registration as well as a successful handling of the RANAP message encapsulated in the RUA message received (at step 4) from the HNB-GW 1315.

[00171] The HNB-GW 1315 then signals (at step 6) the source HNB 1320 to handover the UE 1305 to the target HNB 1310, using a RANAP message encapsulated in a RUA message. In some embodiments, the RANAP message is a RANAP Relocation Command message. In some embodiments, the RANAP message is a RUA Direct Transfer message. The remaining exchange of relocation messages continues (at step 7) among UE 1305, the target HNB 1310, HNB-GW 1315, and the source HNB 1320.

[00172] As described above, unlike the handover procedures for an ongoing CS/PS session from a macro network to a target HNB described above, a handover procedure for an ongoing CS/PS session from a HNB to another HNB does not have a problem with applying the above mentioned rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value in some embodiments. **Figures 14 and 15** illustrate the same handover procedure illustrated in **Figure 13** with steps showing the values of UE Context Id and Iu signalling connection identifier in RANAP messages. As described above, for the messages exchanged with the target HNB 1310, HNB-GW 1315 can use the same UE Context Id used for messages exchanged with the source HNB 1320 or allocate another UE Context Id.

[00173] **Figure 14** illustrates an example in which HNB-GW 1315 uses the same UE Context Id for both the RUA messages that HNB-GW exchanges with the source HNB 1320 and for the RUA messages HNB-GW exchanges with the target HNB 1310. The source HNB 1320 sends (at step 1) an RUA message. As shown in step 1, the value of the UE Context Id is 0xxx. The UE Context Id has a 0 as its MSB because it used as Iu signalling connection identifier values of the RANAP messages constructed by HNB-GW 1315 or the source HNB 1320. The RANAP message encapsulated (at step 1) in the RUA Direct Transfer message also has 0xxx as shown in step 1, because the source HNB 1320 used the UE Context Id when the RANAP message was constructed by the source HNB 1320.

[00174] When HNB-GW 1315 constructs a RUA message to send to the target HNB 1310, HNB-GW 1310 uses the same UE Context Id it received (at step 1) from the source HNB 1320.

The RANAP message constructed by HNB-GW 1315, which is encapsulated in the RUA message sent (at step 3) to the target HNB 1310, has the UE Context Id as its Iu signalling connection identifier value, as shown in step 3. Similarly, the RUA and RANAP messages constructed by the target HNB 1310 and HNB-GW 1315 will all have the same UE Context Ids and Iu signalling connection identifier values, as shown in steps 5 and 6.

[00175] **Figure 15** illustrates an example in which HNB-GW 1315 allocates a UE Context Id that is different from the UE Context Id that the HNB-GW 1315 uses for the RUA messages that it exchanges with the source HNB 1315. As shown, the source HNB 1320 sends (at step 1) an RUA Direct Transfer message. As shown in step 1, the value of the UE Context Id is 0xxx. The UE Context Id received at step 1 has a 0 as its MSB because it used as Iu signalling connection identifier values of the RANAP messages constructed by HNB-GW 1315 or the source HNB 1320. Likewise, the UE Context Id allocated by HNB-GW 1315 and sent to the target HNB has a 0 as its MSB because it is also used as Iu signalling connection identifier values of the RANAP messages constructed by HNB-GW 1315 or the target HNB 1310. However, the UE Context Id allocated by HNB-GW 1315 has a different value, for instance, 0yyy, since it is newly allocated by HNB-GW 1315.

[00176] The Iu signalling connection identifier values of the RANAP messages exchanged between the target HNB 1310 and the HNB-GW 1315 will be 0yyy, as shown in steps 3 and 5, because HNB-GW 1315 and the target HNB 1310 used the newly allocated UE Context Id as the Iu signalling connection identifier values of the RANAP messages. When HNB-GW 1315 constructs a RUA message to send to the source HNB 1320, HNB-GW 1310 uses the UE Context Id it received (at step 1) from the source HNB 1320 because this RUA message is going to the source HNB 1320. The RANAP message constructed by HNB-GW 1315, which is encapsulated in the RUA message sent (at step 6) to the target HNB 1310, has the UE Context Id received(at step 1) from the source HNB 1320 as its Iu signalling connection identifier value, as shown in step 6. The UE Context Id from source 1310 and the allocated UE Context Id are different, but all of the Iu signalling connection identifier values will have a 0 as the MSB because the UE Context Ids have a 0 as their MSBs as shown in the above steps.

[00177] As described in the examples of **Figures 14** and **15**, whether the UE Context Ids are the same or different, there is no need for the HNB-GW 1315 to inspect and replace the Iu

signalling connection identifier values of the RANAP messages because in any case UE Context Ids have 0s as their MSBs.

b) Explicit UE Registration Command

[00178] **Figure 16** illustrates a network-triggered UE registration in some embodiments. This UE registration procedure is the similar to the procedure illustrated in **Figure 9** except that there are few more steps associated with an explicit message command to create UE registration.

[00179] As shown, before HNB-GW 1610 sends (at step 3) a RUA message to the target HNB 1605, HNB-GW 1610 sends (at step 2a) an explicit command to the target HNB 1605 to create necessary UE registration. In some embodiments, the explicit command to create necessary UE registration is a HNBAP message. In some embodiments, the HNBAP message is a HNBAP UE Register Command message. The explicit command to create UE registration contains the necessary information (e.g. UE IMSI and a UE Context Id allocated by HNB-GW 1610) to create the necessary UE registration at the target HNB 1605

[00180] In some embodiments, upon receiving the explicit UE Register command to create UE registration, the target HNB 1605 optionally sends (at step 2b) to HNB-GW 1610 an explicit successful confirmation response acknowledging the reception of the explicit command and the new UE Context Id contained in the explicit command. The explicit successful confirmation response also indicates successful creation of UE registration. In some embodiments, the explicit successful confirmation message is a HNBAP message. In some embodiments, the HNBAP message is a HNBAP UE Register Command Confirm message. HNB-GW 1610 then sends (at step 3) to the target HNB 1605 a RUA message encapsulating a RANAP message. In some embodiments, the RANAP message is a RANAP Relocation Request message. In some embodiments, the RUA message is a RUA Direct Transfer message. The message includes the UE Context Id and CN domain identification). HNB-GW 1610 then proceeds with the remainder of the relocation procedure. This network-triggered UE registration is described in detail later in this application.

i. Relocation from Macro Network Cell to HNB Target

[00181] **Figure 17** illustrates a CS/PS handover from a macro network cell to HNB (i.e. from the macro network via CN to HNB) in some embodiments. This handover procedure is

similar to the procedure illustrated in **Figure 10** except that there are few more steps associated with an explicit command to create UE registration. As described above in **Figure 10**, the above rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value pose a problem when they are applied during a handover procedure from a macro network cell to a target HNB. The description of the problem and the two solutions are the same as described in **Figures 10, 11** and **12** and are not described in detail in this section. In other words, in one solution according to some embodiments, the HNB is able to determine and distinguish UE-associated signalling connections which are triggered by the network and signalling connections that are triggered by the HNB. In the other solution, the HNB-GW is able to determine and distinguish UE-associated signalling connections which are triggered by the network and signalling connections that are triggered by the HNB.

[00182] As shown, before HNB-GW 1015 sends (at step 3) a RUA message to the target HNB 1010, HNB-GW 1015 sends (at step 2a) an explicit command to the target HNB 1010 to create necessary UE registration. In some embodiments, the explicit command to create necessary UE registration is a HNBAP message, for instance, a HNBAP UE Register Command message. The explicit command to create UE registration contains the necessary information (e.g. UE IMSI and a UE Context Id allocated by HNB-GW 1015) to create necessary UE registration at the target HNB 1010.

[00183] In some embodiments, upon receiving the explicit UE Register command to create UE registration, the target HNB 1010 optionally sends (at step 2b) to HNB-GW 1015 an explicit confirm response acknowledging the reception of the explicit command and the UE Context Id contained in the explicit command. The explicit confirm response also indicates successful creation of UE registration. In some embodiments, the explicit successful confirmation message is a HNBAP message. In some embodiments, the HNBAP message is a HNBAP UE Register Command Confirm message. HNB-GW 1015 then sends (at step 3) to the target HNB 1010 an RUA message encapsulating the RANAP message received (at step 1) from CN 1020. In some embodiments, the RUA message is a RUA Direct Transfer message. The RUA message includes the UE Context Id and CN domain identification. The target HNB 1010 then allocates (at step 4) resources for relocation. The steps 5- 7 are the same as described above for the steps 5-7 in **Figure 10**.

ii. Relocation from one HNB to another HNB

[00184] **Figure 18** illustrates a CS/PS handover from one HNB to another HNB both of which are communicatively connected to the same HNB-GW in some embodiments. This handover procedure is similar to the procedure illustrated in **Figure 13** except that there are few more steps associated with an explicit command to create UE registration. As described above in **Figure 10**, the above rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value pose a problem when they are applied during a handover procedure from a macro network cell to a target HNB. As described above in **Figures 13, 14** and **15**, unlike the handover procedures for an ongoing CS/PS session from a macro network to a target HNB described above, a handover procedure for an ongoing CS/PS session from a HNB to another HNB both of which are communicatively coupled to a HNB-GW do not have a problem with applying the rules regarding the MSBs of an Iu signalling connection identifier and a UE Context Id used as an Iu signalling connection identifier value in some embodiments.

[00185] As shown, before HNB-GW 1315 sends (at step 3) a RUA message to the target HNB 1310, HNB-GW 1315 sends (at step 2a) an explicit command to the target HNB 1310 to create necessary UE registration. In some embodiments, the explicit command to create necessary UE registration is a HNBAP message, for instance, a HNBAP UE Register Command message. The explicit command to create UE registration contains the necessary information (e.g. UE IMSI and a UE Context Id) to create necessary UE registration at the target HNB 1310.

[00186] In some embodiments, upon receiving the explicit UE Register command to create UE registration, the target HNB 1310 optionally sends (at step 2b) to the HNB-GW 1315 an explicit confirm response acknowledging the reception of the explicit command and the UE Context Id contained in the explicit command. The explicit confirm response also indicates successful creation of UE registration. In some embodiments, the explicit successful confirmation message is a HNBAP message. In some embodiments, the HNBAP message is a HNBAP UE Register Command Confirm message. HNB-GW 1315 then sends (at step 3) to the target HNB 1310 an RUA message encapsulating the RANAP message received (at step 1) from CN 1320. In some embodiments, the RUA message is a RUA Direct Transfer message. The RUA message includes the UE Context Id and CN domain identification. The target HNB 1310

then allocates (at step 4) resources for relocation. The steps 5- 7 are the same as described above for the steps 5-7 in **Figure 13**.

IV. COMPUTER SYSTEM

[00187] Many of the above-described protocol stacks, processes, methods, and functionalities are implemented as software processes that are specified as a set of instructions recorded on a computer readable storage medium (also referred to as computer readable medium). When these instructions are executed by one or more computational or processing element(s) (such as processors or other computational elements like ASICs and FPGAs), they cause the computational element(s) to perform the actions indicated in the instructions. Computer is meant in its broadest sense, and can include any electronic device with computational elements (e.g., HNB and HNB-GW). Examples of computer readable media include, but are not limited to, CD-ROMs, flash drives, RAM chips, hard drives, EPROMs, etc. The computer readable media does not include carrier waves and electronic signals passing wirelessly or over wired connections.

[00188] In this specification, the term "software" is meant in its broadest sense. It can include firmware residing in read-only memory or applications stored in magnetic storage which can be read into memory for processing by a processor. Also, in some embodiments, multiple software inventions can be implemented as sub-parts of a larger program while remaining distinct software inventions. In some embodiments, multiple software inventions can also be implemented as separate programs. Finally, any combination of separate programs that together implement a software invention described here is within the scope of the invention. In some embodiments, the software programs when installed to operate on one or more computer systems define one or more specific machine implementations that execute and perform the operations of the software programs.

[00189] **Figure 19** conceptually illustrates a computer system with which some embodiments of the invention are implemented. The computer system 1900 includes a bus 1905, a processor 1910, a system memory 1915, a read-only memory 1920, a permanent storage device 1925, input devices 1930, and output devices 1935.

[00190] The bus 1905 collectively represents all system, peripheral, and chipset buses that support communication among internal devices of the computer system 1900. For instance, the

bus 1905 communicatively connects the processor 1910 with the read-only memory 1920, the system memory 1915, and the permanent storage device 1925.

[00191] From these various memory units, the processor 1910 retrieves instructions to execute and data to process in order to execute the processes of the invention. In some embodiments the processor comprises a Field Programmable Gate Array (FPGA), an ASIC, or various other electronic components for executing instructions. The read-only-memory (ROM) 1920 stores static data and instructions that are needed by the processor 1910 and other modules of the computer system. The permanent storage device 1925, on the other hand, is a read-and-write memory device. This device is a non-volatile memory unit that stores instruction and data even when the computer system 1900 is off. Some embodiments of the invention use a mass-storage device (such as a magnetic or optical disk and its corresponding disk drive) as the permanent storage device 1925. Some embodiments use one or more removable storage devices (flash memory card or memory stick) as the permanent storage device.

[00192] Like the permanent storage device 1925, the system memory 1915 is a read-and-write memory device. However, unlike storage device 1925, the system memory is a volatile read-and-write memory, such as a random access memory. The system memory stores some of the instructions and data that the processor needs at runtime.

[00193] Instructions and/or data needed to perform processes of some embodiments are stored in the system memory 1915, the permanent storage device 1925, the read-only memory 1920, or any combination of the three. For example, the various memory units include instructions for processing multimedia items in accordance with some embodiments. From these various memory units, the processor 1910 retrieves instructions to execute and data to process in order to execute the processes of some embodiments.

[00194] The bus 1905 also connects to the input and output devices 1930 and 1935. The input devices enable the user to communicate information and select commands to the computer system. The input devices 1930 include alphanumeric keyboards and cursor-controllers. The output devices 1935 display images generated by the computer system. The output devices include printers and display devices, such as cathode ray tubes (CRT) or liquid crystal displays (LCD). Finally, as shown in **Figure 19**, bus 1905 also couples computer 1900 to a network 1965 through a network adapter (not shown). In this manner, the computer can be a part of a network of

computers (such as a local area network ("LAN"), a wide area network ("WAN"), or an Intranet) or a network of networks (such as the Internet).

[00195] Any or all of the components of computer system 1900 may be used in conjunction with the invention. For instance, some or all components of the computer system described with regards to **Figure 19** comprise some embodiments of the UE, HNB, HNB-GW, and SGSN described above. However, one of ordinary skill in the art will appreciate that any other system configuration may also be used in conjunction with the invention or components of the invention.

[00196] Some embodiments include electronic components, such as microprocessors, storage and memory that store computer program instructions in a machine-readable or computer-readable medium (alternatively referred to as computer-readable storage media, machine-readable media, or machine-readable storage media). Some examples of such computer-readable media include RAM, ROM, read-only compact discs (CD-ROM), recordable compact discs (CD-R), rewritable compact discs (CD-RW), read-only digital versatile discs (e.g., DVD-ROM, dual-layer DVD-ROM), a variety of recordable/rewritable DVDs (e.g., DVD-RAM, DVD-RW, DVD+RW, etc.), flash memory (e.g., SD cards, mini-SD cards, micro-SD cards, etc.), magnetic and/or solid state hard drives, read-only and recordable blu-ray discs, ultra density optical discs, any other optical or magnetic media, and floppy disks. The computer-readable media may store a computer program that is executable by at least one processor and includes sets of instructions for performing various operations. Examples of hardware devices configured to store and execute sets of instructions include, but are not limited to application specific integrated circuits (ASICs), field programmable gate arrays (FPGA), programmable logic devices (PLDs), ROM, and RAM devices. Examples of computer programs or computer code include machine code, such as produced by a compiler, and files including higher-level code that are executed by a computer, an electronic component, or a microprocessor using an interpreter.

[00197] As used in this specification and any claims of this application, the terms "computer", "server", "processor", and "memory" all refer to electronic or other technological devices. These terms exclude people or groups of people. For the purposes of the specification, the terms display or displaying means displaying on an electronic device. As used in this specification and any claims of this application, the terms "computer readable medium" and

"computer readable media" are entirely restricted to tangible, physical objects that store information in a form that is readable by a computer. These terms exclude any wireless signals, wired download signals, and any other ephemeral signals.

[00198] Many of the above figures illustrate a single access point (e.g., HNB 205) communicatively coupled to a network controller (e.g., HNB-GW 215). However, it should be apparent to one of ordinary skill in the art that the network controller (e.g., HNB-GW 215) of some embodiments is communicatively coupled to several HNBs and the network controller communicatively couples all such HNBs to the core network. The figures merely illustrate a single HNB communicatively coupled to the HNB-GW for purposes of simplifying the discussion to interactions between a single access point and a single network controller. However, the same network controller of some embodiments may have several of the same interactions with several different access points.

[00199] Additionally, many of the above figures illustrate the access point to be a HNB and the network controller to be a HNB-GW. These terms are used to provide a specific implementation for the various procedures, messages, and protocols described within some of the embodiments described with reference to the figures. However, it should be apparent to one of ordinary skill in the art that the procedures, messages, and protocols may be used with other communication systems and the HNB system was provided for exemplary purposes. For example, such procedures, messages, and protocols may be adapted to function with a Femtocell cell system that includes Femtocell access points and a Femtocell network controller (e.g., Generic Access Network Controller).

[00200] Similarly, many of the messages and protocol stacks were described with reference to particular HNB-AN functionality such as control plane functionality or user plane functionality. However, it should be apparent to one of ordinary skill in the art that such functionality may apply across multiple HNB-AN functions or may apply to a different HNB-AN function altogether. Moreover, it should be apparent to one of ordinary skill in the art that the above described messaging may include additional or alternative information elements to those enumerated above.

[00201] While the invention has been described with reference to numerous specific details, one of ordinary skill in the art will recognize that the invention can be embodied in other

specific forms without departing from the spirit of the invention. Thus, one of ordinary skill in the art would understand that the invention is not to be limited by the foregoing illustrative details, but rather is to be defined by the appended claims.

V. ABBREVIATIONS AND DEFINITIONS

A. Abbreviations

Second Generation of Cellular Wireless Standards	2G
Third Generation of Cellular Wireless Standards	3G
3rd Generation Partnership Project	3GPP
Fourth Generation of Cellular Wireless Standards	4G
Authorization, Authentication, and Accounting	AAA
Access Network	AN
Automatic Number Identification	ANI
Advice of Charge	AoC
Access Point	AP
Asynchronous Transfer Mode	ATM
Base Station	BS
Base Transceiver Station	BTS
Cell Broadcast Center	CBC
Call Control	CC
Cable Modem Termination System	CMTS
Core Network	CN
Customer Premise Equipment	CPE
Circuit Switched	CS
Closed Subscriber Group	CSG
Digital Subscriber Line	DSL
DSL Access Multiplexer	DSLAM
ES Protocol	ESP
Encapsulating Security Payload	ESP

GSM/EDGE Radio Access Network	GERAN
Gateway GPRS Support Node	GGSN
General Packet Radio Service	GPRS
Global System for Mobile communications	GSM
Home Enhanced Node B	HeNB
Home Location Register	HLR
Home Node-B	HNB
HNB Access Network	HNB-AN
HNB Application Part	HNBAP
HNB Gateway	HNB-GW
Information Element	IE
Internet Assigned Numbers Authority	IANA
Identifier	ID
International Mobile Subscriber Identity	IMSI
Internet Protocol	IP
IP Security	IPSec
Internet Service Provider	ISP
Interworking Functionality	IWF
Layer 3	L3
Location Area	LA
Location Area Code	LAC
Location Area Identifier	LAI
Location Area Update	LAU
Location Update	LU
MTP3 User Adaptation Layer	M3UA
Media Access Control	MAC
Mobility Management	MM

Most Significant Bit	MSB
Mobile Switching Center	MSC
Non Access Stratum	NAS
Network Address Translation	NAT
Neighbor Configuration List	NCL
Personal Communication Services	PCS
Packet Control Unit	PCU
Protocol Data Unit	PDU
Public Land Mobile Network	PLMN
Payload Protocol Identifier	PPI
Packet Switched	PS
Public Switched Telephone Network	PSTN
Packet-Temporary Mobile Subscriber Identity	P-TMSI (or PTMSI)
Either Packet TMSI or TMSI	(P)TMSI
Permanent Virtual Circuit	PVC
Quality of Service	QoS
Routing Area	RA
Radio Access Bearer	RAB
RANAP Adaptation Layer	RAL
Radio Access Network Application Part	RANAP
Radio Frequency	RF
Radio Link Control	RLC
Radio Network Controller	RNC
Iu U-Plane	RNL
Radio Resource Control	RRC
Radio Resource Management	RRM
RANAP Transport Adaptation	RTA
Real-Time Protocol	RTP

RANAP User Adaptation	RUA
Service Area Identifier	SAI
System Architecture 1	SA1
Signalling Connection Control Part	SCCP
Stream Control Transmission Protocol	SCTP
Security Gateway	SeGW
Serving GPRS Support Node	SGSN
Subscriber Identity Module	SIM
Service Mobile Location Center	SMLC
Short Message Services	SMS
Signaling System 7	SS7
Transmission Control Protocol	TCP
Temporary Mobile Subscriber Identity	TMSI
Traffic Selector	TS
User Equipment	UE
Unlicensed Mobile Access	UMA
Universal Mobile Telecommunications System	UMTS
Universal Subscriber Identity Module	USIM
Either SIM or USIM	(U)SIM
UMTS Terrestrial Radio Access Network	UTRAN
Visitor Location Register	VLR
Wireless Local Area Network	WLAN
Wireless Service Provider	WSP
World Zone 1	WZ1

B. Definitions

Allowed CSG List: A list of CSG cells, each of which is identified by a CSG identity, allowed for a particular subscriber.

Access Control: It is the mechanism of ensuring that access to particular HNB is based on the subscription policy of the subscriber as well as that of the HNB.

Closed Subscriber Group (CSG): A list of subscribers which have access to mobile network using a particular HNB (a.k.a HeNB or Femtocell).

CSG Cell: A cell (e.g. HNB) which allows mobile network access to CSG only. A CSG cell may broadcast a specific CSG identifier over the air interface.

CSG Identity: The identity of the CSG cell. A CSG identity may be shared by multiple CSG cells.

CSG UE: A UE which has support for CSG white-list and can autonomously detect and select CSG cells.

E.164: A public networking addressing standard

Femtocell Access Network: The Femtocell access network constitutes of the HNB and the HNB-GW (same as HNB access network)

Legacy UE: A UE which does not have support for CSG white-list (e.g. R99 or pre-release 8 UE).

Operator: Licensed wireless service provider

White-List: It is the allowed CSG list stored on the UE or in the subscriber database record (such as in the HLR or HSS).

CLAIMS

What is claimed is:

1. A method of handling a handover of an ongoing session of a user equipment (UE) in a communication system comprising (i) a first wireless communications system comprising a licensed wireless radio access network and a core network and (ii) a second wireless communications system comprising a plurality of short range access points for establishing service regions of the second wireless communications system using licensed wireless frequencies and a network controller for communicatively coupling the UE operating in the service regions to the core network, the method comprising:

receiving, at the network controller, a handover message from the core network, the handover message comprising a first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network;

allocating by the network controller a second connection identifier to identify a connection associated with the UE between the network controller and an access point of the second wireless communication system communicatively connected to the network controller, the second connection identifier different than the first connection identifier;

sending the handover message and the second connection identifier from the network controller to the access point;

receiving a reply message from the access point in response to the handover message, the reply message comprising the second connection identifier as the identifier for the connection associated with the UE between the network controller and the core network;

replacing, at the network controller, the second connection identifier in the reply message with the first connection identifier as the identifier for the connection associated with the UE between the network controller and the core network; and

sending the reply message from the network controller to the core network.

2. The method of claim 1, wherein each of the first and second connection identifiers identifies a node of the communication system that has assigned a value for the first and second identifiers respectively.

3. The method of claim 1, wherein the identifier for the connection associated with the UE between the network controller and the core network is an Iu signaling connection identifier of a Radio Access Network Application Part (RANAP) message.

4. The method of claim 1, wherein the second identifier is a UE context identifier information element (IE) that uniquely identifies the UE within a service region of the access point.

5. The method of claim 1, wherein the ongoing session is at least one of a circuit switched (CS) session and a packet switched (PS) session.

6. The method of claim 1, wherein each of the handover message and the reply message is a Radio Access Network Application Part (RANAP) message, wherein the network controller encapsulates the handover message in a RANAP User Adaptation (RUA) message when the network controller sends the handover message to the access point.

7. The method of claim 6, wherein the reply message is a RANAP message encapsulated in a RUA message by the access point when the reply message is sent by the access point to the network controller.

8. The method of claim 7, wherein each of said RUA messages comprises the second identifier.

9. The method of claim 6, wherein each of said RANAP messages comprises the first connection identifier.

10. The method of claim 1, wherein the handover message is a Radio Access Network Application Part (RANAP) Relocation Request message.

11. The method of claim 1, wherein the reply message is a Radio Access Network Application Part (RANAP) Relocation Request Ack message.

12. The method of claim 1, wherein each of (i) the connection associated with the UE between the network controller and the core network and (ii) the connection associated with the UE between the network controller and the access point is a signalling connection.

13. A computer readable medium of a network controller that operates in a communication system comprising (i) a first wireless communications system comprising a licensed wireless radio access network and a core network and (ii) a second wireless communications system comprising a plurality of short range access points for establishing service regions of the second wireless communications system using licensed wireless

frequencies and the network controller for communicatively coupling a user equipment (UE) operating in the service regions to the core network, the computer readable medium storing a computer program for execution by at least one processing unit, the computer program comprising:

a set of instructions for receiving a handover message from the core network, the handover message comprising a first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network;

a set of instructions for allocating a second connection identifier to identify a connection associated with the UE between the network controller and an access point of the second wireless communication system communicatively connected to the network controller, the second connection identifier different than the first connection identifier;

a set of instructions for sending the handover message and the second connection identifier to the access point;

a set of instructions for receiving a reply message from the access point in response to the handover message, the reply message comprising the second connection identifier as the identifier for the connection associated with the UE between the network controller and the core network;

a set of instructions for replacing the second connection identifier in the reply message with the first connection identifier as the identifier for the connection associated with the UE between the network controller and the core network; and

a set of instructions for sending the reply message to the core network.

14. A method of handling a handover of an ongoing session of a user equipment (UE) in a communication system comprising (i) a first wireless communications system comprising a licensed wireless radio access network and a core network and (ii) a second wireless communications system comprising a plurality of short range access points for establishing service regions of the second wireless communications system using licensed wireless frequencies and a network controller for communicatively coupling the UE operating in the service regions to the core network, the method comprising:

receiving a handover message at an access point of the plurality of access points from the network controller, the handover message comprising (i) a first connection identifier as an identifier for a first connection associated with the UE between the network controller and a

first node of the communication system and (ii) a second connection identifier allocated by the network controller, the second connection identifier to identify a second connection associated with the UE between the network controller and the access point, the second connection identifier different than the first connection identifier;

determining whether the first connection identifier identifies the first connection as a connection between the network controller and the core network;

when the first connection identifier identifies the first connection as a connection between the network controller and the core network, sending a reply message from the access point to the network controller, the reply message comprising the first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network; and

when the first connection identifier identifies the first connection as a connection between the network controller and a node of the communication system other than the core network, sending a reply message from the access point to the network controller, the reply message comprising the second connection identifier as an identifier for a connection associated with the UE between the network controller and the node of the communication system.

15. The method of claim 14, wherein the reply message is for being relayed by the network to the first node.

16. The method of claim 14, wherein each of the first and second identifiers identifies a node of the communication system that has assigned a value for the first and second identifiers respectively.

17. The method of claim 14, wherein each of the handover message and the reply message is a Radio Access Network Application Part (RANAP) message, wherein the access point encapsulates the reply message in a RANAP User Adaptation (RUA) message.

18. The method of claim 17, wherein the handover message is encapsulated in a RUA message by the network controller when the handover message is sent by the network controller to the access point.

19. The method of claim 18, wherein each of said RUA messages comprises the second identifier.

20. The method of claim 17, wherein each of the RANAP messages comprises the first connection identifier.

21. A computer readable medium of an access point of a plurality of short range access points that operate in a communication system comprising (i) a first wireless communications system comprising a licensed wireless radio access network and a core network and (ii) a second wireless communications system comprising the plurality of short range access points for establishing service regions of the second wireless communications system using licensed wireless frequencies and a network controller for communicatively coupling a user equipment (UE) operating in the service regions to the core network, the computer readable medium storing a computer program for execution by at least one processing unit, the computer program comprising:

a set of instructions for receiving a handover message from the network controller, the handover message comprising (i) a first connection identifier as an identifier for a first connection associated with the UE between the network controller and a first node of the communication system and (ii) a second connection identifier allocated by the network controller, the second connection identifier to identify a second connection associated with the UE between the network controller and the access point, the second connection identifier different than the first connection identifier;

a set of instructions for determining whether the first connection identifier identifies the first connection as a connection between the network controller and the core network;

a set of instructions for, when the first connection identifier identifies the first connection as a connection between the network controller and the core network, sending a reply message to the network controller, the reply message comprising the first connection identifier as an identifier for a connection associated with the UE between the network controller and the core network; and

a set of instructions for, when the first connection identifier identifies the first connection as a connection between the network controller and a node of the communication system other than the core network, sending a reply message to the network controller, the reply message comprising the second connection identifier as an identifier for a connection associated with the UE between the network controller and the node of the communication system.

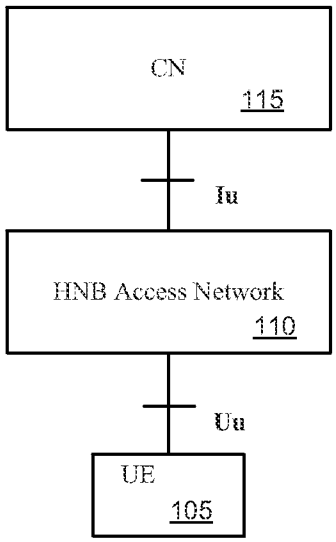

Figure 1

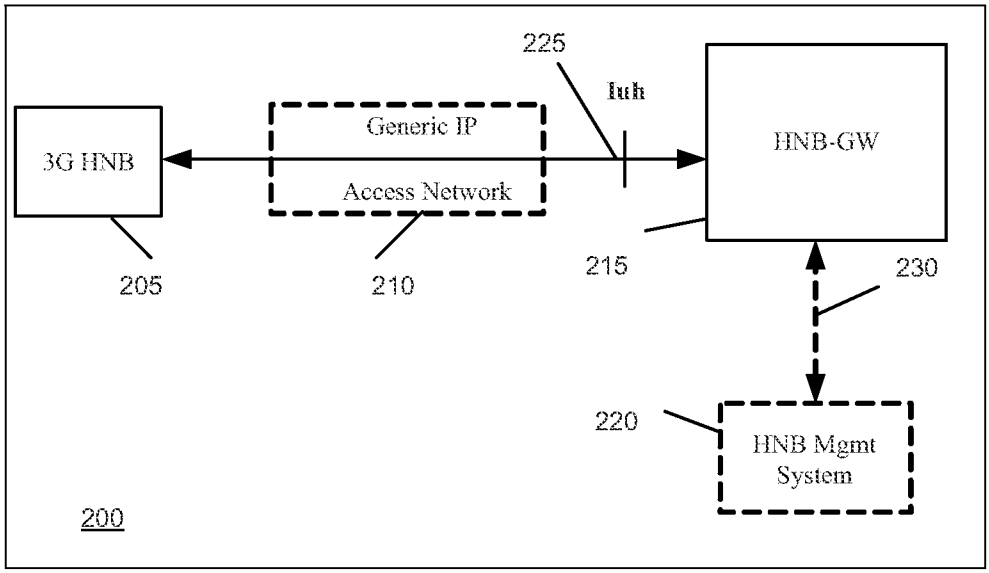

Figure 2

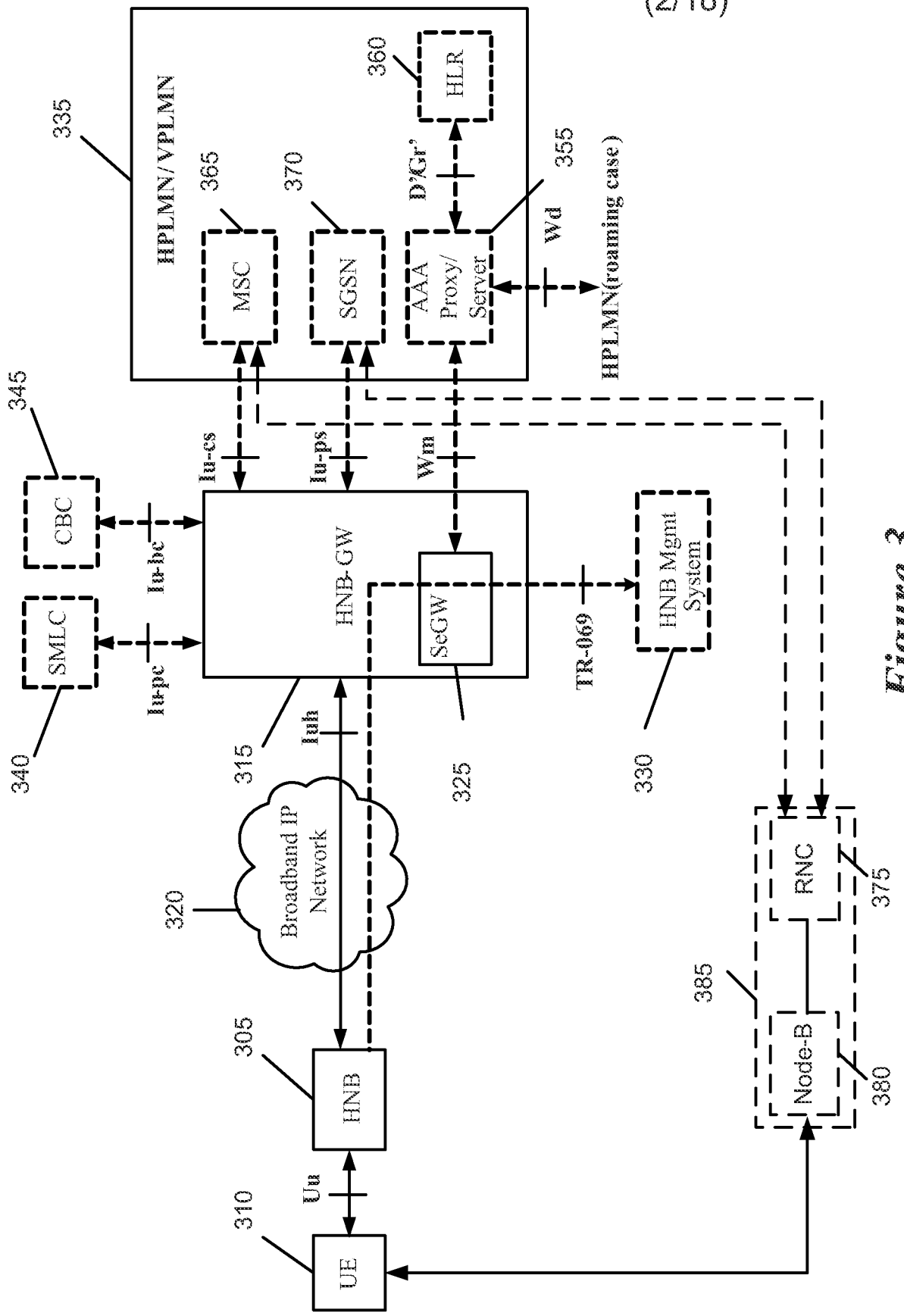
335
HPLMN/VPLMN
360
HLR
365
MSC
370
SGSN
D'/Gr'
355
AAA Proxy/ Server
Wd
HPLMN(roaming case)
345
CBC
Iu-cs
Iu-ps
Wm
Iu-bc
HNB-GW
SeGW
TR-069
HNB Mgmt System
SMLC
Iu-pc
340
315
Iuh
325
330
Broadband IP Network
320
RNC
375
385
Node-B
380
305
HNB
Uu
310
UE

Figure 3

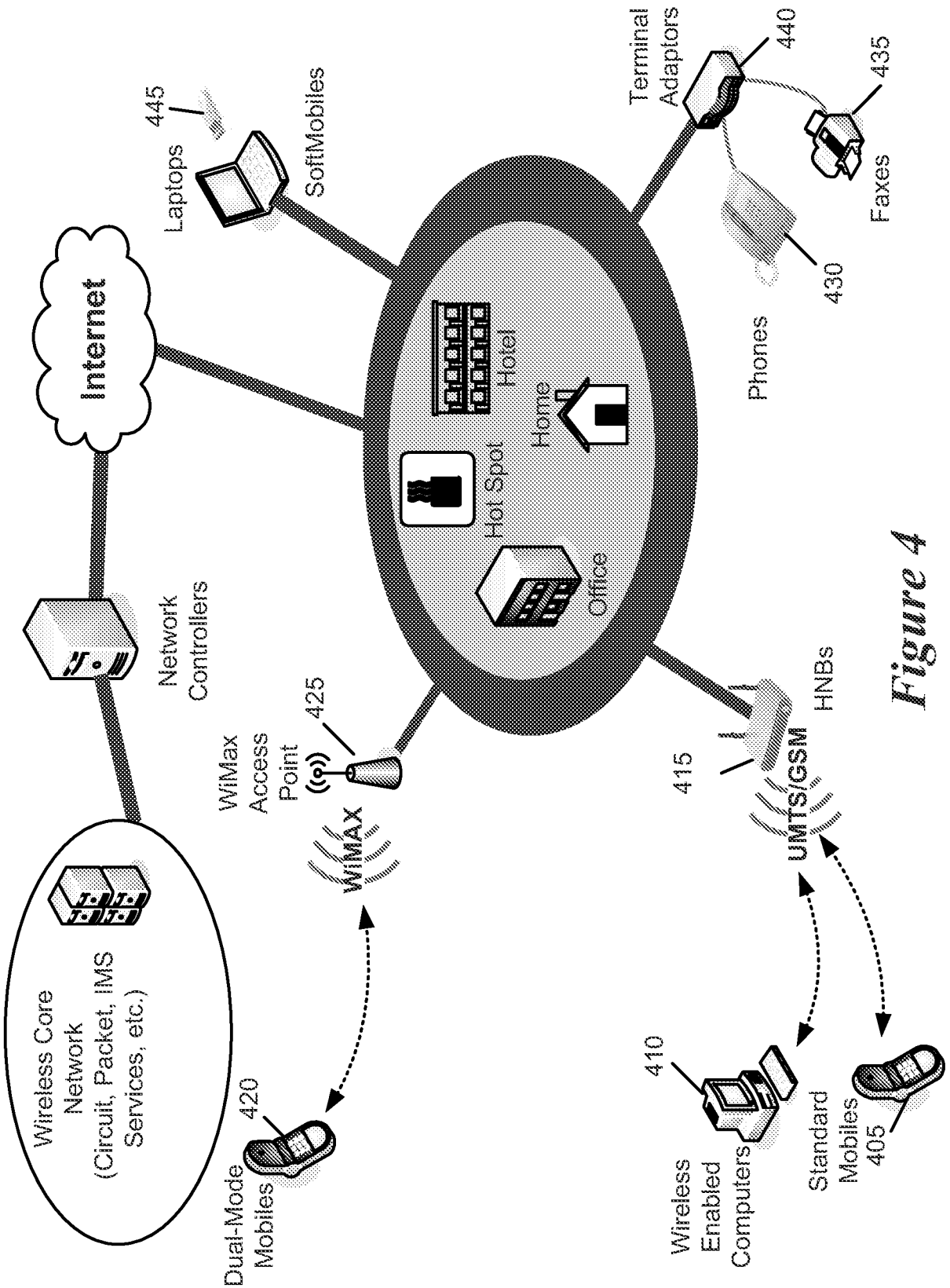
Wireless Core Network (Circuit, Packet, IMS Services, etc.)
Internet
Network Controllers
WiMax Access Point
425
WiMAX
Dual-Mode Mobiles
420
Laptops
445
SoftMobiles
Hotel
Home
Hot Spot
Office
Terminal Adaptors
440
Faxes
435
Phones
430
HNBs
415
UMTS/GSM
Wireless Enabled Computers
410
Standard Mobiles
405

Figure 4

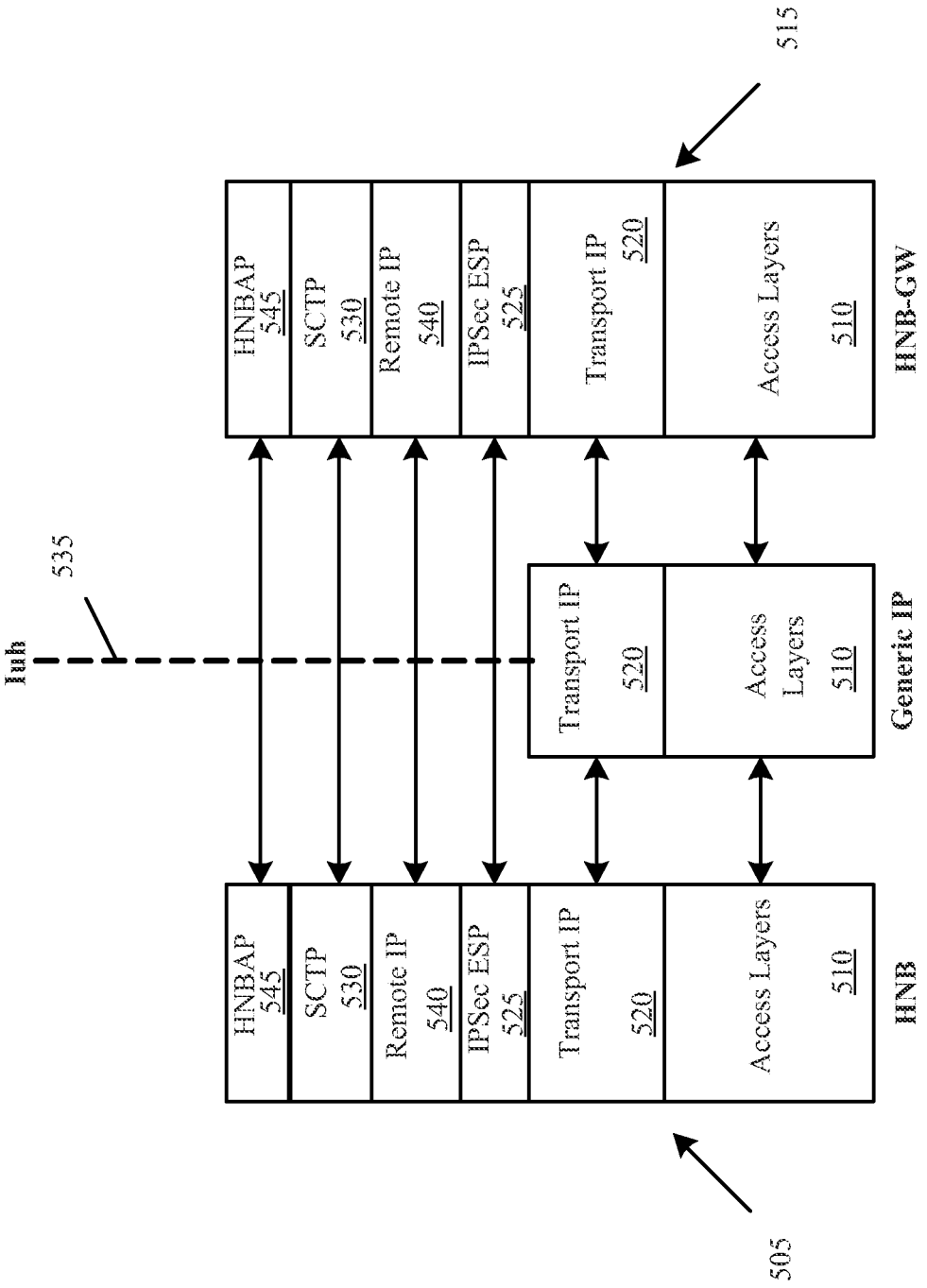
515
HNBAP 545
SCTP 530
Remote IP 540
IPSec ESP 525
Transport IP 520
Access Layers 510
HNB-GW
535
Iuh
Transport IP 520
Access Layers 510
Generic IP Network
HNBAP 545
SCTP 530
Remote IP 540
IPSec ESP 525
Transport IP 520
Access Layers 510
HNB
505

Figure 5

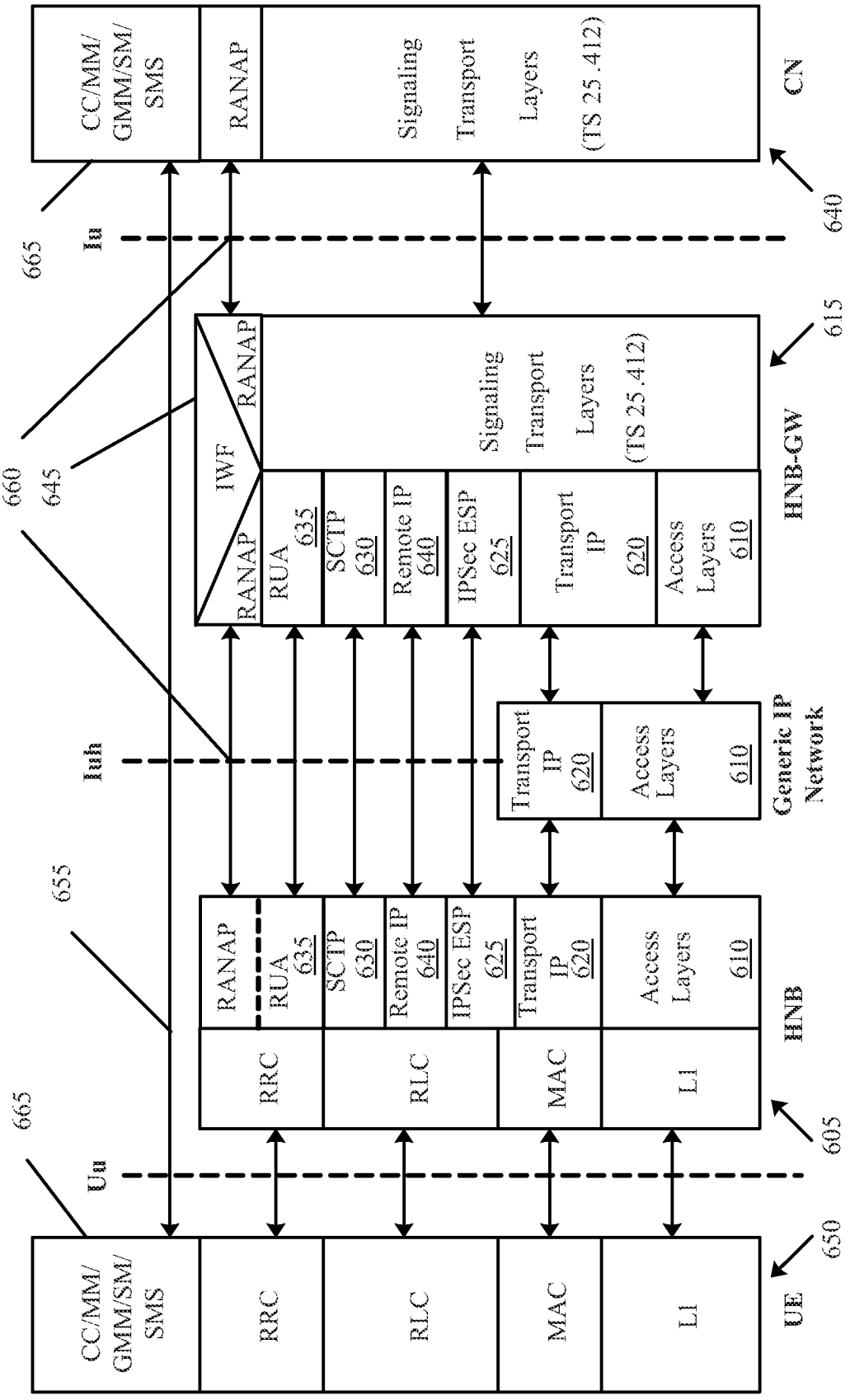
CC/MM/ GMM/SM/ SMS
RANAP
Signaling Transport Layers (TS 25.412)
CN
640
665
Iu
615
IWF
RANAP
RANAP
RUA 635
SCTP 630
Remote IP 640
IPSec ESP 625
Transport IP 620
Access Layers 610
HNB-GW
660
645
Iuh
Transport IP 620
Access Layers 610
Generic IP Network
655
RANAP
RUA 635
SCTP 630
Remote IP 640
IPSec ESP 625
Transport IP 620
Access Layers 610
RRC
RLC
MAC
L1
HNB
605
665
Uu
650
CC/MM/ GMM/SM/ SMS
RRC
RLC
MAC
L1
UE

Figure 6

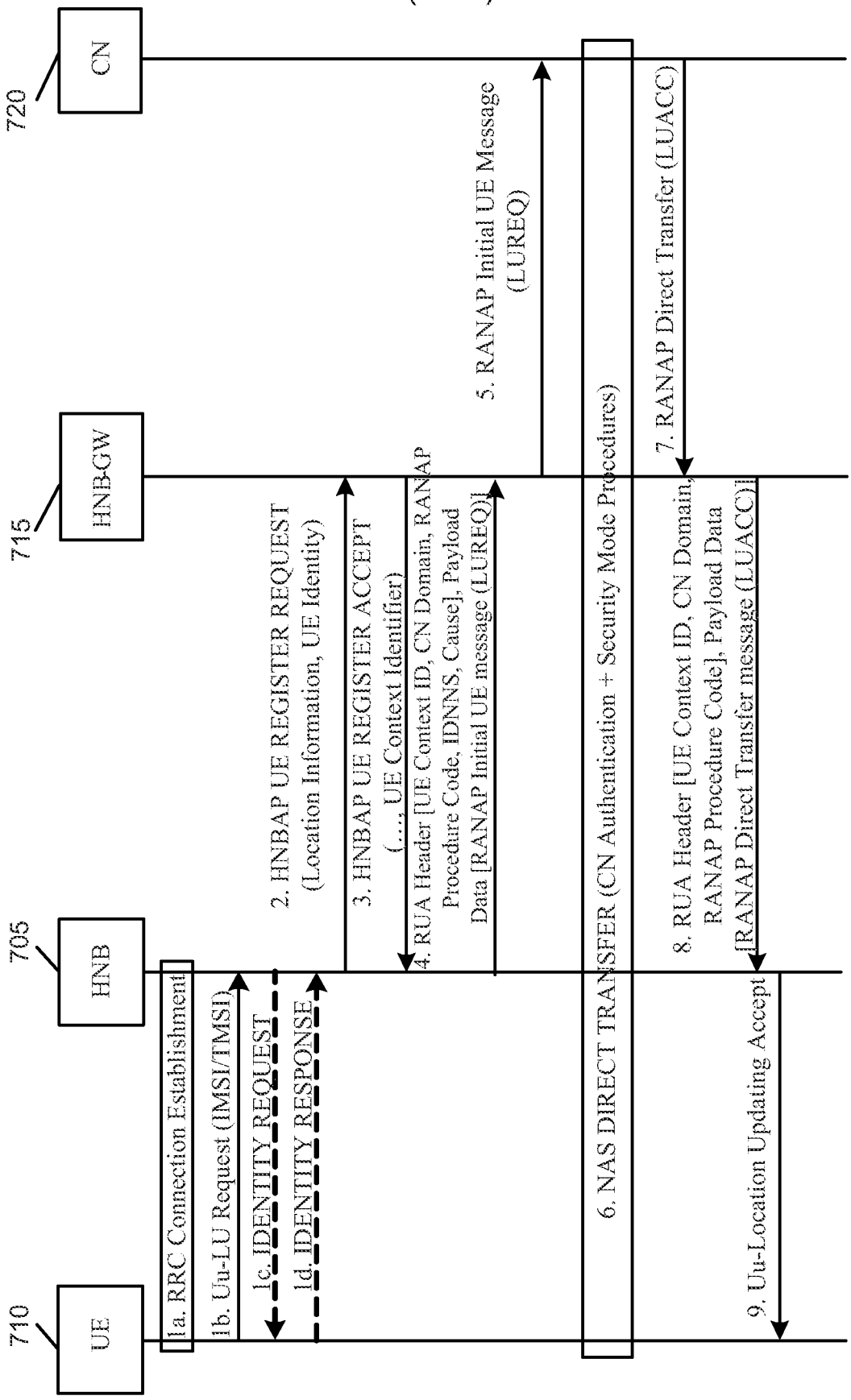
UE
710
HNB
705
HNB-GW
715
CN
720
1a. RRC Connection Establishment
1b. Uu-LU Request (IMSI/TMSI)
1c. IDENTITY REQUEST
1d. IDENTITY RESPONSE
2. HNBAP UE REGISTER REQUEST (Location Information, UE Identity)
3. HNBAP UE REGISTER ACCEPT (..., UE Context Identifier)
4. RUA Header [UE Context ID, CN Domain, RANAP Procedure Code, IDNNS, Cause], Payload Data [RANAP Initial UE message (LUREQ)]
5. RANAP Initial UE Message (LUREQ)
6. NAS DIRECT TRANSFER (CN Authentication + Security Mode Procedures)
7. RANAP Direct Transfer (LUACC)
8. RUA Header [UE Context ID, CN Domain, RANAP Procedure Code], Payload Data [RANAP Direct Transfer message (LUACC)]
9. Uu-Location Updating Accept

Figure 7

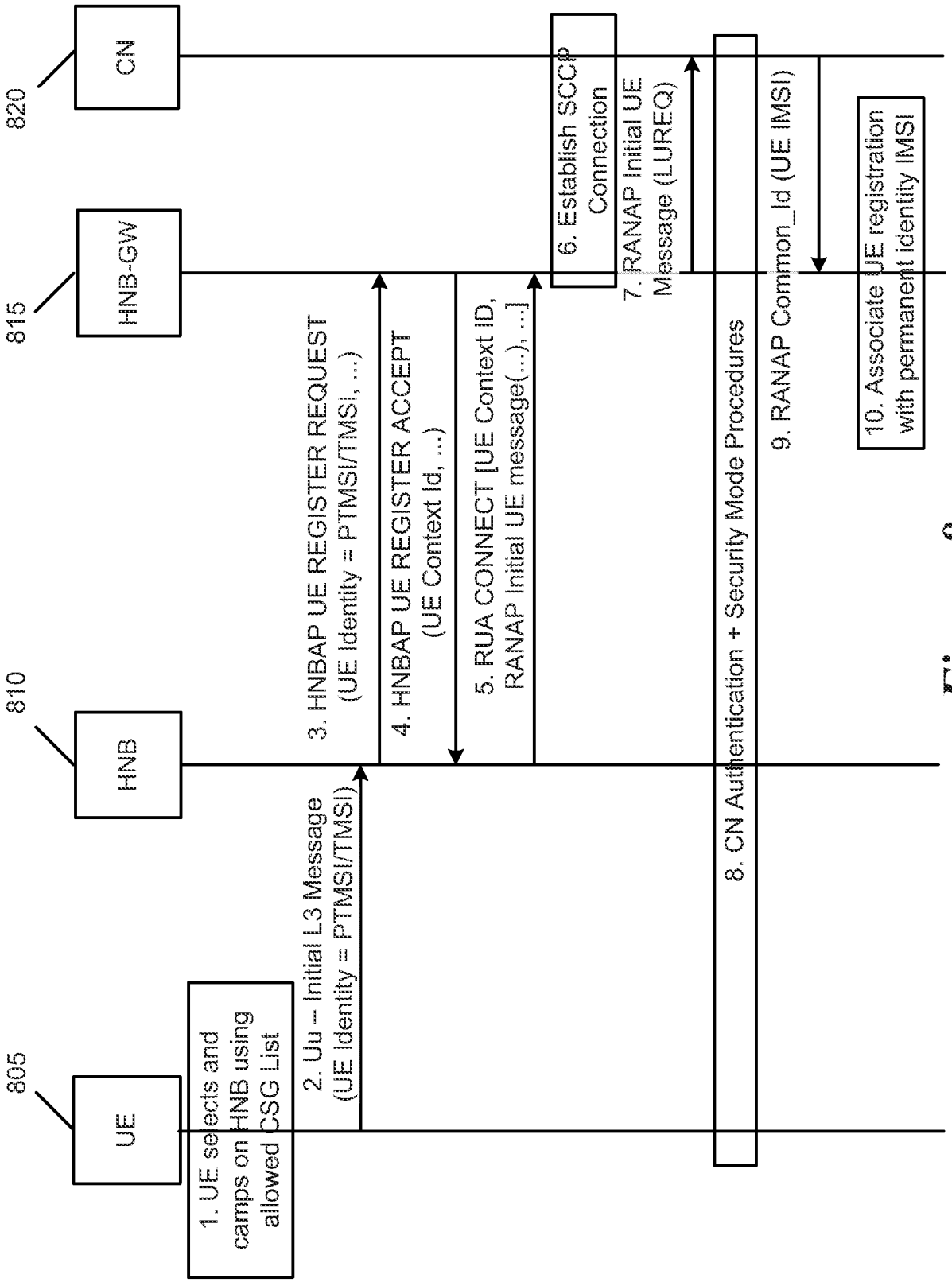
805
UE
810
HNB
815
HNB-GW
820
CN
1. UE selects and camps on HNB using allowed CSG List
2. Uu – Initial L3 Message (UE Identity = PTMSI/TMSI)
3. HNBAP UE REGISTER REQUEST (UE Identity = PTMSI/TMSI, ...)
4. HNBAP UE REGISTER ACCEPT (UE Context Id, ...)
5. RUA CONNECT [UE Context ID, RANAP Initial UE message(...), ...]
6. Establish SCCP Connection
7. RANAP Initial UE Message (LUREQ)
8. CN Authentication + Security Mode Procedures
9. RANAP Common_Id (UE IMSI)
10. Associate UE registration with permanent identity IMSI

Figure 8

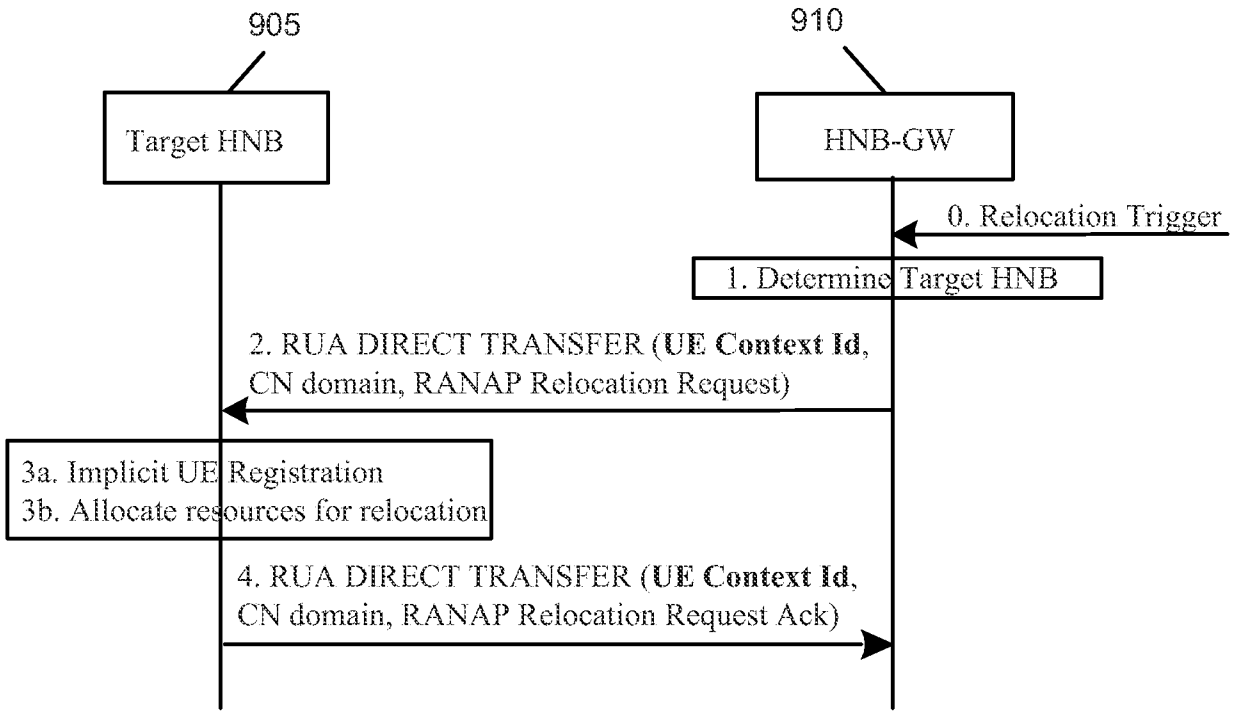
905
910
Target HNB
HNB-GW
0. Relocation Trigger
1. Determine Target HNB
2. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request)
3a. Implicit UE Registration
3b. Allocate resources for relocation
4. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request Ack)

Figure 9

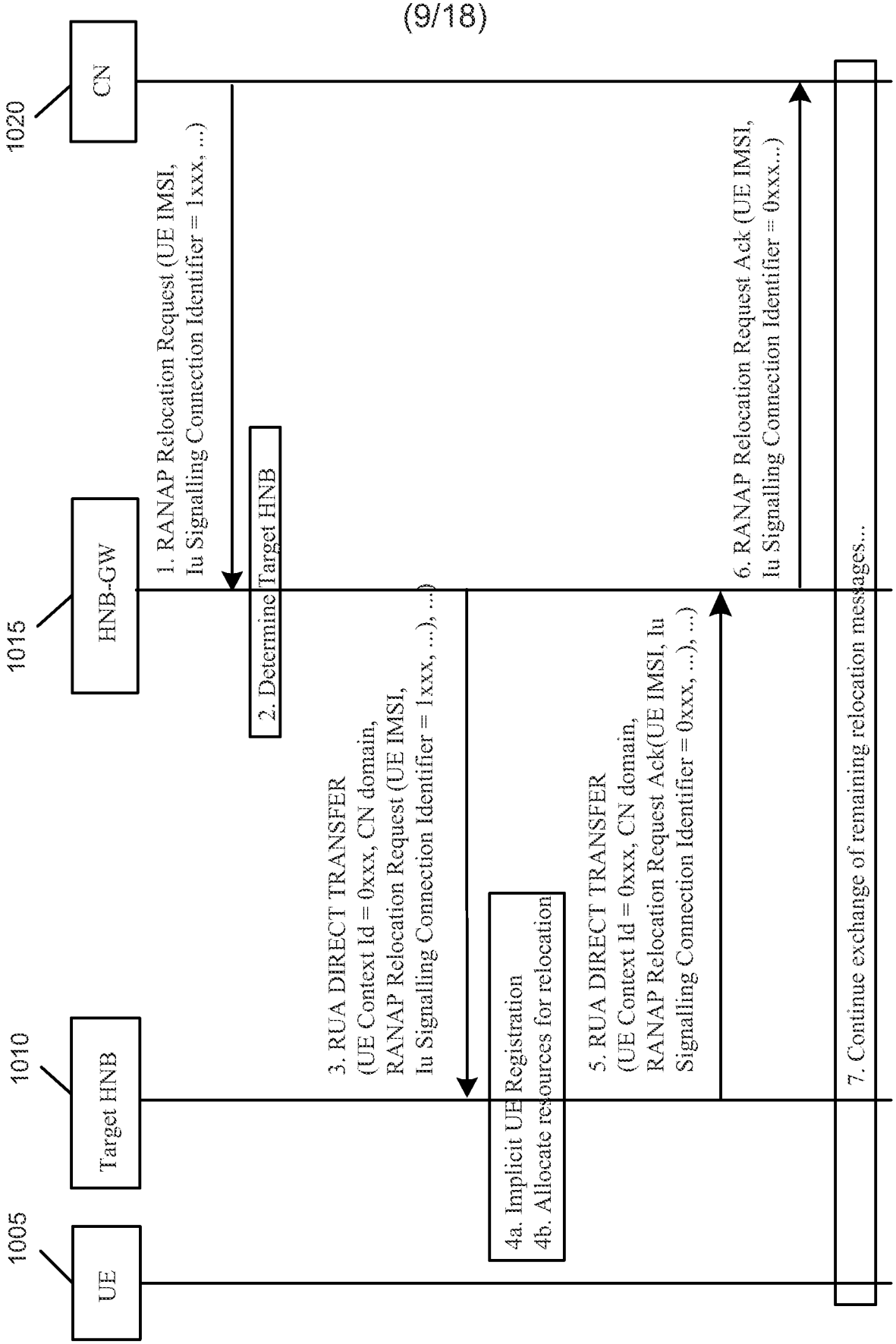
1005
UE
1010
Target HNB
1015
HNB-GW
1020
CN
1. RANAP Relocation Request (UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...)
2. Determine Target HNB
3. RUA DIRECT TRANSFER (UE Context Id = 0xxx, CN domain, RANAP Relocation Request (UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...), ...)
4a. Implicit UE Registration
4b. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id = 0xxx, CN domain, RANAP Relocation Request Ack(UE IMSI, Iu Signalling Connection Identifier = 0xxx, ...), ...)
6. RANAP Relocation Request Ack (UE IMSI, Iu Signalling Connection Identifier = 0xxx...)
7. Continue exchange of remaining relocation messages...

Figure 10

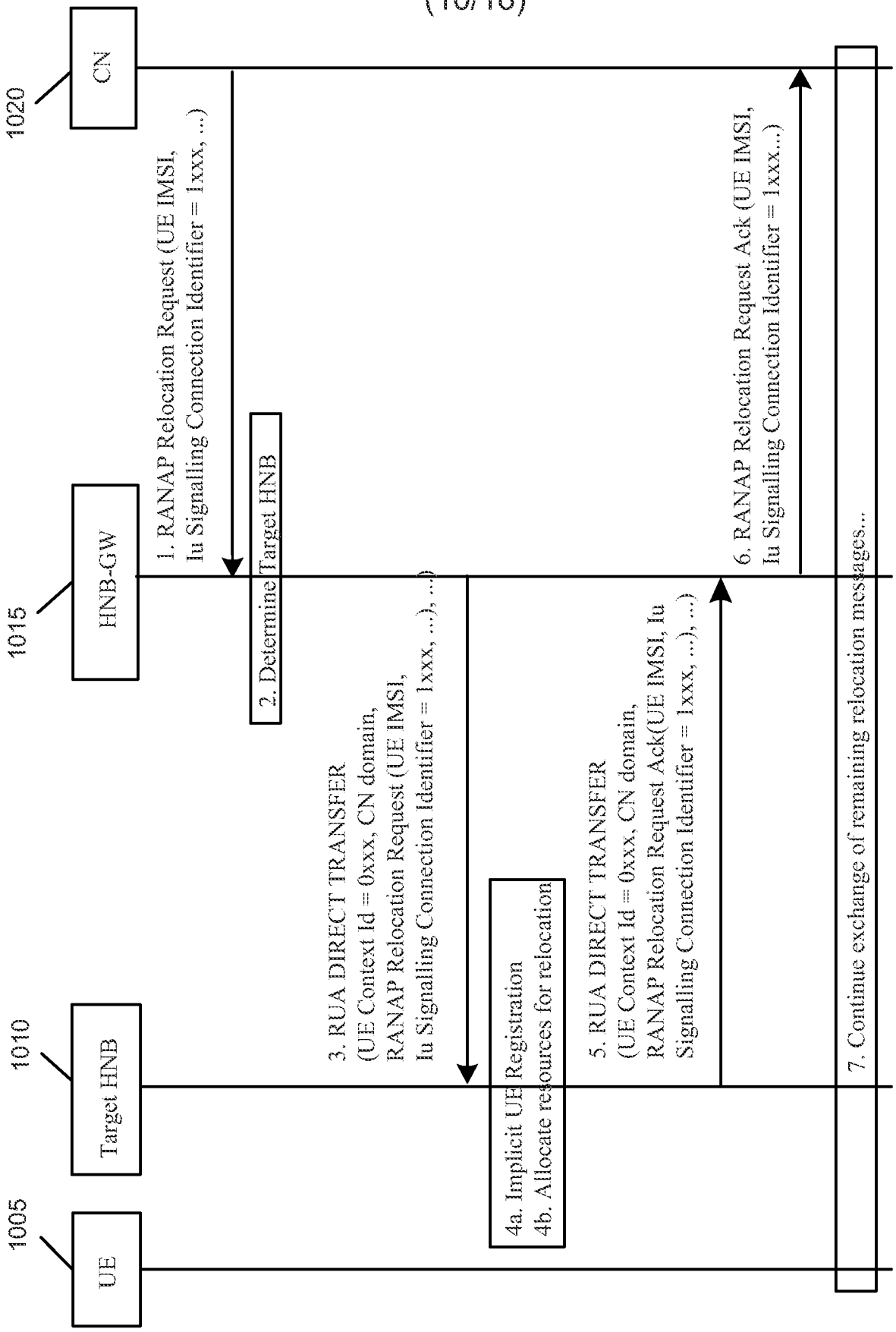
1005
UE
1010
Target HNB
1015
HNB-GW
1020
CN
1. RANAP Relocation Request (UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...)
2. Determine Target HNB
3. RUA DIRECT TRANSFER (UE Context Id = 0xxx, CN domain, RANAP Relocation Request (UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...), ...)
4a. Implicit UE Registration
4b. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id = 0xxx, CN domain, RANAP Relocation Request Ack(UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...), ...)
6. RANAP Relocation Request Ack (UE IMSI, Iu Signalling Connection Identifier = 1xxx...)
7. Continue exchange of remaining relocation messages...

Figure 11

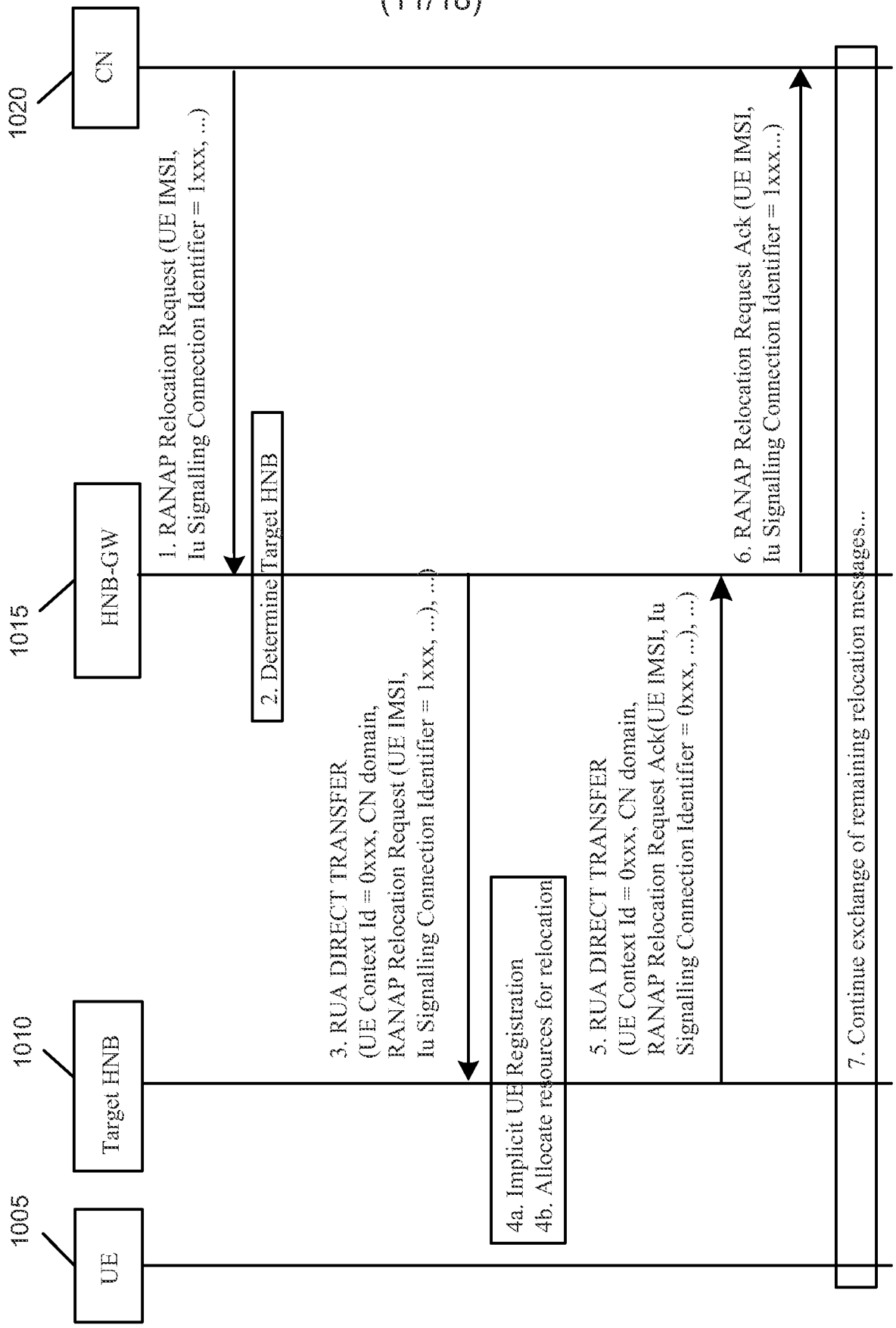
UE
1005
Target HNB
1010
HNB-GW
1015
CN
1020
1. RANAP Relocation Request (UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...)
2. Determine Target HNB
3. RUA DIRECT TRANSFER (UE Context Id = 0xxx, CN domain, RANAP Relocation Request (UE IMSI, Iu Signalling Connection Identifier = 1xxx, ...), ...)
4a. Implicit UE Registration
4b. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id = 0xxx, CN domain, RANAP Relocation Request Ack(UE IMSI, Iu Signalling Connection Identifier = 0xxx, ...), ...)
6. RANAP Relocation Request Ack (UE IMSI, Iu Signalling Connection Identifier = 1xxx...)
7. Continue exchange of remaining relocation messages...

Figure 12

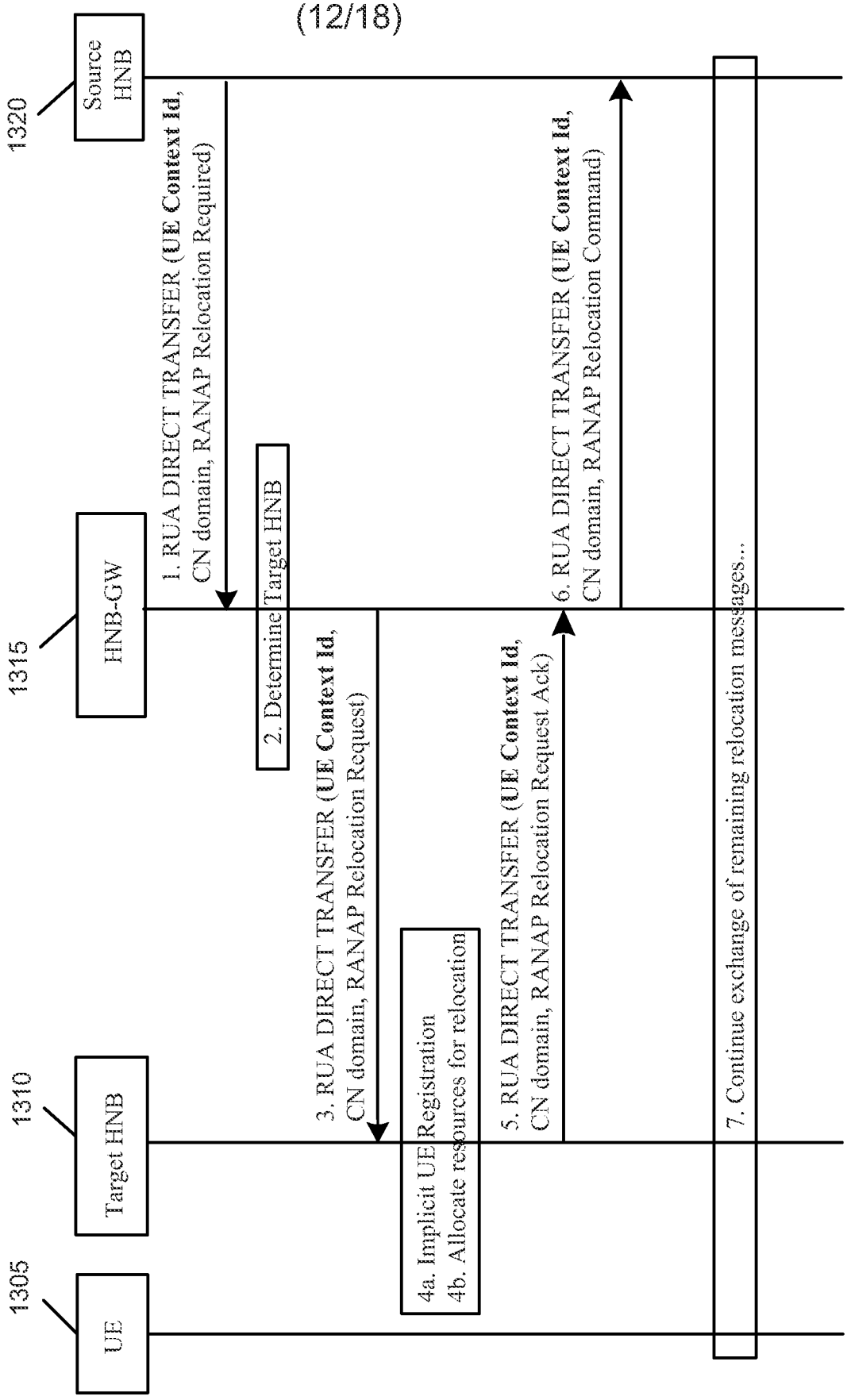
1320
Source HNB
1315
HNB-GW
1310
Target HNB
1305
UE
1. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Required)
2. Determine Target HNB
3. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request)
4a. Implicit UE Registration
4b. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request Ack)
6. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Command)
7. Continue exchange of remaining relocation messages...

Figure 13

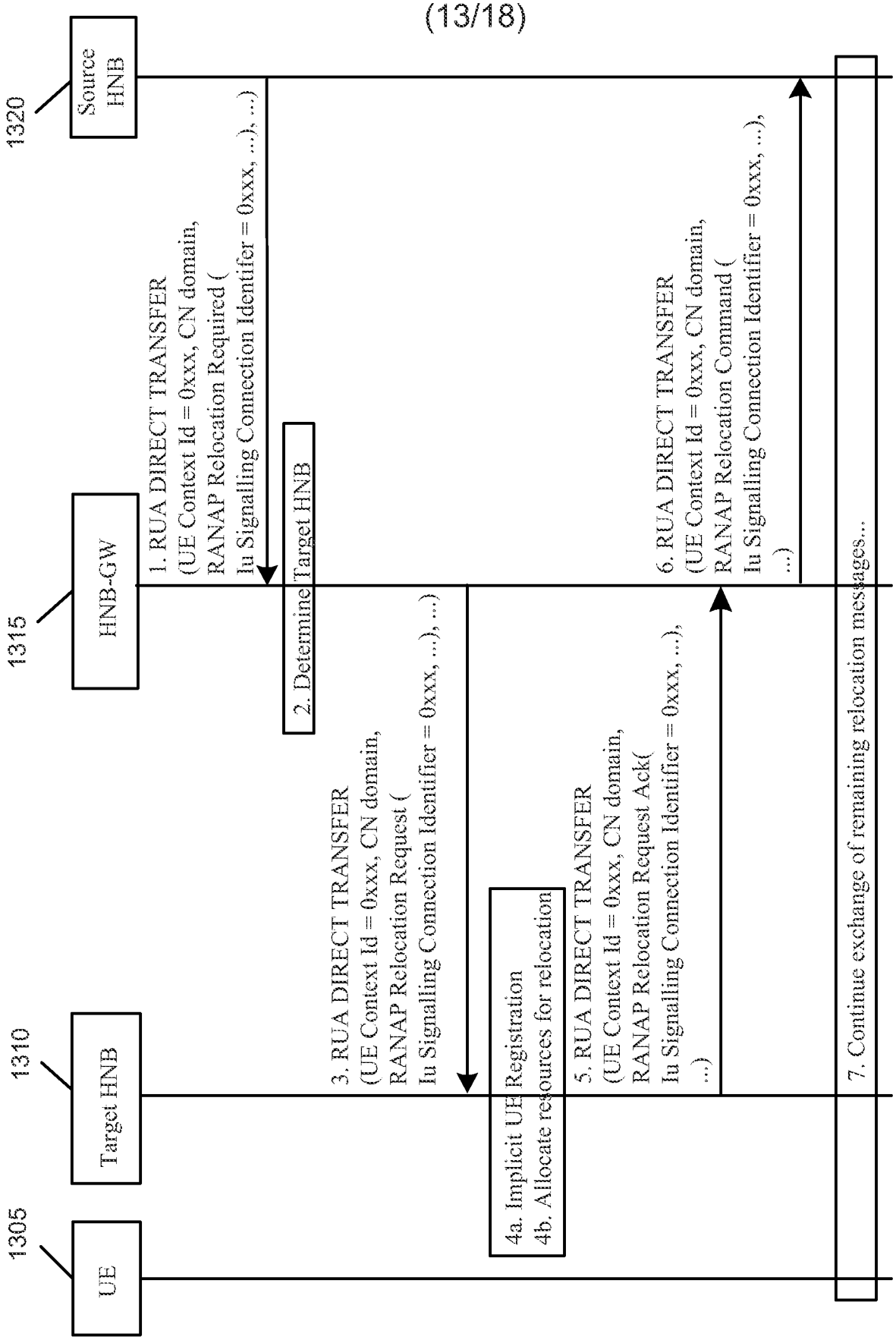
1305
UE
1310
Target HNB
1315
HNB-GW
1320
Source HNB
1. RUA DIRECT TRANSFER
(UE Context Id = 0xxx, CN domain,
RANAP Relocation Required (
Iu Signalling Connection Identifer = 0xxx, ...), ...)
2. Determine Target HNB
3. RUA DIRECT TRANSFER
(UE Context Id = 0xxx, CN domain,
RANAP Relocation Request (
Iu Signalling Connection Identifier = 0xxx, ...), ...)
4a. Implicit UE Registration
4b. Allocate resources for relocation
5. RUA DIRECT TRANSFER
(UE Context Id = 0xxx, CN domain,
RANAP Relocation Request Ack(
Iu Signalling Connection Identifier = 0xxx, ...),
...)
6. RUA DIRECT TRANSFER
(UE Context Id = 0xxx, CN domain,
RANAP Relocation Command (
Iu Signalling Connection Identifier = 0xxx, ...),
...)
7. Continue exchange of remaining relocation messages...

Figure 14

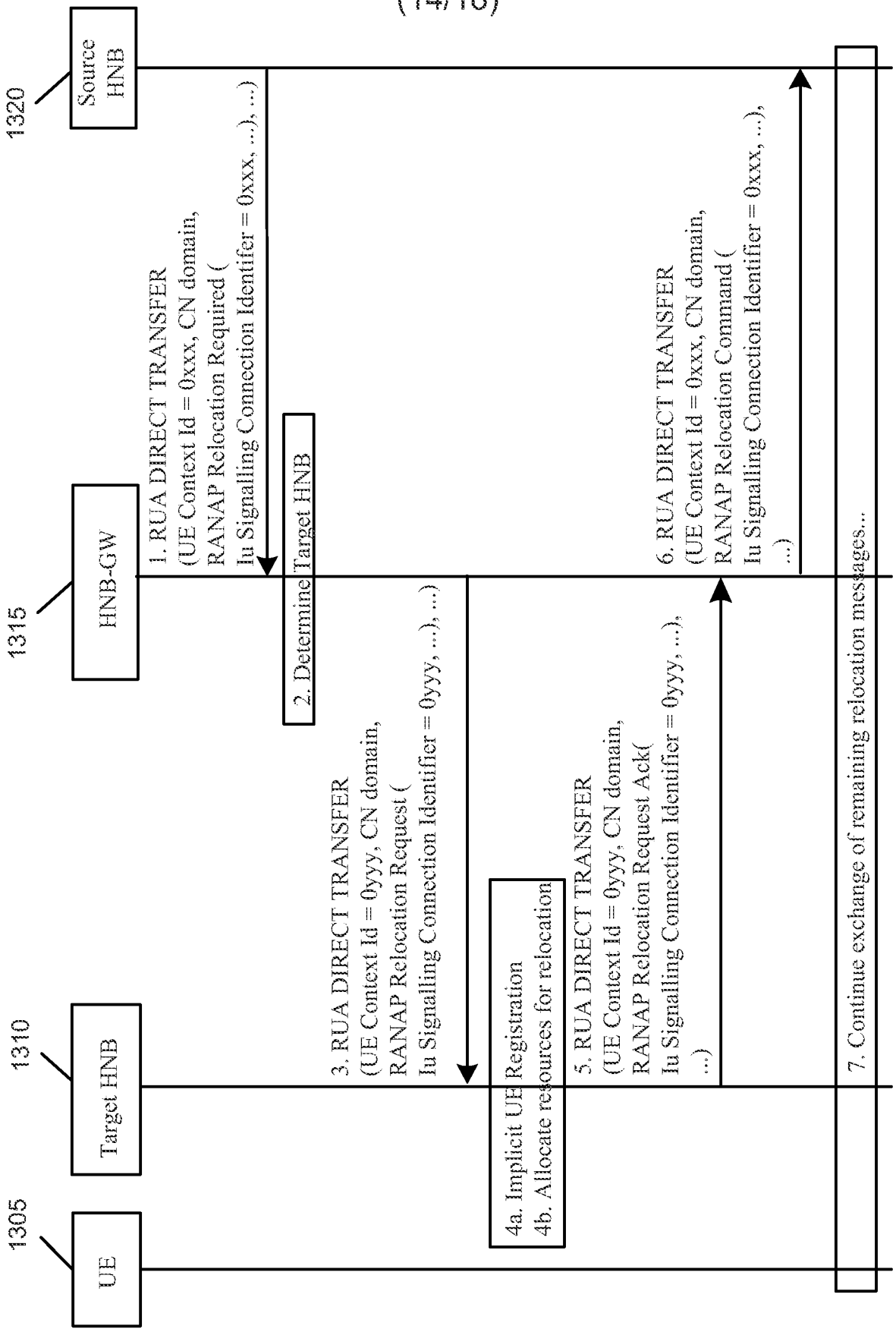
1305
UE
1310
Target HNB
1315
HNB-GW
1320
Source HNB
1. RUA DIRECT TRANSFER
(UE Context Id = 0xxx, CN domain,
RANAP Relocation Required (
Iu Signalling Connection Identifer = 0xxx, ...), ...)
2. Determine Target HNB
3. RUA DIRECT TRANSFER
(UE Context Id = 0yyy, CN domain,
RANAP Relocation Request (
Iu Signalling Connection Identifier = 0yyy, ...), ...)
4a. Implicit UE Registration
4b. Allocate resources for relocation
5. RUA DIRECT TRANSFER
(UE Context Id = 0yyy, CN domain,
RANAP Relocation Request Ack(
Iu Signalling Connection Identifier = 0yyy, ...),
...)
6. RUA DIRECT TRANSFER
(UE Context Id = 0xxx, CN domain,
RANAP Relocation Command (
Iu Signalling Connection Identifier = 0xxx, ...),
...)
7. Continue exchange of remaining relocation messages...

Figure 15

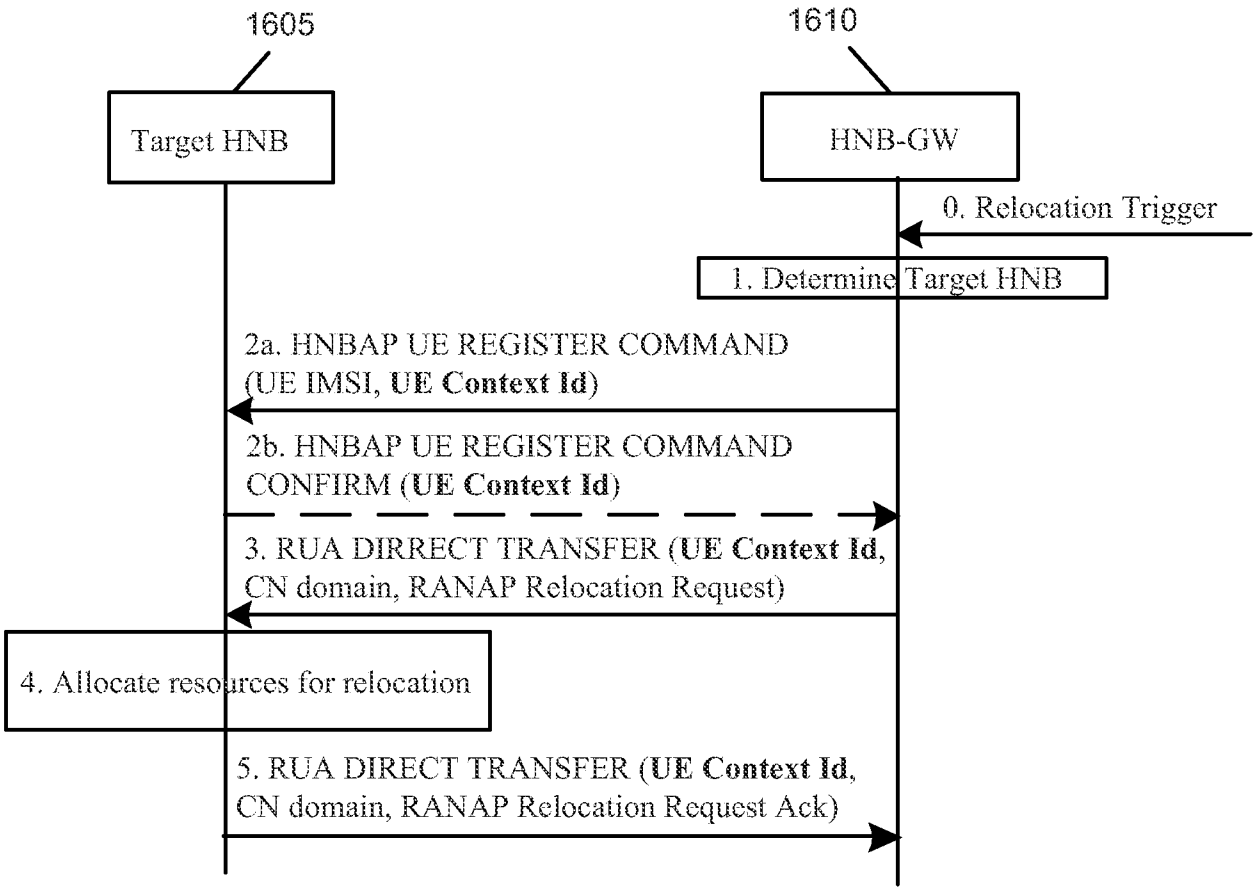
1605
1610
Target HNB
HNB-GW
0. Relocation Trigger
1. Determine Target HNB
2a. HNBAP UE REGISTER COMMAND
(UE IMSI, UE Context Id)
2b. HNBAP UE REGISTER COMMAND
CONFIRM (UE Context Id)
3. RUA DIRRECT TRANSFER (UE Context Id,
CN domain, RANAP Relocation Request)
4. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id,
CN domain, RANAP Relocation Request Ack)

Figure 16

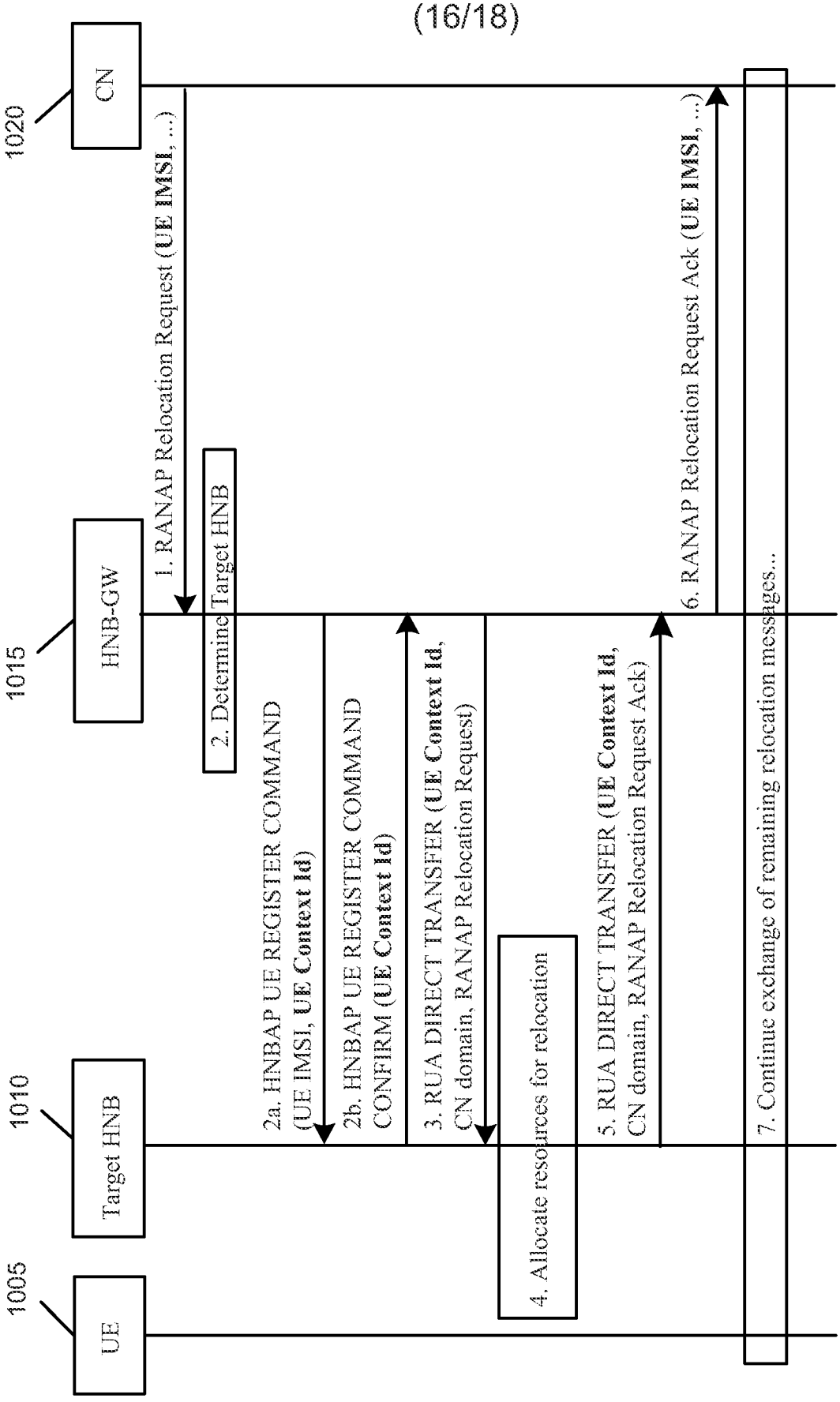
1005
UE
1010
Target HNB
1015
HNB-GW
1020
CN
1. RANAP Relocation Request (UE IMSI, ...)
2. Determine Target HNB
2a. HNBAP UE REGISTER COMMAND (UE IMSI, UE Context Id)
2b. HNBAP UE REGISTER COMMAND CONFIRM (UE Context Id)
3. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request)
4. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request Ack)
6. RANAP Relocation Request Ack (UE IMSI, ...)
7. Continue exchange of remaining relocation messages...

Figure 17

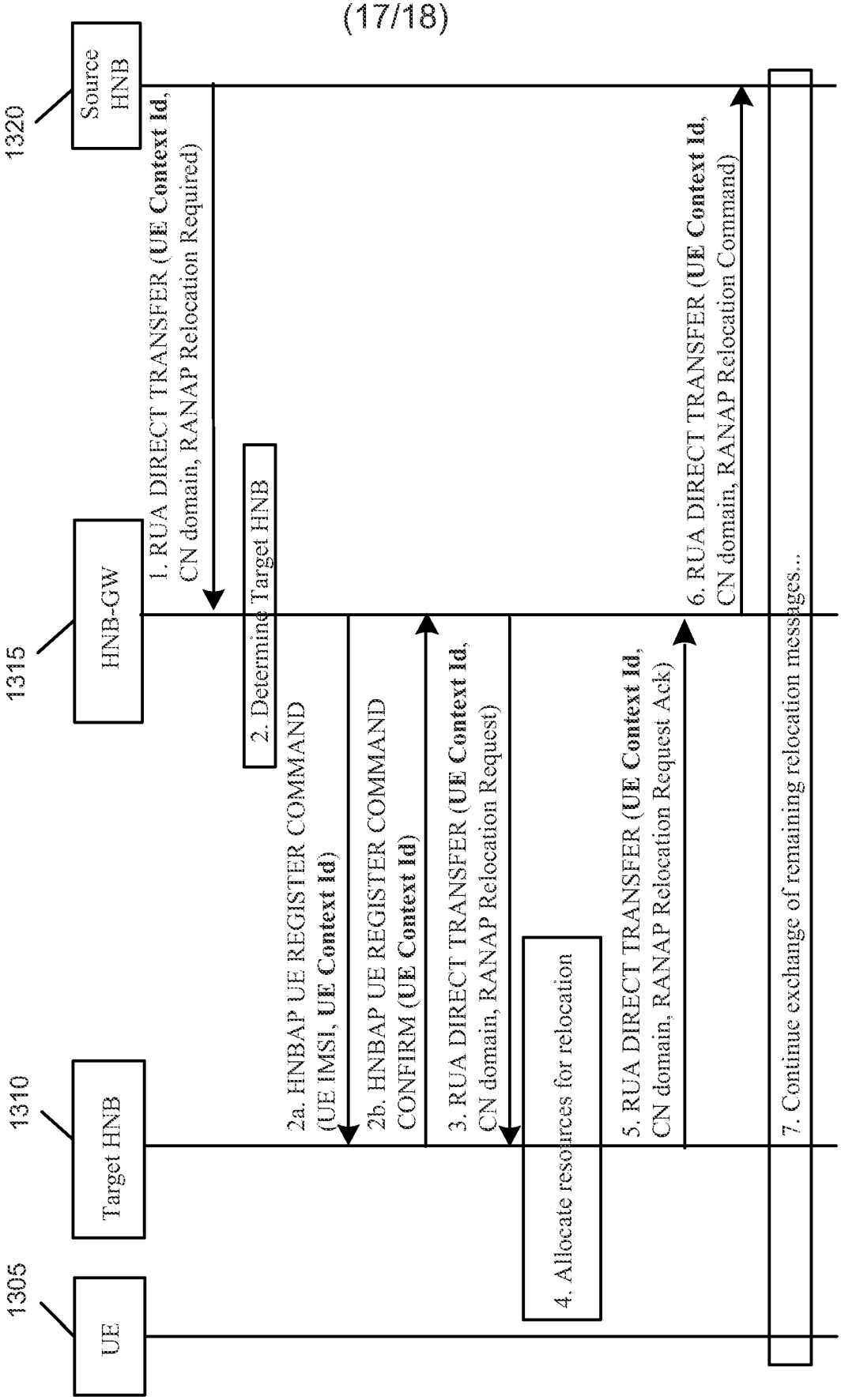
1305
UE
1310
Target HNB
1315
HNB-GW
1320
Source HNB
1. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Required)
2. Determine Target HNB
2a. HNBAP UE REGISTER COMMAND (UE IMSI, UE Context Id)
2b. HNBAP UE REGISTER COMMAND CONFIRM (UE Context Id)
3. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request)
4. Allocate resources for relocation
5. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Request Ack)
6. RUA DIRECT TRANSFER (UE Context Id, CN domain, RANAP Relocation Command)
7. Continue exchange of remaining relocation messages...

Figure 18

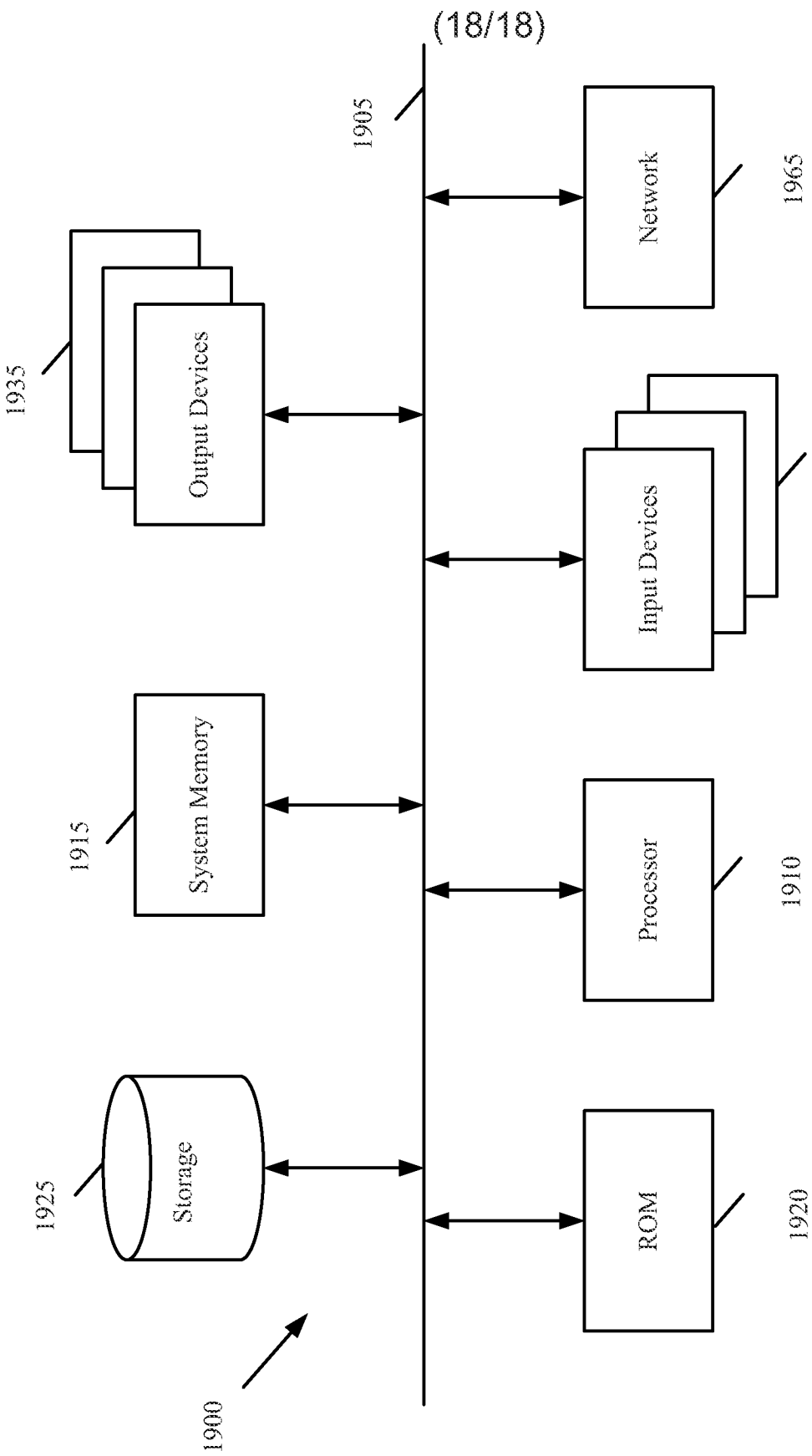
1900
1905
Network
1965
Output Devices
1935
Input Devices
1930
System Memory
1915
Processor
1910
Storage
1925
ROM
1920

Figure 19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/026883

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04W 36/00(2010.01)
USPC - 370/331
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)
IPC(8) - H04W 4/00; H04W 36/00; H04Q 7/20 (2010.01)
USPC - 370/331; 455/436, 438, 444

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)
MicroPatent, Google Scholar, Google Patents

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0101301 A1 (THOMAS et al.) 01 May 2008 (01.05.2008), entire document	1-5, 10-16 and 21
Y	US 2007/0183427 A1 (NYLANDER et al.) 09 August 2007 (09.08.2007), para. 0074-0077	1-5, 10-16 and 21
A	US 2008/0132239 A1 (KHETAWAT et al.) 05 June 2008 (05.06.2008), entire document	1-21
A	US 2008/0076420 A1 (KHETAWAT et al.) 27 March 2008 (27.03.2008), entire document	1-21
A	US 2008/0130564 A1 (GALLAGHER et al.) 05 June 2008 (05.06.2008), entire document	1-21

☐ Further documents are listed in the continuation of Box C. ☐

* 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
21 April 2010	04 MAY 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)