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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 January 2010 (28.01.2010)

PCT

(10) International Publication Number
WO 2010/010800 A2

(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/JP2009/062159

(22) International Filing Date:
26 June 2009 (26.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2008-192343 25 July 2008 (25.07.2008) JP

(71) Applicant *(for all designated States except US)*: **NEC CORPORATION** [JP/JP]; 7-1, Shiba 5-chome, Minato-ku, Tokyo 108-8001 (JP).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PRASAD, Raghawa** [NL/JP]; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo 108-8001 (JP).

(74) Agents: **TANAI, Sumio** et al.; 1-9-2, Marunouchi, Chiyoda-ku, Tokyo 100-6620 (JP).

(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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

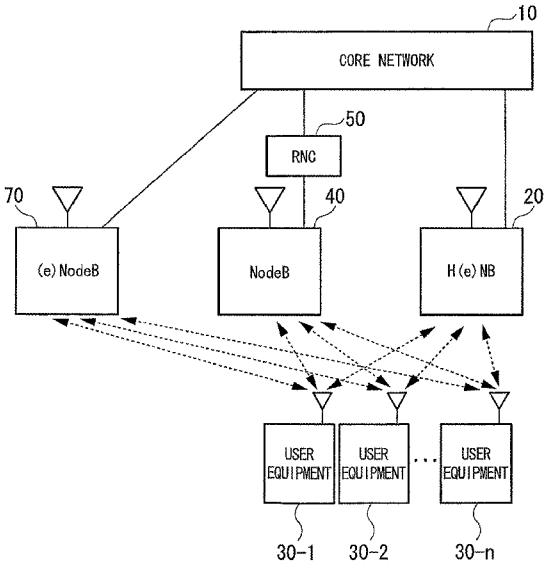
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: METHOD FOR CONNECTING USER EQUIPMENT AND H(E)NB, METHOD FOR AUTHENTICATING USER EQUIPMENT, MOBILE TELECOMMUNICATION SYSTEM, H (E)NB, AND CORE NETWORK

FIG. 2



(57) **Abstract**: In a mobile telecommunication system having a core network, user equipment, and H(e)NB and NodeB that are connected to the core network and communicate therewith, and that also perform radio communication with the user equipment, after the H(e)NB has been connected to the core network, a subscriber identity of the user equipment requesting a connection for the first time is set as an owner identity, and the owner identity is stored in the core network in association with a H(e)NB of the H(e)NB. The user equipment corresponding to the owner identity stores in the core network an access control list which contains the subscriber identity of the user equipment whose connection to the H(e)NB is allowed. The core network then performs authentication processing of the connection request from the user equipment to connect to the H(e)NB based on the access control list.

WO 2010/010800 A2

DESCRIPTION

METHOD FOR CONNECTING USER EQUIPMENT AND H(E)NB, METHOD FOR AUTHENTICATING USER EQUIPMENT, MOBILE TELECOMMUNICATION SYSTEM, H(E)NB, AND CORE NETWORK

TECHNICAL FIELD

[0001]

The present invention relates to a method for connecting user equipment to a telecommunication network via a radio base station and, in particular, relates to a connection method in which security is maintained.

Priority is claimed on Japanese Patent Application No. 2008-192343, filed July 25, 2008, the content of which is incorporated herein by reference.

BACKGROUND ART

[0002]

In recent years, in wired data communication, there have been remarkable technological developments. Networks that are based on IP (Internet Protocol) technology have become common, and communication at high speeds and at low cost is now provided. However, in radio communication that uses user equipment (UE) for mobile telecommunication such as, for example, mobile telephones and portable information terminals, communication which is based on IP technology is not as commonly used as data communication via wires.

[0003]

However, in mobile telecommunication a technology exists that provides user

equipment with high-speed and low-cost communication by installing a small radio station that has a communication range of several meters to several tens of meters (i.e., a Femto Cell) in a home or in a SOHO (Small Office Home Office). Here, the small radio base station is a radio base station that provides a user equipment with mobile telecommunication, and is a type of radio base stations having a low power radio wave and having a communication range of several meters to several tens of meters. The small radio base station is a device having technology in which, by narrowing the communication range and reducing the number of user equipments that are connected thereto, a wide frequency band is allocated between the small radio base station and the connected user equipment, and high-speed, low-cost communication is provided.

Moreover, a small radio base station is connected by wires to a core network (CN), which is a wired network, via a fixed telephone line or the Internet in the same way as communication provided by, for example, a DSL (Digital Subscriber Line).

[0004]

Usage of this type of Femto cell which employs a small radio base station has advantages not only for subscribers, but also for businesses that provide mobile telecommunication. For example, conventionally, in order to create a wider communication range, it has been necessary to install a large number of radio base stations that are able to house a large number of user equipments. Since such a radio base station is expensive, there have been great financial burden on a provider who provides an expensive radio base station. On the other hand, a small radio base station is not expensive and therefore can be sold or leased to subscribers, reducing financial burden of providers. Further, a subscriber installs a small radio base station, and therefore can accurately install the small radio base station at a place where communication is required by subscribers.

[0005]

Moreover, such a small radio base station is proposed in the form of HNB (home Node B) and H(e)NB (Home evolved Node B) which provide communication to CSG (Closed Subscriber Groups) in 3GPP (3rd Generation Partnership Projects) (See Non-Patent Literature).

SUMMARY OF THE INVENTION

Technical Problem

[0006]

However, when a small radio base station that is installed by a subscriber is connected to a core network via a fixed telephone or the Internet or the like, since management of the small radio base station is not being performed by the provider providing the mobile telecommunication, a problem arises in that there is a possibility of illegal connection of a small radio base station, incorrect connection of a small radio base station, illegal connection of a user equipment to a small radio base station, and incorrect connection of a user equipment being made.

[0007]

Accordingly, it is an object of the present invention to provide a means that performs authentication processing when a small radio base station is being connected and when a user equipment is being connected to a wired telecommunication network in order to prevent illegal use and incorrect use, and to provide a means that makes settings and performs management of a small radio base station in which security is guaranteed.

Solution to Problem

[0008]

In order to solve the above described problems, the present invention is a method for connecting, using radio communication, a user equipment and a H(e)NB in a mobile telecommunication system having the user equipment, the H(e)NB, and a core network. The method includes: a step in which the H(e)NB transmits connection request information, which contains a subscriber identity that identifies the user equipment, to the core network; and a step in which the core network determines, based on the connection request information that has been received, whether or not to connect the user equipment to the H(e)NB by referring to an access control list that is stored in advance.

[0009]

Moreover, the present invention is a method for authenticating user equipment in communication system having a wired base station and a network. The method includes: creating a secure connection between said wireless base station and said network; allowing a communication between said user equipment connecting to said wireless base station and said network; and starting communication between said user equipment and said network through said wireless base station.

[0010]

Moreover, the present invention is a H(e)NB included in a mobile telecommunication system further having a user equipment and a core network. The H(e)NB transmits connection request information including a subscriber identity for identifying the user equipment to the core network.

[0011]

Moreover, the present invention is a core network included in a mobile telecommunication system having a user equipment and a H(e)NB. The core network determines whether or not to connect the user equipment to the H(e)NB based on

connection request information which contains a subscriber identity for identifying the user equipment and a H(e)NB identity allocated to the H(e)NB in advance, and which is received from the H(e)NB while referring to an access control list stored therein in advance.

[0012]

Moreover, the present invention is a mobile telecommunication system including: a user equipment, a H(e)NB, and core network. The user equipment includes: a subscriber identity database containing a subscriber identity for identifying a host terminal; a terminal control unit generating and outputting terminal connection request information which contains the subscriber identity, and which requests a connection to the H(e)NB; and a terminal communication unit transmitting the terminal connection request information received from the terminal control unit to the H(e)NB to which a connection is requested. The H(e)NB includes: a base station communication unit receiving the terminal connection request information from the user equipment; an identity database containing a H(e)NB identity allocated in advance; and a base station control unit generating and transmitting connection request information which contains the subscriber identity and the H(e)NB identity contained in the terminal connection request information, and which indicates a request for a connection from the user equipment corresponding to the subscriber identity, to the core network. The core network includes: an access control list database containing information in which the subscriber identity of the user equipment whose connection to the H(e)NB is allowed is associated with the H(e)NB identity of the H(e)NB; and an authentication control unit determining whether or not to connect the user equipment corresponding to the subscriber identity contained in the connection request information received from the H(e)NB to the H(e)NB corresponding to the H(e)NB identity based on information stored

in the access control list database.

Advantageous Effects of the Invention

[0013]

According to this invention, in mobile telecommunications performed via a radio base station, by using an access control list in which user equipment for which connections have been allowed are registered for each radio base station, it is possible to ensure the security that is needed to prevent illegal and incorrect use.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014]

FIG. 1 is a schematic view showing the outline of the present invention.

FIG. 2 is a schematic view showing the structure of a mobile telecommunication system in a first embodiment.

FIG. 3 is a schematic view showing the structure of a core network, a H(e)NB, and a user equipment terminal in the first embodiment.

FIG. 4 is authentication information which is stored by an Authentication Center Database in the first embodiment.

FIG. 5 is an access control list which is stored by an Access Control List database in the first embodiment.

FIG. 6 is a sequence diagram showing registration processing to the core network of a H(e)NB in the first embodiment.

FIG. 7 is a sequence diagram showing connection processing for a user equipment terminal in the first embodiment.

FIG. 8 is a sequence diagram showing connection processing for a user

equipment terminal in the first embodiment.

FIG. 9 is a sequence diagram showing alteration processing for a membership list in the first embodiment.

FIG. 10 is a sequence diagram showing handover processing in the first embodiment.

FIG. 11 is a sequence diagram showing authentication processing which uses tokens in the first embodiment.

FIG. 12 is a schematic view showing the structure of a mobile telecommunication system in a second embodiment.

FIG. 13 is a sequence diagram showing an operation of the mobile telecommunication system in the second embodiment.

DESCRIPTION OF EMBODIMENTS

[0015]

The outline of the present invention is described below. FIG. 1 is a diagram showing the outline of the present invention.

(Secure Closed Subscriber Group Creation)

Registration: When the user signs-up for H(e)NB service, the operator records the following:

1. H(e)NB identity

2. Subscriber identity

[0016]

Solution as message sequence

1. When switched on and connected to the network, the H(e)NB performs authentication to the mobile operator's core network.

2. A secure connection is created between the core network and the H(e)NB.

3. The core network marks that this is the first connection by the H(e)NB.

4. A user connecting to the H(e)NB is allowed to communicate to the core network (this is only for the case where the ACL is in the network or if ACL is at H(e)NB then the owner is not yet set). This communication contains the H(e)NB identity added by the H(e)NB. The core network verifies whether the user is the owner.

5. If the user is the owner, then the network will inform the H(e)NB about it if the H(e)NB is supposed to maintain the ACL, or the network will allow further communication by the UE through the H(e)NB.

6. The UE can now either start communication or add members to the ACL. To add the CSG to the ACL, the owner starts software to add CSG members, or the owner starts a webpage to add CSG members.

7. On receiving the list, the network adds it in the ACL. If the ACL should be located at the H(e)NB, it is also recorded by the H(e)NB.

8. If a new device connecting to the H(e)NB and if ACL is located at the H(e)NB, it is checked by the H(e)NB. If a new device connecting to the H(e)NB and if the ACL is located at the network, it is checked by the network. Further access is allowed only if the network informs H(e)NB of the existence of the UE in the ACL.

[0017]

Hereinafter, the details of the present invention will be described.

A device according to embodiments of the present invention that guarantees security to prevent illegal use and incorrect use when a user equipment is being connected to a radio base station will be described with reference to the drawings. Note that, in these embodiments, the description uses a H(e)NB as an example of a radio base station.

Example 1

[0018]

FIG. 2 is a schematic block diagram showing a mobile telecommunication system 1 of the first embodiment. As is shown in the drawing, the mobile telecommunication system 1 includes: a core network (CN) 10; a home evolved node B (H(e)NB) 20 (referred to hereinafter as a H(e)NB 20); user equipment terminals (UE) 30-1, 30-2, ..., 30-n; a radio base station (nodeB) 40 (referred to hereinafter as a NodeB 40); a radio network controller (RNC) 50; and a radio base station (evolved NodeB) 70 (referred to hereinafter as a (e)NodeB 70).

Note that the user equipments terminals 30-1, ..., 30-n all have the same structure, and, hereinafter, when any one of or all of the user equipment terminals 30-1, ..., 30-n are being represented, they are referred to simply as user equipment 30. In addition, the H(e)NB 20 is purchased or leased by a user from a business that provides mobile telecommunications, and managed by the user.

[0019]

The core network 10 is the foundational portion of a mobile telecommunication system that provides mobile telecommunications. In addition, in response to a request from the user equipment 30 for a connection to the H(e)NB 20, the core network 10 performs authentication processing to determine whether or not to authenticate the connection based on information relating to whether or not the connection to the H(e)NB 20 by the user equipment 30 is allowed.

The H(e)NB 20 performs communication over a public telephone line or via the Internet or the like with the core network 10, and relays to the user equipment 30 data which it has exchanged with the core network 10, and performs authentication processing

in response to requests made by the user equipment 30.

The user equipment 30 is connected to the H(e)NB 20 and thus allows speech conversations and data communication to be performed with other user equipment 30 and the like via the H(e)NB 20 and the core network 10 and the like. The user equipment 30 is, for example, a terminal such as a mobile telephone or a portable information terminal.

The NodeB 40 is connected via the radio network controller 50 using a dedicated line to the core network 10, and relays to the user equipment 30 data which it has exchanged with the core network 10, and performs handover requests.

The (e)NodeB 70 is connected to the core network 10, and relays to the user equipment 30 data which it has exchanged with the core network 10, and performs handover requests.

[0020]

FIG. 3 is a schematic block diagram showing the structure of the core network 10, the H(e)NB 20, and the user equipment 30. Hereinafter, the respective functional blocks will be described using FIGS. 3, 4, and 5.

[0021]

The core network 10 is provided with an authentication center (AuC) 101, an authentication center database (AuC DB) 102, an access control list database (ACL DB) 103, a security gateway (SeGW) 104, a communication network 105, and a subscriber database (Subscriber DB) 106. The core network 10 is controlled and administered by a business that provides mobile telecommunications.

Note that the authentication center 101, the authentication center database 102, the access control list database 103, and the subscriber database 106 may be constituted by a single server unit. Moreover, the authentication center 101, the authentication

center database 102, the access control list database 103, and the subscriber database 106 may also be constituted by different server units that are connected via the communication network 105.

[0022]

In the core network 10, the authentication center 101 reads information stored in the authentication center database 102 and the access control list database 103 in response to a request for a connection or the like from the H(e)NB 20 or the user equipment 30, and allowance to connect the user equipment 30 to the H(e)NB 20 is given based on this read information. The authentication center 101 also updates authentication information that is stored in the authentication center database 102, and the access control list that is stored in the access control list database 103.

[0023]

Authentication information is stored in the authentication center database 102. Here, the authentication information is managed using a relational database.

FIG. 4 is a schematic view showing the data structure and an example of data that is contained in the authentication information. As is shown in the drawing, the authentication information is, for example, two-dimensional table data made up of rows and columns, and has a column for each of the categories of H(e)NB identities (H(e)NB ID), Owner identities (Owner ID) that identify an owner (i.e., administrator) who administers the H(e)NB 20, and non-connection information (H(e)NB's first connection). A row of the authentication information exists for each H(e)NB 20. The H(e)NB identities are identities that uniquely identify the H(e)NB 20. Moreover, the H(e)NB identities include information that makes it possible to distinguish themselves from the NodeB 40 and the (e)NodeB 70 that provide mobile telecommunication to the user equipment 30. For example, when the H(e)NB identities are made up of a plurality of

bit strings, by making the leading bits information that makes a distinction possible, and including therein proprietary bit strings which are different from those of the NodeB 40 identities and (e)NodeB 70 identities, it becomes possible to distinguish the H(e)NB 20 from the NodeB 40 and the (e)NodeB 70.

Owner identities are subscriber identities that uniquely identify subscribers that perform management of H(e)NB 20 connections. The non-connection information is information indicating the history of H(e)NB 20 connections to the core network 10. If no connection has yet been made [non-connection] (No) is stored, while (No) is stored if a connection is made [already connected]. This information shows whether or not any action has been taken.

In addition, the respective H(e)NB identities of all of the H(e)NB 20 for which a connection to the core network 10 has been allowed are included in advance in the authentication information. Furthermore, in an initial state, all of the owner identities are in an unregistered state, and non-connection information is in a state of [non-connection] (Yes).

[0024]

An access control list is stored in the access control list database 103, and the access control list is managed using a relational database.

FIG. 5 is a schematic view showing the data structure and an example of data that is contained in the access control list. As is shown in the drawing, the access control list is, for example, two-dimensional table data made up of rows and columns, and has a column for each of the categories of Closed Subscriber Group Name (CSG Name), H(e)NB identities (H(e)NB's ID), Owner identities, and a membership list. A row of the access control list exists for each closed (undisclosed) subscriber group.

[0025]

The closed subscriber groups are groups of subscribers for who connections to the core network 10 via prescribed H(e)NB 20 has been approved. The term "Closed Subscriber Group Name" is a designation that uniquely identifies a closed subscriber group. H(e)NB identities are the H(e)NB identities of H(e)NB 20 belonging to a closed subscriber group. Owner identities are subscriber identities of subscribers that have closed subscriber group management rights, for example, rights to make additions or removals or the like of subscribers. The membership list is a list of subscriber identities that are able to connect to the H(e)NB 20 that correspond to the closed subscriber groups.

Note that when the closed subscriber groups to have only one H(e)NB 20, then it is possible to use the H(e)NB identity as the closed subscriber group name.

[0026]

The security gateway 104 is provided between the communication network 105 and the H(e)NB 20, and performs communication with the H(e)NB 20. When performing communication with the H(e)NB 20, the security gateway 104 also establishes individual connections of communication lines that use widely known secure channels with the H(e)NB 20, and prevents leakages and thefts of communication information. For example, the security gateway 104 employs the coding of communication information using IPsec (Security Architecture for Internet Protocol), public key infrastructure (PKI), and tunneling technology in which virtual direct lines are established between the H(e)NB 20 and the core network 10.

[0027]

The communication network 105 is connected to and provides communication lines for a plurality of security gateways 104.

Subscriber identities are stored in the subscriber database 106. User equipment 30 which has a subscriber identity that is stored in the subscriber database 106 can be

connected to the core network 10.

[0028]

The H(e)NB 20 is provided with an authentication module 201, an access list database 202, a base station control unit 203, a base station communication unit 204, and an antenna 205. The H(e)NB 20 is also connected to the core network 10 via a public telephone line or the Internet or the like, and has the function of providing communication between the core network 10 and user equipment 30 belonging to subscribers of a closed subscriber group.

[0029]

In the H(e)NB 20, H(e)NB identities that uniquely identify the H(e)NB 20 are stored in the authentication module 201. Note that the authentication module 201 may be fixed inside the H(e)NB 20 or may be formed by a removable IC card or the like. Moreover, the H(e)NB identities may be stored in advance in the authentication module 201, or the H(e)NB identities may be stored in the authentication module 201 as a result of an operation performed by a subscriber when the H(e)NB 20 is connected to the core network 10 to download the H(e)NB identities via the core network 10 from a business providing mobile telecommunications. The H(e)NB identities may also be written to and stored in the authentication module 201 by an operation of a business providing mobile telecommunications when the business sells or leases the H(e)NB 20.

[0030]

The stored closed subscriber group name, owner identity, and membership list that are assigned to the host H(e)NB identity from the access control list stored in the access control list database 103 are duplicated and stored in the access list database 202. Furthermore, tokens that are used in the authentication processing for connections between the H(e)NB 20 and the user equipment 30 are stored in the access list database

202.

[0031]

The base station control unit 203 performs communication with the core network 10, and also performs processing for connection requests and the like from the user equipment 30.

[0032]

The base station communication unit 204 has commonly known functions for performing radio communication via the antenna 205, or has functions for performing radio communication that is compatible with UTRAN (UMTS Terrestrial Radio Access Network) or E-UTRN (Evolved UTRAN) standards, and performs radio communication with the user equipment 30.

[0033]

The user equipment 30 is provided with a universal subscriber identity module (USIM) 301, a terminal communication unit 302, a terminal control unit 303, a terminal input/output unit 304, and an antenna 305.

[0034]

In the user equipment 30, subscriber identities that uniquely identify the user equipment 30 and information, for example the Closed Subscriber Group Name and the H(e)NB identity for the H(e)NB 20 for which the connection is allowed, that is used in authentication processing are stored in the universal subscriber identity module 301. Tokens that are used in authentication processing for connections between the H(e)NB 20 and the user equipment 30 are also stored in the universal subscriber identity module 301. Note that the universal subscriber identity module 301 may be fixed in the user equipment 30 or may be formed by a removable IC card or the like.

[0035]

The terminal communication unit 302 has commonly known functions for performing radio communication via the antenna 305, or has functions for performing radio communication that is compatible with UTRAN or E-UTRN standards, and performs radio communication with the H(e)NB 20.

[0036]

The terminal control unit 303 performs processing to connect to the H(e)NB 20, and processing to set closed subscriber groups.

[0037]

The terminal input/output unit 304 receives inputs through the operation of a subscriber and, consequently, provides an output to the terminal control unit 303. The terminal input/output unit 304 outputs information that has been input from the terminal control unit 303 thereby enabling subscribers to be authenticated. The input/output terminal 304 has, for example, a display screen on which text is displayed, and a plurality of input buttons for subscriber input.

[0038]

FIG. 6 is a sequence diagram showing registration processing for the H(e)NB 20 to the core network 10, H(e)NB initial connection processing, and closed subscriber group creation processing. Processing of the mobile telecommunication system 1 is described below using this drawing.

[0039]

(H(e)NB registration processing)

Firstly, when the H(e)NB 20 is connected to the core network 10 via a public telephone line or via the Internet, the base station control unit 203 reads the H(e)NB identities from the authentication module 201 and generates an initial connection request that includes the read H(e)NB identities and a secure channel setting request (step S101).

[0040]

The base station control unit 203 transmits the generated initial connection request to the security gateway 104 of the core network 10 (step S102).

[0041]

When the security gateway 104 receives the initial connection request from the H(e)NB 20, the security gateway 104 outputs the received initial connection request to the authentication center 101 via the communication network 105.

The authentication center 101 detects whether or not the H(e)NB identity that is contained in the initial connection request is stored in the authentication center database 102, and detects whether or not non-connection information that has been assigned to this H(e)NB identity is unconnected (YES). Furthermore, if the authentication center 101 reads that the H(e)NB identity is stored in the authentication center database 102 and the non-connection information is unconnected from the authentication center database 102, it writes "existing connection" (NO) in the non-connection information that is assigned to the relevant H(e)NB identity, and updates the authentication information. Note that if the input H(e)NB identity is not stored in the authentication center database 102, or if the non-connection information that is assigned to the input H(e)NB identity is an existing connection (NO), the authentication center 101 treats the initial connection request as an illegal request and ends the processing.

[0042]

Next, the authentication center 101 generates key information used in a secure channel, and outputs initial connection command information that includes a secure channel setting command, the H(e)NB identity, and the generated key information to the security gateway 104.

When the security gateway 104 receives the initial connection command

information from the authentication center 101, the security gateway 104 sets a secure channel between the security gateway 104 and the H(e)NB 20 indicated by the H(e)NB identity that is contained in the initial connection command information. Subsequently, the security gateway 104 performs communication with the relevant H(e)NB 20 via the secure channel set with the H(e)NB 20 using the key information contained in the initial connection command information (step S103).

[0043]

Next, the security gateway 104 transmits information indicating that processing of the initial connection request has been completed to the base station control unit 203 of the H(e)NB 20 (step S104).

[0044]

When the base station control unit 203 receives the information indicating that the processing of the initial connection request has been completed from the security gateway 104, the base station control unit 203 sets a secure channel between itself and the security gateway 104, and generates the key information used for communication via the secure channel (step S105).

Thereafter, using the generated key information, the base station control unit 203 performs communication with the core network 10 via the secure channel set between the base station control unit 203 and the security gateway 104.

[0045]

As has been described above, the H(e)NB 20 is registered in the core network 10, and generates settings for the secure channel and is connected. Identities of H(e)NB 20 for which connections have already been approved are stored in the authentication center database 102. In addition, based on whether or not the H(e)NB identity for the H(e)NB 20 for which a connection is being requested is stored in the authentication center

database 102, the authentication control unit 101 performs authentication processing to determine whether or not to recognize the relevant connection request. As a result, it is possible to prevent illegal connections and incorrect connections to the core network 10 by the H(e)NB 20.

Note that when the connection to the core network 10 has been completed, the H(e)NB 20 is placed in a state in which it is able to relay to the core network 10 only information that requires authentication processing from user equipment 30.

[0046]

(Initial connection processing of the H(e)NB 20)

After registration of the H(e)NB 20 has been completed, in the user equipment 30, a request to connect to the H(e)NB 20 is input manually into the terminal input/output unit 304 by a subscriber in order to perform communication with the core network 10. The terminal input/output unit 304 outputs the input request to the terminal control unit 303. The terminal control unit 303 generates terminal connection request information requesting a connection to the H(e)NB 20 (step S111).

Here, the terminal connection request information includes a subscriber identity that is read from the universal subscriber identity module 301 by the terminal control unit 303, and a request to connect to the core network 10.

[0047]

The terminal control unit 303 transmits the generated terminal connection request information to the H(e)NB 20 through the terminal communication unit 302 (step S112).

[0048]

When the base station communication unit 204 receives the terminal connection request information from the user equipment 30, the base station communication unit 204

outputs the received terminal connection request information to the base station control unit 203. When the terminal connection request information is input into the base station control unit 203, the base station control unit 203 generates connection request information indicating the connection request from the user equipment 30 (step S113).

Here, the connection request information includes the received terminal connection request information, and the H(e)NB identity read from the authentication module 201. Namely, the connection request information includes the request for the user equipment 30 to connect to the H(e)NB 20, the subscriber identity, and the H(e)NB identity.

[0049]

The base station control unit 203 transmits the generated connection request information to the core network 10 (step S114).

[0050]

When the security gateway 104 receives the connection request information from the H(e)NB 20, the security gateway 104 outputs the received connection request information to the authentication center 101 via the communication network 105. When the authentication center 101 receives the connection request information from the security gateway 104, the authentication center 101 performs authentication processing to determine whether or not to recognize the connection request based on whether or not the subscriber identity contained in the connection request information is stored in the subscriber database 106. In addition, when the authentication center 101 detects that the subscriber identity is stored in the subscriber database 106, and also that the owner identity which corresponds to the H(e)NB identity contained in the connection request information is in an unconnected state, the authentication center 101 writes the relevant subscriber identity in the authentication center database 102 as an owner identity. The

authentication center 101 also generates owner registration command information (step S115).

[0051]

Here, the owner registration, and information includes information indicating that the connection which corresponds to the connection request information is allowed, the subscriber identity of the user equipment 30 requesting the connection, and the H(e)NB identity of the H(e)NB 20 for which the connection has been requested.

Note that if the subscriber identity contained in the connection request information is not stored in the subscriber database 106, it is treated as an illegal connection request, and the processing of the initial connection of the H(e)NB 20 is ended.

[0052]

The authentication center 101 transmits the generated owner registration command information to the base station control unit 203 of the H(e)NB 20 via the security gateway 104 (step S116).

[0053]

When the base station control unit 203 receives the owner registration command information from the core network 10, the base station control unit 203 writes and stores the owner registration command information in the access list database 202 while assigning thereto the subscriber identity contained in the owner registration command information as an owner identity (step S117).

[0054]

The base station control unit 203 also transmits the owner registration command information via the base station communication unit 204 to the user equipment 30 corresponding to the subscriber identity contained in the received owner registration

command information (step S118).

[0055]

When the terminal communication unit 302 receives the owner registration command information from the H(e)NB 20, the terminal communication unit 302 notifies the subscriber making the output that the H(e)NB 20 corresponding to the H(e)NB identity contained in the owner registration command information has been registered as an owner in the terminal input/output unit 304. In addition, the terminal communication unit 302 generates information that urges the setting of a closed subscriber group which is a group of user equipment 30 that is able to connect to the H(e)NB 20 which has now become an owner, and also outputs this to the terminal input/output unit 304 and urges the subscriber to make an input. Here, this setting of the closed subscriber group refers to the setting of a closed subscriber group name, and of the subscriber identities of the subscribers who are members of this closed subscriber group, namely, to the setting of a membership list.

[0056]

When the closed subscriber group name and membership list is input manually by a subscriber via the terminal input/output unit 304, the terminal control unit 303 generates CSG setting request information (step S121).

Here, the CSG setting request information is information that includes the closed subscriber group name, the H(e)NB identity of the H(e)NB 20 which for which the setting is to be made, the subscriber identity that is stored in the universal subscriber identity module 301, the membership list, and the CSG setting request.

[0057]

The terminal control unit 303 transmits the generated CSG setting request information to the H(e)NB 20 via the terminal communication unit 302 (step S122).

[0058]

When the base station communication unit 204 receives the CSG setting request information from the user equipment 30, the base station communication unit 204 outputs the received CSG setting request information to the base station control unit 203. When the CSG setting request information is input into the base station control unit 203, the base station control unit 203 writes the closed subscriber group name, the H(e)NB identity, the owner identity, and the membership list that are contained in the input CSG setting request information in the access list database 202, thereby storing them therein (step S123).

[0059]

The base station control unit 203 transmits the input CSG setting request information to the security gateway 104 of the core network 10 (step S124).

[0060]

When the security gateway 104 receives the CSG setting request information, the security gateway 104 outputs the received CSG setting request information to the authentication center 101. When the CSG setting request information is input into the authentication center 101, the authentication center 101 assigns the closed subscriber group name, the H(e)NB identity, the owner identity, and the membership list that are contained in the input CSG setting request information and writes those items in the access control list database 102, thereby storing those items therein (step S125).

[0061]

As a result of the above described processing, the owner of the H(e)NB 20 is set. In addition, setting of the closed subscriber group offered by the H(e)NB 20 is also performed. In this manner, the owner of the H(e)NB 20 is set, and the subscriber identity of the owner who is able to set a closed subscriber group is registered. By

making it possible for only this particular owner to be able to set a closed subscriber group, only user equipment 30 whose owners are allowed to make connections are registered in the access control list.

Note that transmissions are made from the user equipment 30 to the core network 10 via the H(e)NB 20, however, it is also possible to prepare an interface such as a webpage or the like via the Internet or the like, and for a computer that a subscriber has manually connected to the Internet or the like to transmit the CSG setting request information to the core network 10.

[0062]

(User equipment 30 connection processing)

FIG. 7 is a sequence diagram showing processing for user equipment 30 to connect to the core network 10 via the H(e)NB 20.

[0063]

Firstly, in the user equipment 30, when a connection request is input manually by a subscriber into the core network 10 via the terminal input/output unit 304, the terminal control unit 303 generates terminal connection request information (step S201).

[0064]

Next, the user equipment 30 transmits the generated terminal connection request information to the H(e)NB 20 (step S202).

[0065]

When the base station control unit 203 receives the terminal connection request information from the user equipment 30 via the base station communication unit 204, the base station control unit 203 generates connection request information (step S203).

[0066]

The base station control unit 203 transmits the generated connection request

information to the core network 10 (step S204).

[0067]

The authentication center 101 receives the connection request information from the H(e)NB 20 via the security gateway 104. The authentication center 101 also performs authentication processing to determine whether or not to authenticate the connection request based on whether or not the H(e)NB identity and the subscriber identity that are contained in the connection request information are assigned to the access control list database 103 and are stored therein. The authentication center 101 performs the authentication processing by reading the membership list that corresponds to the H(e)NB identity contained in the connection request information, and detecting whether or not the subscriber identity that is contained in the connection request information is contained in the read membership list.

When the authentication center 101 detects that the H(e)NB identity and the subscriber identity that are contained in the connection request information have been assigned to the access control list database 103 and are stored therein, the authentication center 101 allows the connection request. If the authentication center 101 detects that the H(e)NB identity and the subscriber identity that are contained in the connection request information have not been assigned to the access control list database 103 and are not stored therein, the authentication center 101 denies the connection request. The authentication center 101 also generates connection response information that gives notification of the result of the connection request (step S205).

[0068]

Furthermore, the authentication center 101 transmits the generated connection response information to the H(e)NB 20 via the security gateway 104 (step S206).

[0069]

When the base control unit 203 receives the connection response information from the core network 10, the base control unit 203 transmits the received connection response information to the user equipment 30 that is indicated by the subscriber identity contained in the received connection response information, and gives notification of the result of the terminal connection request information of the user equipment 30 (step S207).

[0070]

By performing the above described authentication processing, the core network 10 is able to determine whether or not to authenticate the terminal connection request from the user equipment 30 to connect to the H(e)NB 20. If the terminal connection request is allowed, the H(e)NB 20 relays exchanged data between the user equipment 30 and the core network 10, and the user equipment 30 is connected to the core network 10 via the H(e)NB 20 and performs communication therewith.

Because only user equipment 30 that is registered in the access control list is allowed to connect to the H(e)NB 20, it is possible to prevent illegal access to the H(e)NB 20 and incorrect access to the H(e)NB 20.

[0071]

Note that it is also possible for the H(e)NB 20 to perform authentication processing using the membership list stored in the access list database 202 without transmitting the terminal connection request information to the core network 10. In this case, the base control unit 203 performs the authentication processing based on whether or not the subscriber identity contained in the received terminal connection request information is contained in the membership list stored in the access list database 202. At this time, the base control unit 203 allows the connection request if the subscriber identity that is contained in the received terminal connection request information is

contained in the membership list, and denies the connection request if the subscriber identity is not contained therein.

[0072]

Next, another processing which is different from the above described user equipment 30 connection processing will be described.

Here, the security gateway 104 sets a secure channel using IPsec between the security gateway 104 and the H(e)NB 20. The core network 10 includes a security association database, which is not shown in the drawings.

Security association information is stored in advance in the security association database. Here, the security association information is information that contains IP address information that is allocated to the H(e)NB 30, the algorithm used in the secure channel, and the key information used in the secure channel, and is associated with the H(e)NB identity. Note that the IP address information allocated by security gateway 104 when the secure channel is set is also stored in the authentication module 201.

[0073]

FIG. 8 is a sequence diagram showing processing by which the user equipment 30 is connected to the core network 10 via the H(e)NB 20.

Firstly, in the user equipment 30, when a connection request is input manually by a subscriber into the core network 10 via the terminal input/output unit 304, the terminal control unit 303 generates terminal connection request information (step S251).

Next, the user equipment 30 transmits the generated terminal connection request information to the H(e)NB 20 (step S252).

[0074]

When the base station control unit 203 receives the terminal connection request information from the user equipment 30 via the base station communication unit 204, the

base station control unit 203 generates connection request information (step S253).

Here, the connection request information contains the received terminal connection request information and the IP address information stored in the authentication module 201.

The base station control unit 203 transmits the generated connection request information to the core network 10 (step S254).

When the security gateway 104 receives the connection request information from the H(e)NB 20, the security gateway 104 reads out the H(e)NB identity associated with the key information for the secure channel from the security association database. The security gateway 104 outputs the received connection request information and the read H(e)NB identity to the authentication center 101 (step S255).

[0075]

When the authentication center 101 receives the connection request information and the H(e)NB identity from the security gateway 104, the authentication center 101 performs authentication processing to determine whether or not to authenticate connection request based on whether or not the H(e)NB identity and the subscriber identity that are contained in the connection request information are stored in the access control list database 103 and in a manner associated with each other. When the authentication center 101 detects that the H(e)NB identity and the subscriber identity that are contained in the connection request information have been assigned to the access control list database 103 and are stored therein, the authentication center 101 allows the connection request. If the authentication center 101 detects that the H(e)NB identity and the subscriber identity that are contained in the connection request information have not been stored in the access control list database 103 in a manner associated with each other, the authentication center 101 denies the connection request. The authentication

center 101 also generates connection response information that gives notification of the result of the connection request (step S256).

Furthermore, the authentication center 101 transmits the generated connection response information to the H(e)NB 20 via the security gateway 104 (step S257).

When the base control unit 203 receives the connection response information from the core network 10, the base control unit 203 transmits the received connection response information to the user equipment 30 that is indicated by the subscriber identity contained in the received connection response information, and gives notification of the result of the terminal connection request information of the user equipment 30 (step S258).

[0076]

By performing the above described authentication processing, the core network 10 is able to determine whether or not to authenticate the terminal connection request from the user equipment 30 to connect to the H(e)NB 20. If the terminal connection request is allowed, the H(e)NB 20 relays exchanged data between the user equipment 30 and the core network 10, and the user equipment 30 is connected to the core network 10 via the H(e)NB 20 and performs communication therewith.

Because only user equipment 30 that is registered in the access control list is allowed to connect to the H(e)NB 20, it is possible to prevent illegal access to the H(e)NB 20 and incorrect access to the H(e)NB 20. Furthermore, because the H(e)NB 20 and the core network 10 do not transmit the H(e)NB identities, it is possible to prevent leakages and thefts of the H(e)NB identities.

[0077]

Note that the security gateway 104 may read out the H(e)NB identity associated with the key information for secure channel from the security association database in step

S255 only when the security gateway 104 detects that a received packet is connection request information.

[0078]

(Membership list modification processing)

FIG. 9 is a sequence diagram showing processing to add a subscriber identity to a closed subscriber group membership list. Note that in the description below, user equipment 30 belonging to owner subscribers of a closed subscriber group is referred to as owner user equipment (Owner UE) 30-O, and user equipment 30 belonging to a subscriber who is newly added to the membership list is referred to as member user equipment (Member UE) 30-M.

[0079]

Firstly, in the owner user equipment 30-O, the subscriber identity of the subscriber to be newly added and the H(e)NB identity and name of the closed subscriber group adding this new subscriber are input manually via the terminal input/output unit 304 into the terminal control unit 303 by the owner subscriber. The terminal control unit 303 also generates membership list modification request information that includes the input subscriber identity, closed subscriber group name, and H(e)NB identity (step S301).

[0080]

Next, in the owner user equipment 30-O, the terminal control unit 303 transmits the generated membership list modification request information and the subscriber identity read from the universal subscriber identity module 301 to the H(e)NB 20 via the terminal communication unit 302 (step S302).

[0081]

The base station control unit 203 receives the membership list modification

request information and subscriber identity from the owner user equipment 30-O via the base station communication unit 204. In addition, the base station control unit 203 transmits the received membership list modification request information and subscriber identity to the core network 10 (step S303).

[0082]

When the authentication center 101 receives the membership list modification request information via the security gateway 104, the authentication center 101 generates member addition confirmation information (step S304). Here, the member addition confirmation information includes a confirmation message urging that a response be made as to whether or not an addition should be made to the closed subscriber group that corresponds to the closed subscriber group name contained in the received membership list modification request, the subscriber identity that is to be added, and the closed subscriber group name and H(e)NB identity of the relevant closed subscriber group.

[0083]

The authentication center 101 transmits the generated member addition confirmation information to the H(e)NB 20 (step S305).

[0084]

When the base station control unit 203 receives the member addition confirmation information from the core network 10, the base station control unit 203 transmits the received member addition confirmation information to the member user equipment 30-M belonging to the subscriber identity contained in the received member addition confirmation information (step S306).

[0085]

In the member user equipment 30-M, when the terminal control unit 303 receives the member addition confirmation information via the terminal communication

unit 302, the terminal control unit 303 outputs a confirmation message which is contained in the received member addition confirmation information to the terminal input/output unit 304. The terminal input/output unit 304 outputs the input confirmation message, and urges the subscriber to respond as to whether or not they wish to participate in the closed subscriber group, namely, to make a response relating to whether or not the subscriber agrees to their subscriber identity being stored in the membership list of the closed subscriber group.

In the member user equipment 30-M, the terminal control unit 303 receives by manual operation of the subscriber via the terminal input/output unit 304 the input of the response information as to whether or not the subscriber will participate in the closed subscriber group. When the response information is input into the terminal communication unit 302, the terminal communication unit 302 generates member addition response information (step S307). Here, the member addition response information includes the subscriber identities stored in the universal subscriber identity module 301, the response information relating to whether or not the subscriber intends to participate in the closed subscriber group, and the closed subscriber group name and H(e)NB identity of the relevant closed subscriber group. Note that when the response information contains "will participate", the terminal control unit 303 stores the closed subscriber group name and the H(e)NB identity that are contained in the member addition confirmation information in the universal subscriber identity module 301.

[0086]

The base station control unit 203 receives the member addition response information from the member user equipment 30-M via the base station communication unit 204. When the response information contained in the received member addition response information indicates "will participate", the base station control unit 203 causes

the subscriber identity contained in the received member addition response information to be written in and consequently stored in the membership list stored in the access list database 202 (step S309).

When, however, the response information contained in the received member addition response information indicates "will not participate", the membership list modification processing is ended.

[0087]

In addition, the base station control unit 203 transmits the received member addition response information to the core network 10 (step S310).

[0088]

The authentication center 101 receives the member addition response information from the H(e)NB 20 via the security gateway 104. When the response information contained in the received member addition response information indicates "will participate", the authentication center 101 writes the subscriber identity to be added in the access control list database 103, and adds it to the membership list of the H(e)NB identity and closed subscriber group name that correspond to the relevant member addition response information. In addition, the authentication center 101 generates member addition completion information (step S311).

Here, the member addition completion information includes information indicating that the processing to modify the membership list of the closed subscriber group has been completed, response information from the member user equipment 30-M, and the subscriber identity of the owner of the closed subscriber group being modified.

[0089]

The authentication center 101 transmits the generated member addition completion information to the H(e)NB 20 via the security gateway 104 (step S312).

[0090]

When the base station control unit 203 receives the member addition completion information from the core network 10, the base station control unit 203 transmits the received member addition completion information to the user equipment 30 indicated by the subscriber identity contained in the received member addition completion information (step S313).

[0091]

In the owner user equipment 30-O, when the terminal control unit 303 receives the member addition completion information from the H(e)NB 20, the terminal control unit 303 outputs response information contained in the received member addition completion information to the terminal input/output unit 304. The terminal input/output unit 304 outputs the response information which has been input from the terminal control unit 303, and notifies the subscriber of the result of the membership list modification processing (step S314).

[0092]

As a result of the above described processing, the user equipment 30 adds a new subscriber to the membership list stored in the core network 10 and H(e)NB 20 by means of a manual operation performed by the owner subscriber. Moreover, although a description of addition processing is given above, the same processing applies to delete a subscriber from the membership list.

Because only an owner is able to modify the membership list of a closed subscriber group, and because the result of the modification is received by the user equipment 30 of the owner, it is possible to prevent any modification of the membership list of a closed subscriber group that is not performed intentionally by an owner, and it is possible to prevent any illegal connection of the user equipment 30 to the H(e)NB 20, or

any incorrect connection of the user equipment 30 to the H(e)NB 20.

Note that when the H(e)NB 20 has a structure that is not provided with the access list database 202, the operations of step S309 are not performed.

[0093]

(Handover processing)

FIG. 10 is a sequence diagram showing handover processing in which a connection of the user equipment 30 is changed from a (e)NodeB 70 to the H(e)NB 20. Note that it is assumed that the user equipment 30 is connected to and performs communication with the (e)NodeB 70, however, it also receives radio waves from the H(e)NB 20.

[0094]

In a state in which the user equipment 30 is connected to and performs communication with the (e)NodeB 70, the terminal communication unit 302 generates a reception signal report that shows the state of received radio waves at fixed time intervals (step S401).

Here, the reception signal report includes information indicating communication states such as the radio wave strength and signal error rate of each received radio wave, the identities and closed subscriber group names of the respective radio base stations transmitting the relevant radio waves, and the subscriber identity of the host terminal.

[0095]

The terminal communication unit 302 transmits the generated reception signal report to the (e)NodeB 70 (step S402).

[0096]

The (e)NodeB 70 detects whether or not the H(e)NB identity of the H(e)NB 20 is contained in the reception signal report received from the user equipment 30. When

the (e)NodeB 70 detects that the H(e)NB identity is contained therein, the (e)NodeB 70 generates handover request information (step S403).

Here, the handover request information includes the H(e)NB identity, the subscriber identity, and the closed subscriber group name that are contained in the reception signal report, and information indicating a handover request to change a connection of the user equipment 30 which corresponds to the relevant subscriber identity to the H(e)NB 20 which corresponds to the relevant H(e)NB identity.

[0097]

The (e)NodeB 70 transmits the generated handover request information to the core network 10 via the radio network controller 50 (step S404).

[0098]

The authentication center 101 receives the handover request information from the (e)NodeB 70 via the radio network controller 50 and the security gateway 104. The authentication center 101 performs authentication processing based on whether or not the H(e)NB identity, the subscriber identity, and the closed subscriber group name that are contained in the received handover request information have been assigned and stored in the access control list database 103. If the authentication center 101 detects that the H(e)NB identity and subscriber identity contained in the received handover request information are assigned and stored in the access control list database 103 and the handover is allowed, the authentication center 101 authenticates a connection change made via handover, and generates handover command information (step S405).

If the authentication center 101 detects that the H(e)NB identity and subscriber identity contained in the received handover request information are not assigned and stored in the access control list database 103, the handover is denied and the processing is ended.

Here, the handover command information includes the subscriber identity of the user equipment 30 for which the handover is to be effected, the H(e)NB identity of the handover destination of this user equipment 30, and the handover command.

[0099]

The authentication center 101 transmits the generated handover command information to the (e)NodeB 70 via the security gateway 104 and the radio network controller 50 (step S406).

[0100]

The (e)NodeB 70 receives handover command information from the core network 10 via the radio network controller 50. The (e)NodeB 70 transmits the received handover command information to the user equipment 30 indicated by the subscriber identity contained in the received handover command information (step S407).

[0101]

When the terminal control unit 303 receives the handover command information from the (e)NodeB 70 via the terminal communication unit 302, the terminal control unit 303 generates terminal connection request information (step S408).

[0102]

The terminal control unit 303 transmits the generated terminal connection request information to the H(e)NB 20 indicated by the H(e)NB identity contained in the received handover command information (step S409).

[0103]

Thereafter, because the processing of steps S410 to S414 is the same as the user equipment 30 connection processing of steps S203 to S207 shown in FIG. 7, a description thereof is omitted.

By performing the above described processing, the user equipment 30 performs a handover to change a connection from the currently connected (e)NodeB 70 to a H(e)NB 20, and performs authentication processing for this handover. When communication with the H(e)NB 20 is possible, it is possible to select fast and low-cost communication by changing the connection destination of user equipment 30 to a H(e)NB 20.

[0104]

Note that when the closed subscriber group name of the handover source (e)NodeB 70 matches the closed subscriber group name of the handover destination H(e)NB 20, then it is also possible for the (e)NodeB 70 to create handover command information that contains the H(e)NB identity of the handover destination H(e)NB 20, and transmit the handover command information to the user equipment 30. Furthermore, a handover from a (e)NodeB 70 to a H(e)NB 20 is described, however, a handover from a H(e)NB 20 to another H(e)NB 20 is also performed in the same way. In this case, based on information that shows the communication states contained in the reception signal report, it is possible to select a H(e)NB 20 that allows fast communication to be performed.

[0105]

Furthermore, in a case in which the base station communication unit 204 transmits the own H(e)NB identity at fixed time intervals, when the terminal control unit 303 detects that the received H(e)NB identity is stored in the universal subscriber identity module 301, the terminal control unit 303 may perform a handover to change a connection from the currently connected (e)NodeB 70 to the H(e)NB 20 associated with the received H(e)NB identity. At this time, the user equipment 30 performs the operation in step S408, and after that, the mobile telecommunications system 1 performs

the operations in step S409 and in steps thereafter.

Furthermore, in a case in which the base station communication unit 204 transmits the own closed subscriber group name at fixed time intervals, when the terminal control unit 303 detects that the received closed subscriber group name is stored in the universal subscriber identity module 301, the terminal control unit 303 may perform a handover to change a connection from the currently connected (e)NodeB 70 to the H(e)NB 20 of the closed subscriber group. At this time, the user equipment 30 performs the operation in step S408, and after that, the mobile telecommunications system 1 performs the operations in step S409 and in steps thereafter.

[0106]

(Authentication processing employing tokens)

FIG. 11 is a sequence diagram showing authentication processing performed using tokens between a H(e)NB 20 and user equipment 30. Note that it is assumed that the closed subscriber group creation processing shown in FIG. 6 has ended. In addition, it is also assumed that the H(e)NB 20 is transmitting its own host H(e)NB identity, and that the user equipment 30 has acquired the H(e)NB identity of the H(e)NB 20 transmitting the connection request prior to the connection request being transmitted.

[0107]

In the core network 10, the authentication center 101 generates a token for each closed subscriber group stored in the authentication center database 102 (step S501).

These tokens are generated such that the information contained in each token is not duplicated. For example, the tokens may be generated randomly, and may be formed by numerical values in which there are no duplicated numerical values.

[0108]

The authentication center 101 transmits generated tokens to the H(e)NB 20 via

the security gateway 104 (step S502).

[0109]

When the base station control unit 103 receives a token from the core network 10, the base station control unit 103 writes the received token in the access list database 202 thereby storing the token therein (step S503).

[0110]

The base station control list 203 transmits the received token to all of the user equipment 30 indicated by the subscriber identities contained in the membership list that is stored in the access list database 202 (step S504).

[0111]

When the terminal control unit 303 receives the token from the H(e)NB 20 via the terminal communication unit 302, the terminal control unit 303 stores the received token in the universal subscriber identity module 301 (step S505).

[0112]

Next, in the user equipment 30, when a connection request to connect to the core network 10 is manually input by a subscriber into the terminal control unit 303 via the terminal input/output unit 304, the terminal control unit 303 generates terminal connection request information (step S511).

Here, the terminal request information includes the subscriber identity and token that the terminal control unit 303 has read from the universal subscriber identity module 301, and the request to connect to the core network 10.

[0113]

The terminal control unit 303 transmits the generated terminal connection request information to the H(e)NB 20 via the terminal communication unit 302 (step S512).

[0114]

When the base station control unit 203 receives the terminal connection request information from the user equipment 30, the base station control unit 203 reads the tokens stored in the access list database 202, and performs authentication processing by detecting whether or not there is a match with the token contained in received terminal connection request information. When the base station control unit 203 detects a match between two tokens, the base station control unit 203 allows the connection request, while if it detects no match between two tokens, the base station control unit 203 denies the connection request. Moreover, the base station control unit 203 generates terminal connection response information that includes the result of the authentication processing for the terminal connection request information (step S513).

[0115]

The base station control unit 203 transmits the generated terminal connection response information to the user equipment 30, and announces the result (step S514).

[0116]

As has been described above, the H(e)NB 20 performs authentication processing for a token-based connection request from user equipment 30. Because this token-based authentication processing is performed using tokens that have been transmitted and stored in advance in the user equipment 30, it is possible to deny connection requests from user equipment 30 whose subscriber identity is fraudulent or has been forged, and security can be maintained.

[0117]

Note that each time the membership list shown in FIG. 9 is modified, the authentication center 101 regenerates the tokens, and transmits the newly generated tokens to the H(e)NB 20 and user equipment 30 that correspond to the closed subscriber

group whose membership list was modified. In addition, it is also possible for the tokens to not only be used in authentication processing for connection requests from the user equipment 30, but for the authentication center 101 to create tokens and transmit the generated tokens to the H(e)NB 20 and to the user equipment 30 indicated by the owner identity of the access control list in order to perform authentication processing for owners of closed subscriber groups.

Furthermore, the authentication center 101 may generate a token for each subscriber identity. In this case, the base station control unit 203 stores tokens associated with the user equipment for which the connection is allowed in the access list database 202. Because of this, the deletion processing that removes the subscribers identity from the membership list is able to be performed only by removing the token associated with the relevant subscriber's identity from the access list database 202. As a result, it is possible to reduce the amount of communication between the H(e)NB 20 and the core network 10 that is required for the deletion processing.

[0118]

Note that when the mobile telecommunications system 1 has a plurality of H(e)NB 20, in step S502, the authentication center 101 transmits a different token for each H(e)NB 20. Moreover, in step S511, the token that is contained in the terminal connection request information generated by the terminal control unit 303 selects the token that corresponds to the destination H(e)NB 20. Here, the terminal control unit 303 selects a token using the H(e)NB identity that the terminal communication unit 302 received from the H(e)NB 20.

[0119]

As is described above, in the first embodiment a structure is employed in which a subscriber identity whose connection is allowed is stored in the access control list

database 103 of the core network 10 for each H(e)NB identity of the H(e)NB 20. Furthermore, in this structure, when the H(e)NBb 20 transmits a connection request or the like from the user equipment 30 to the core network 10, the H(e)NB identity is added to the transmitted request and is transmitted to the core network 10. Because of this, the authentication center 101 is able to perform authentication processing for a request from the user equipment 30 indicated by a subscriber identity to connect to a H(e)NB 20 indicated by a H(e)NB identity by referring to an access control list that is stored in the access control list database 103. As a result, it is possible for the setting of a closed subscriber group for a H(e)NB (i.e., a Home evolved Node B) 20, connections of user equipment 30 to a H(e)NB 20, and handovers to a H(e)NB 20 to be performed securely. Moreover, by performing token-based authentication processing, it is possible to reduce the amount of communication to the core network 10 that is required for the authentication processing.

[0120]

Note that in the mobile telecommunication system 1 of the first embodiment, it is assumed that a H(e)NB 20 is owned and managed by a subscriber, however, it may also be managed by a business which provides mobile telecommunications. Furthermore, in the mobile telecommunication system 1, a description is given in FIGS. 2 and 3 of a structure in which there is one H(e)NB 20, however, there may also be a plurality of H(e)NB 20.

[0121]

Note also that in the mobile telecommunication system 1 of the first embodiment, it is also possible for the membership lists to not be stored in the access list database 202. In this case, the authentication processing for a connection request is performed in the core network 10.

Example 2

[0122]

FIG. 12 is a schematic diagram showing the structure of a mobile telecommunication system 2 of the second embodiment. The mobile telecommunication system 2 has a core network 10a, a mobile management entity (MME) 60 (referred to hereinafter as an MME 60), a home evolved node B (H(e)NB) 20a (referred to hereinafter as a H(e)NB 20a), a NodeB 40 (referred to hereinafter as a NodeB 40), a radio network controller (RNC) 50, user equipment terminals (UE) 30-1, 30-2, ..., 30-n, and an evolved NodeB 70 (referred to hereinafter as a (e)NodeB 70). Note that the user equipments terminals 30-1, ..., 30-n all have the same structure, and, hereinafter, when any one of or all of the user equipment terminals 30-1, ..., 30-n are being represented, they are referred to simply as user equipment 30. In addition, because the user equipment 30, the NodeB 40, the (e)NodeB 70 and the radio network controller 50 all have the same structure as those in the mobile telecommunication system 1 of the first embodiment, the same symbols 40 and 50 are applied thereto and a description thereof is omitted.

[0123]

As is shown in the drawing, the MME 60 is connected between the core network 10a and the H(e)NB 20a, and relays communication data that is exchanged between the core network 10a and the H(e)NB 20a. Moreover, by exchanging data with the H(e)NB 20a, the user equipment 30 is connected to the core network 10a.

The core network 10a is the foundational portion of the mobile telecommunications system 2 that provides mobile telecommunications. In addition, in response to a request from user equipment 30 for a connection to the H(e)NB 20a, the

core network 10a performs authentication processing to determine whether or not to authenticate the connection based on information relating to whether or not the connection to the H(e)NB 20a by the user equipment 30 is allowed.

The H(e)NB 20a is connected to the core network 10a via a public telephone line or via the Internet or the like, and has the function of providing communication between user equipment 30 belonging to a subscriber to a closed subscriber group and the core network 10a.

[0124]

Next, FIG. 13 is a sequence diagram showing processing in the second embodiment.

Firstly, when the H(e)NB 20a is connected to the core network 10a via a public telephone line or via the Internet, an initial connection request that includes a H(e)NB identity that uniquely identifies its own host device is transmitted to the core network 10a via the MME 60 (steps S601 and S602).

When the core network 10a receives the initial connection request from the H(e)NB 20a, the core network 10a sets a secure channel between the core network 10a and the relevant H(e)NB 20a, and generates key information. Subsequently, the core network 10a performs communication with the relevant H(e)NB 20 using the secure channel set with the relevant H(e)NB 20a (step S603).

[0125]

The core network 10a transmits information indicating that a secure channel has been set to the H(e)NB 20a via the MME 60 (step S604).

When the H(e)NB 20a receives the information from the core network 10a indicating that the secure channel has been set, the H(e)NB 20a sets a secure channel between the H(e)NB 20a and the core network 10a, and generates key information (step

S605).

[0126]

After the H(e)NB 20a has been connected to the core network 10a, the user equipment 30 transmits terminal connection request information requesting a connection to the H(e)NB 20 to the H(e)NB 20a (steps S611 and S612).

Here, the terminal connection request information includes a subscriber identity that uniquely identifies the user equipment 30, and information requesting a connection to the H(e)NB 20a.

[0127]

When the H(e)NB 20a receives the terminal connection request information from the user equipment 30, the H(e)NB 20a transmits connection request information that includes the H(e)NB identity to the core network 10a via the MME 60 (steps S613 and S614).

When the core network 10a receives the connection request information which was received from the H(e)NB 20a via the MME 60, the core network 10a determines whether or not to authenticate the connection requested by the received connection request information (step S615).

Moreover, the core network 10a also transmits owner registration command information, which contains information indicating that the connection has been authenticated in the connection request information, the H(e)NB identity of the relevant H(e)NB 20a, and the subscriber identity of the user equipment 30, to the MME 60 (step S616).

[0128]

When the MME 60 receives the owner registration command information from the core network 10a, the MME 60 assigns and then stores the H(e)NB identity and the

subscriber identity contained in the received owner registration command information (step S617).

The MME 60 also transmits the received owner registration command information to the H(e)NB 20a (step S618).

[0129]

When the H(e)NB 20a receives the owner registration command information from the MME 60, the H(e)NB 20a stores the subscriber identity contained in the received owner registration command information as an owner identity which shows the owner of its own host device (step S619).

The H(e)NB 20a also transmits the received owner registration command information to the user equipment 30 (step S620).

[0130]

When the user equipment 30 receives the owner registration command information from the H(e)NB 20a, the user equipment 30 notifies the subscriber that it has been registered to the owner of the relevant H(e)NB 20a, and urges the setting of a closed subscriber group (CSG) which is a group of user equipment 30 that is able to connect to the relevant H(e)NB 20.

[0131]

When the closed subscriber group name and subscriber identities (i.e., membership list) of the closed subscriber group are input manually into the user equipment 30 by the subscriber who is registered as the owner, the user equipment 30 generates CSG setting request information, and the generated CSG setting request information is transmitted to the core network 10a via the H(e)NB 20a and the MME 60 (steps S621 and S622).

Here, the CSG setting request information includes the closed subscriber group

name that corresponds to the closed subscriber group, the subscriber identity whose connection is allowed, the H(e)NB identity of the H(e)NB 20a that corresponds to the closed subscriber group, and the owner identity.

[0132]

The core network 10a receives the CSG setting request information, and stores the CSG setting request information as an access control list to which the closed subscriber group name contained in the received CSG setting request information, the subscriber identity whose connection is allowed, the H(e)NB identity, and the owner identity are assigned (step S623).

The core network 10a then performs authentication processing for the request to connect to the H(e)NB 20a of the user equipment 30 based on the stored access control list.

[0133]

As has been described above, in the second embodiment, a structure is employed in which the core network 10a assigns and stores the H(e)NB identity of the H(e)NB 20a and the subscriber identity for which the connection is allowed. Furthermore, in this structure, when the H(e)NB 20a transmits a connection request from the user equipment 30 to the core network 10a, the H(e)NB identity is added to the transmitted request and is also transmitted to the core network 10a. Because of this, the core network 10a is able to perform authentication processing for a request from the user equipment 30 indicated by the subscriber identity to connect to the H(e)NB 20a indicated by the H(e)NB identity based on whether or not the subscriber identity and the H(e)NB identity have been assigned and stored. As a result, a connection of user equipment 30 to a H(e)NB 20a can be performed securely.

[0134]

The above described authentication center 101, authentication center database 102, access control list database 103, security gateway 104, subscriber database 106, base station control unit 203, terminal control unit 303, H(e)NB 20a, and core network 10a may be provided with an internal computer system. In this case, the procedures of the initial H(e)NB 20 connection processing, the user equipment 30 connection processing, the membership list modification processing, the handover processing, and the token-based authentication processing are stored in program form on a recordable medium that can be read by a computer. The above procedures are then performed as a result of this program being read by the computer. Here, the computer-readable recording medium may be a magnetic disk, a magneto-optical disk, a CD-ROM, a DVD-ROM, or semiconductor memory. It is also possible for the computer program to be delivered to the computer via a communication line, and for the computer receiving this delivery to execute the program.

INDUSTRIAL APPLICABILITY

[0135]

This invention can be applied to the usage to which looking straight at the input position by those who operate it is indispensable.

REFERENCE SIGNS LIST

[0136]

10 core network

101 authentication center

102 authentication center database

103 access control list database

104 security gateway

105 communication network

106 subscriber database

20 H(e)NB

201 authentication module

202 access list database

203 base station control unit

204 base station communication unit

205 antenna

30, 30-1, 30-2, 30-n user equipment

30-O owner user equipment

30-M member user equipment

301 universal subscriber identity module

302 terminal communication unit

303 terminal control unit

304 terminal input/output unit

305 antenna

40 NodeB

50 radio network controller

10a core network

20a H(e)NB

60 MME

70 (e)NodeB

CITATION LIST

Non Patent Literature

[0137]

3GPP TS 22.011 V8.3.0 (2008-03) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service accessibility (Release 8)

CLAIMS

1. A method for connecting, using radio communication, user equipment and a H(e)NB in a mobile telecommunication system having the user equipment, the H(e)NB, and a core network, the method comprising:

a step in which the H(e)NB transmits connection request information, which contains a subscriber identity that identifies the user equipment, to the core network; and

a step in which the core network determines, based on the connection request information that has been received, whether or not to connect the user equipment to the H(e)NB by referring to an access control list that is stored in advance.

2. The method for connecting the user equipment and the H(e)NB according to claim 1, wherein the connection request information contains a H(e)NB identity that is allocated in advance to the H(e)NB.

3. The method for connecting the user equipment and the H(e)NB according to claim 1, wherein the core network stores security association information in which a H(e)NB identity that is allocated in advance to the H(e)NB is associated with IP address information that is allocated to the H(e)NB; and

the connection request information contains the IP address information.

4. The method for connecting the user equipment and the H(e)NB according claim 2 or 3, wherein the access control list contains information in which the H(e)NB identity of the H(e)NB is associated with the subscriber identity of the user equipment whose connection to the H(e)NB is allowed.

5. The method for connecting the user equipment and the H(e)NB according to claim 4, further comprising

a step in which the user equipment transmits terminal connection request information, which contains the subscriber identity of the user equipment and indicates a connection request, to the H(e)NB to which the user equipment requests to be connected.

6. The method for connecting the user equipment and the H(e)NB according to claim 5, further comprising

a step in which the core network determines whether or not to connect the H(e)NB to the core network when receiving the connection request information from the H(e)NB by referring to authentication information that is stored in advance, wherein

the authentication information is information containing the H(e)NB identity of the H(e)NB whose connection to the core network is allowed.

7. The method for connecting the user equipment and the H(e)NB according to claim 6, further comprising

a step in which the core network stores, for each H(e)NB, the subscriber identity as an owner identity and the H(e)NB identity contained in the authentication information in an associated manner, and updates the authentication information, wherein

the subscriber identity contained in the authentication information as the owner identity is the subscriber identity that is contained in the terminal connection request information received by the H(e)NB for the first time, and

the information, which is contained in the access control list and in which the H(e)NB identity is associated with the subscriber identity, is the information determined

by using the user equipment corresponding to the owner identity.

8. The method for connecting the user equipment and the H(e)NB according to claim 7, further comprising, when the user equipment corresponding to the owner identity stores the subscriber identity in the access control list:

a step in which the user equipment corresponding to the subscriber identity outputs information notifying the subscriber of the fact that the subscriber identity is to be stored in the access control list;

a step in which the user equipment transmits response information which is input by an operation of the subscriber, and which contains information indicating whether or not the subscriber approves storing of the subscriber identity in the access control list, to the core network; and

a step in which the core network stores the subscriber identity in the access control list based on information contained in the response information.

9. The method for connecting the user equipment and the H(e)NB according to claim 8, wherein the mobile telecommunication system further comprises a (e)NodeB, and the method further comprises, when the user equipment performs a handover processing to switch a connection from the (e)NodeB to the H(e)NB:

a step in which the user equipment transmits at fixed time intervals a reception signal report concerning radio waves that are received from the (e)NodeB or the H(e)NB to the (e)NodeB or H(e)NB to which the user equipment is connected;

a step in which, based on the received reception signal reports, the (e)NodeB or the H(e)NB transmits handover request information to the core network in order for the connection to the H(e)NB to be switched;

a step in which the core network performs an authentication processing to authenticate the connection in response to the handover request information based on the access control list, and transmits handover command information, which causes the handover to take place based on the result of the authentication processing, to the user equipment; and

a step in which the user equipment switches the connection based on the handover command information.

10. The method for connecting the user equipment and the H(e)NB according to claim 8, wherein

the mobile telecommunication system further comprises a (e)NodeB, and the method further comprises, when the user equipment performs a handover processing to switch a connection from the (e)NodeB to the H(e)NB:

a step in which the H(e)NB transmits the H(e)NB identity of the H(e)NB or a CSG name of the H(e)NB; and

a step in which the user equipment establishes the connection to the H(e)NB based on the H(e)NB identity that is received from the H(e)NB, or the CSG name that is received from the H(e)NB.

11. The method for connecting the user equipment and the H(e)NB according to claim 9 or 10, wherein

the terminal connection request information contains a token that is stored by the user equipment, and the method further comprises:

a step in which the core network generates a different one of these tokens for each H(e)NB based on the access control list stored therein, and transmits one of the

generated tokens to the H(e)NB to which that the one of the generated tokens corresponds and to the user equipment whose connection to the H(e)NB has been allowed, and also causes the one of the generated tokens to be stored therein; and

a step in which the H(e)NB performs an authentication processing for the terminal connection request information by determining whether or not the stored token matches the token contained in the received terminal connection request information.

12. The method for connecting the user equipment and the H(e)NB according to claim 11, wherein

the token that is stored in the user equipment corresponding to the owner identity is different from the token that is stored in the other user equipment, and

the H(e)NB stores two tokens, one of which corresponds to the user equipment corresponding to the owner identity and the other of which corresponds to the other user equipment, that are used in each authentication processing.

13. The method for connecting the user equipment and the H(e)NB according to claim 9 or 10, wherein

a step in which the core network generates a different one of the tokens for each user equipment based on the access control list stored therein, and transmits one of the generated tokens to the user equipment to which the token corresponds and to the H(e)NB whose connection to the user equipment has been allowed, and also causes the token to be stored therein; and

a step in which the H(e)NB performs an authentication processing for the terminal connection request information by determining whether or not the stored token matches the token contained in the received terminal connection request information.

14. The method for connecting the user equipment and the H(e)NB according to any one of claims 2 to 13, wherein the mobile telecommunication system further comprises a mobile management entity, and the method further comprises

a step in which the mobile management entity receives information transmitted from the H(e)NB, and forwards the received information to the core network.

15. A method for authenticating user equipment in communication system having a radio base station and a network, the method comprising:

creating a secure connection between said radio base station and said network;

allowing a communication between said user equipment connecting to said radio base station and said network; and

starting communication between said user equipment and said network through said radio base station.

16. The method for authenticating user equipment according to claim 15, further comprising:

verifying whether said user equipment is owner's equipment in said network; and

allowing further communication between said user equipment and said network through said radio base station, if said user equipment is owner's equipment.

17. The method for authenticating user equipment according to claim 15, further comprising:

verifying whether said user equipment is owner's equipment in said network;

and

informing said radio base station from said network about whether to maintain an access control list.

18. The method for authenticating user equipment according to any one of claims 15 to 17, wherein said radio base station is an H(e)NB.

19. The method for authenticating user equipment according to any one of claims 15 to 18, wherein said network is a core network.

20. A H(e)NB included in a mobile telecommunication system further having user equipment and a core network, wherein

the H(e)NB transmits connection request information, which includes a subscriber identity for identifying the user equipment, to the core network.

21. The H(e)NB according to claim 20, wherein the connection request information contains a H(e)NB identity that is allocated in advance.

22. The H(e)NB according to claim 20, wherein the connection request information contains IP address information that is allocated by the core network.

23. The H(e)NB according to claim 21, comprising:

a base station communication unit receiving from the user equipment terminal connection request information which contains the subscriber identity for identifying the user equipment, and which indicates a request for a connection from the user equipment;

an identity database containing the H(e)NB identity allocated in advance; and

a base station control unit generating and transmitting the connection request information to the core network, wherein

the subscriber identity contained in the connection request information is the subscriber identity contained in the terminal connection request information that is received from the user equipment.

24. The H(e)NB according to claim 22, comprising:

a base station communication unit receiving from the user equipment the terminal connection request information which contains the subscriber identity for identify the user equipment, and which indicates a request for a connection from the user equipment;

an identity database containing a H(e)NB identity that is allocated in advance, and the IP address information; and

a base station control unit generating and transmitting the connection request information to the core network, wherein

the subscriber identity contained in the connection request information is the subscriber identity contained in the terminal connection request information that is received from the user equipment.

25. A core network included in a mobile telecommunication system further having user equipment and a H(e)NB, the core network determining whether or not to connect the user equipment to the H(e)NB based on connection request information which contains a subscriber identity for identifying the user equipment and a H(e)NB identity allocated to the H(e)NB in advance, and which is received from the H(e)NB while

referring to an access control list stored therein in advance.

26. The core network according to claim 25, wherein the access control list contains information in which the H(e)NB identity of the H(e)NB is associated with the subscriber identity of the user equipment whose connection to the H(e)NB is allowed.

27. The core network according to claim 26, comprising:

an access control list database containing the access control list; and

an authentication control unit determining, based on the connection request information, whether or not to connect the user equipment to the H(e)NB by referring to the access control list, wherein

the connection request information indicates a request from the user equipment corresponding to the subscriber identity contained in the connection request information for a connection to the H(e)NB corresponding to the H(e)NB identity contained in the connection request information.

28. A mobile telecommunication system comprising:

user equipment;

a H(e)NB; and

a core network,

wherein the user equipment comprises:

a subscriber identity database containing a subscriber identity for identifying a host terminal;

a terminal control unit generating and outputting terminal connection request information which contains the subscriber identity, and which requests a

connection to the H(e)NB; and

a terminal communication unit transmitting the terminal connection request information received from the terminal control unit to the H(e)NB to which a connection is requested,

the H(e)NB comprises:

a base station communication unit receiving the terminal connection request information from the user equipment;

an identity database containing a H(e)NB identity allocated in advance; and

a base station control unit generating and transmitting connection request information which contains the subscriber identity contained in the terminal connection request information, and which indicates a request for a connection from the user equipment corresponding to the subscriber identity, to the core network, and

the core network comprises:

an access control list database containing information in which the subscriber identity of the user equipment whose connection to the H(e)NB is allowed is associated with the H(e)NB identity of the H(e)NB; and

an authentication control unit determining whether or not to connect the user equipment corresponding to the subscriber identity contained in the connection request information received from the H(e)NB to the H(e)NB corresponding to the H(e)NB identity based on information stored in the access control list database.

FIG. 1

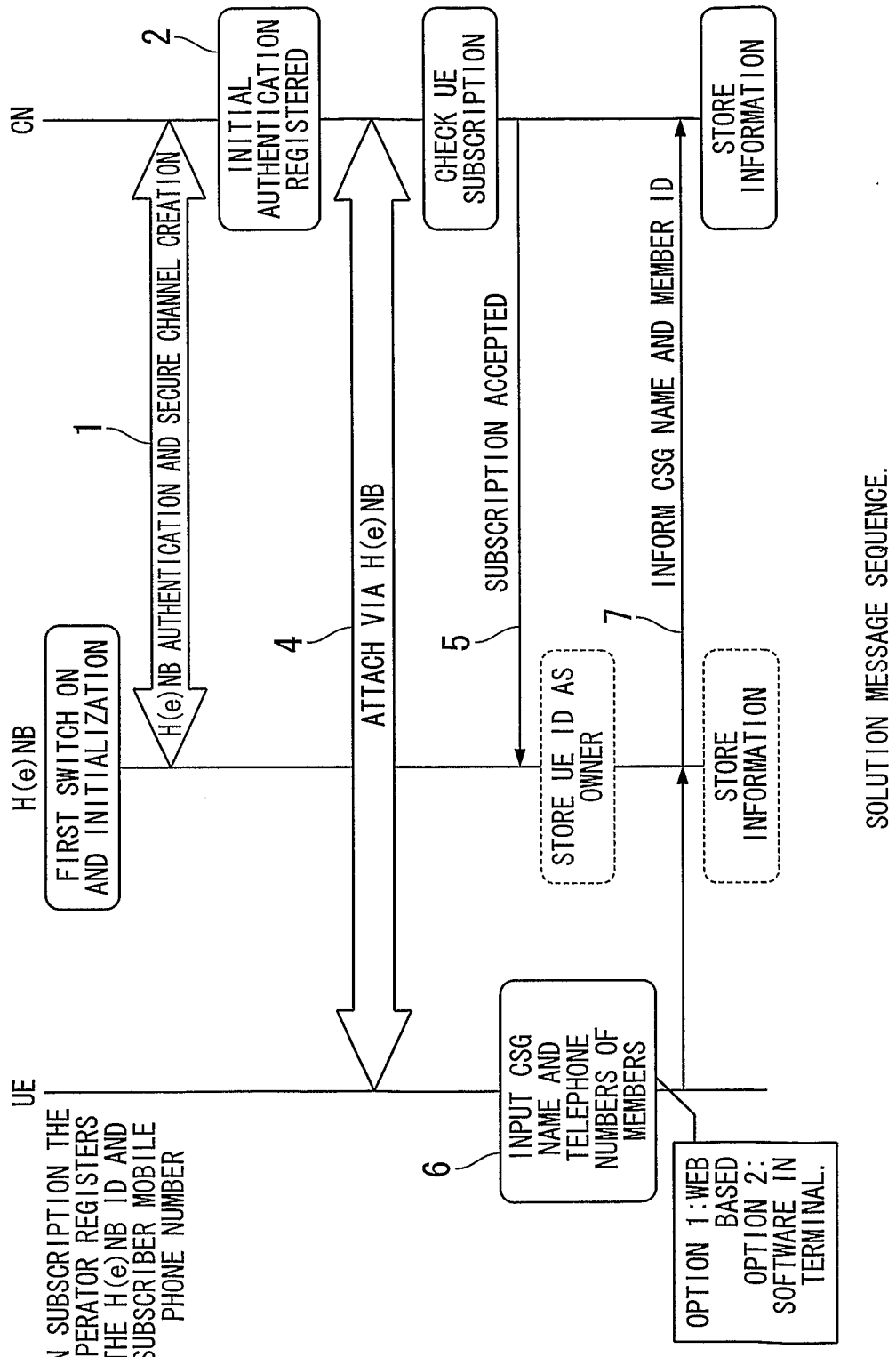

UE
H(e)NB
CN
ON SUBSCRIPTION THE OPERATOR REGISTERS THE H(e)NB ID AND SUBSCRIBER MOBILE PHONE NUMBER
FIRST SWITCH ON AND INITIALIZATION
1
H(e)NB AUTHENTICATION AND SECURE CHANNEL CREATION
2
INITIAL AUTHENTICATION REGISTERED
4
ATTACH VIA H(e)NB
5
SUBSCRIPTION ACCEPTED
CHECK UE SUBSCRIPTION
STORE UE ID AS OWNER
6
INPUT CSG NAME AND TELEPHONE NUMBERS OF MEMBERS
7
INFORM CSG NAME AND MEMBER ID
STORE INFORMATION
STORE INFORMATION
OPTION 1:WEB BASED
OPTION 2: SOFTWARE IN TERMINAL.
SOLUTION MESSAGE SEQUENCE.

FIG. 2

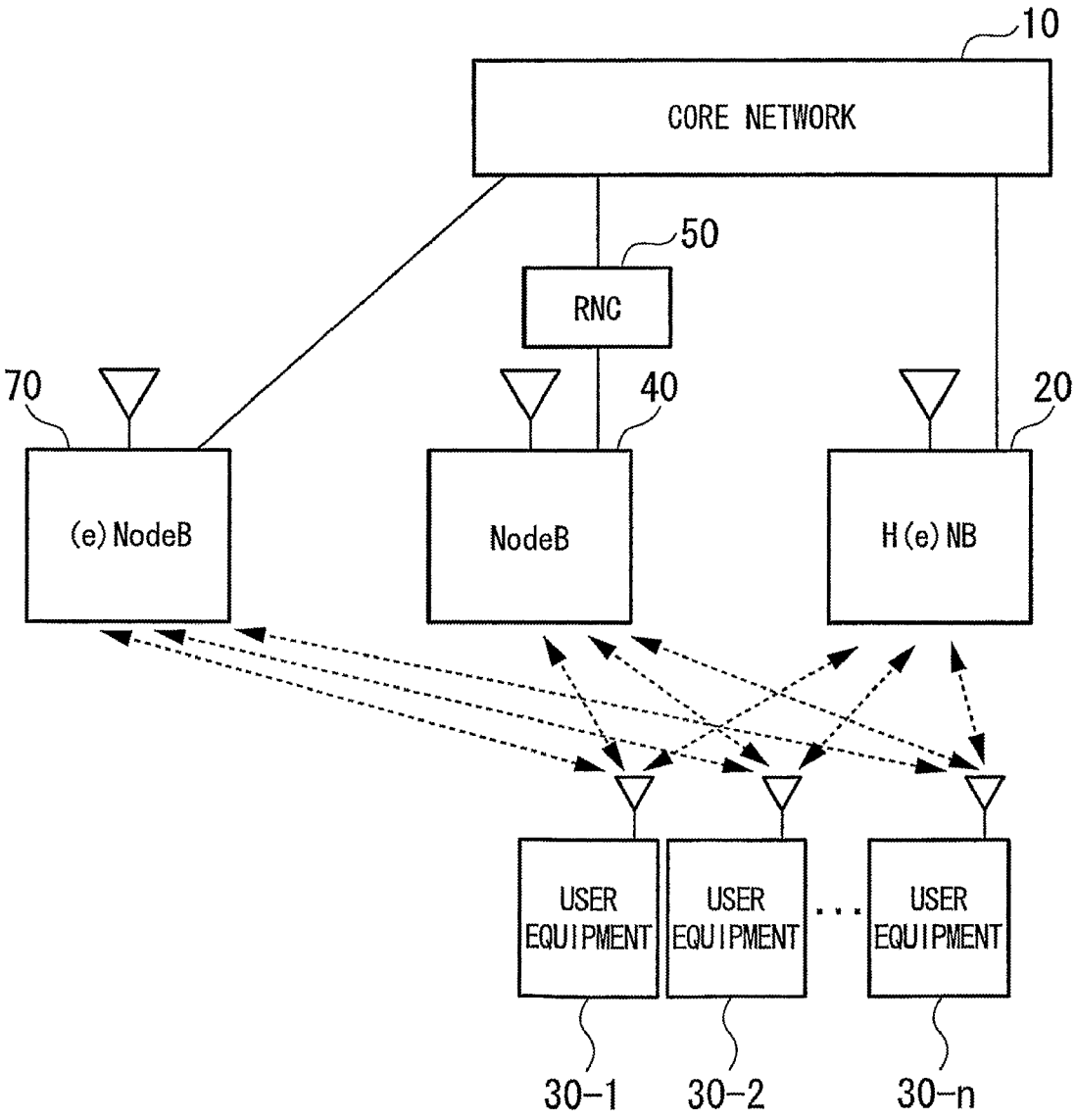

10
CORE NETWORK
50
RNC
70
40
20
(e)NodeB
NodeB
H(e)NB
USER EQUIPMENT
USER EQUIPMENT
USER EQUIPMENT
30-1
30-2
30-n

FIG. 3

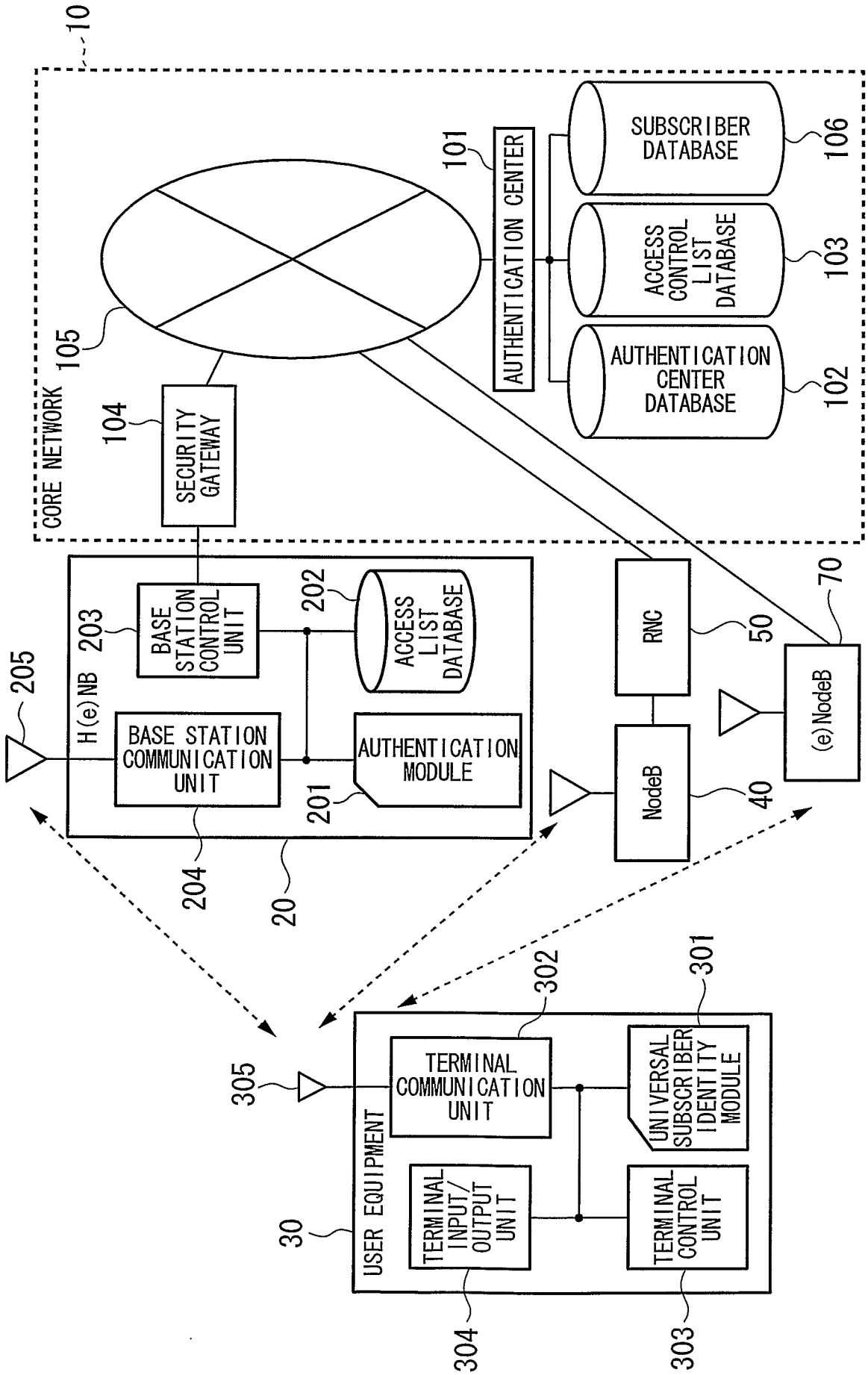

10
CORE NETWORK
105
104
SECURITY GATEWAY
101
AUTHENTICATION CENTER
SUBSCRIBER DATABASE
106
ACCESS CONTROL LIST DATABASE
103
AUTHENTICATION CENTER DATABASE
102
H(e)NB
203
BASE STATION CONTROL UNIT
202
ACCESS LIST DATABASE
205
BASE STATION COMMUNICATION UNIT
AUTHENTICATION MODULE
201
204
20
RNC
50
70
(e)NodeB
NodeB
40
USER EQUIPMENT
30
305
TERMINAL COMMUNICATION UNIT
302
UNIVERSAL SUBSCRIBER IDENTITY MODULE
301
TERMINAL INPUT/OUTPUT UNIT
304
TERMINAL CONTROL UNIT
303

FIG. 4

AUC DB(AUTHENTICATION CENTER DATABASE)

H(e)NB ID	OWNER ID	HENB's FIRST ATTACH
aa0001	0123456789	NO
bb0002		YES
⋮	⋮	⋮

FIG. 5

ACL DB(ACCESS CONTROL LIST DATABASE)

CSG Name	H(e)NB ID	OWNER ID	MEMBERS OF CSG
AAA	aa0001	0123456789	0123456789, 01235556789, 0123456999
BBB	bb0002	0987654321	0987654321, 09875556789, 0987456999
⋮	⋮	⋮	⋮

FIG. 6

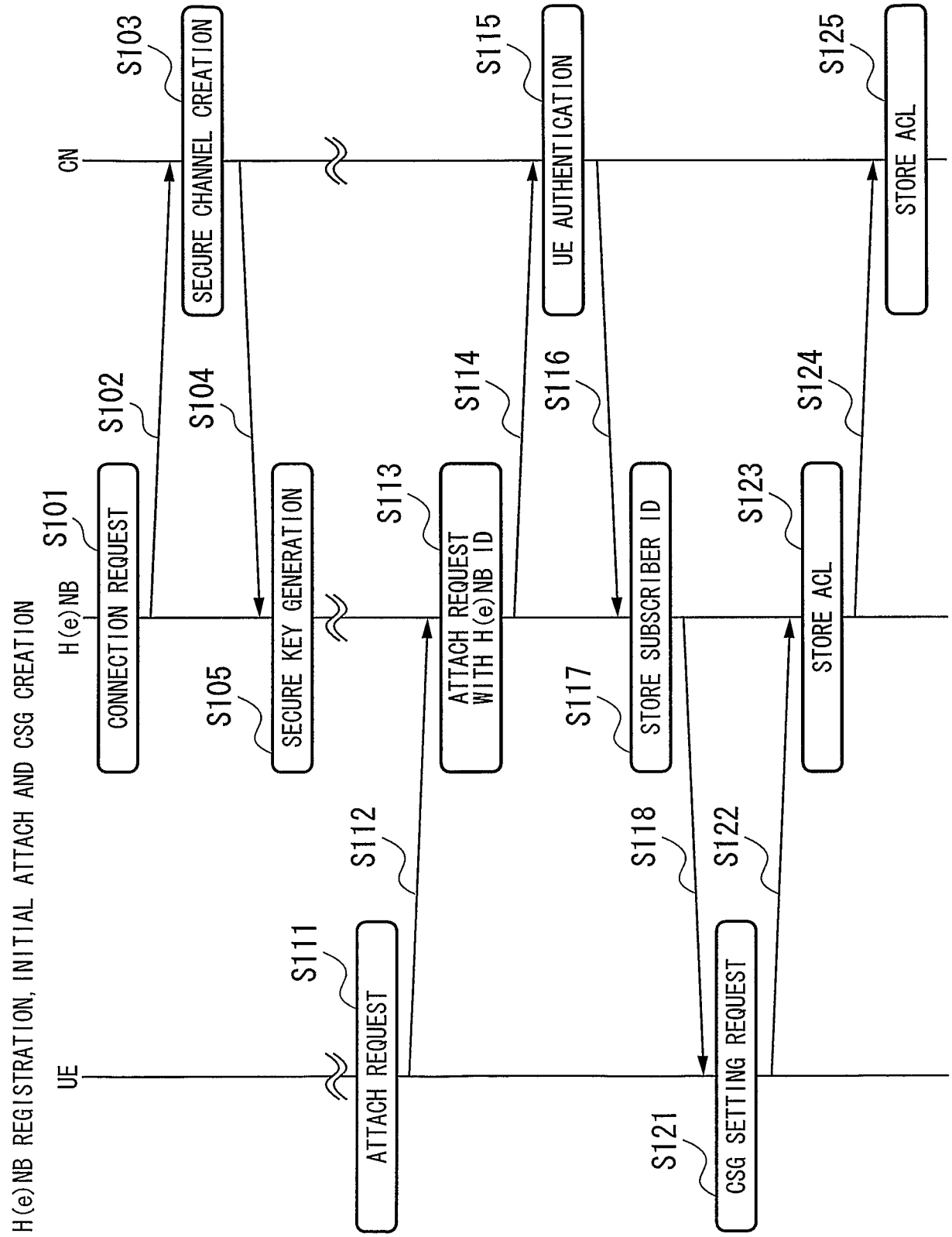

H(e)NB REGISTRATION, INITIAL ATTACH AND CSG CREATION
UE
H(e)NB
CN
S101
CONNECTION REQUEST
S102
S103
SECURE CHANNEL CREATION
S104
S105
SECURE KEY GENERATION
S111
ATTACH REQUEST
S112
S113
ATTACH REQUEST WITH H(e)NB ID
S114
S115
UE AUTHENTICATION
S116
S117
STORE SUBSCRIBER ID
S118
S121
CSG SETTING REQUEST
S122
S123
STORE ACL
S124
S125
STORE ACL

FIG. 7

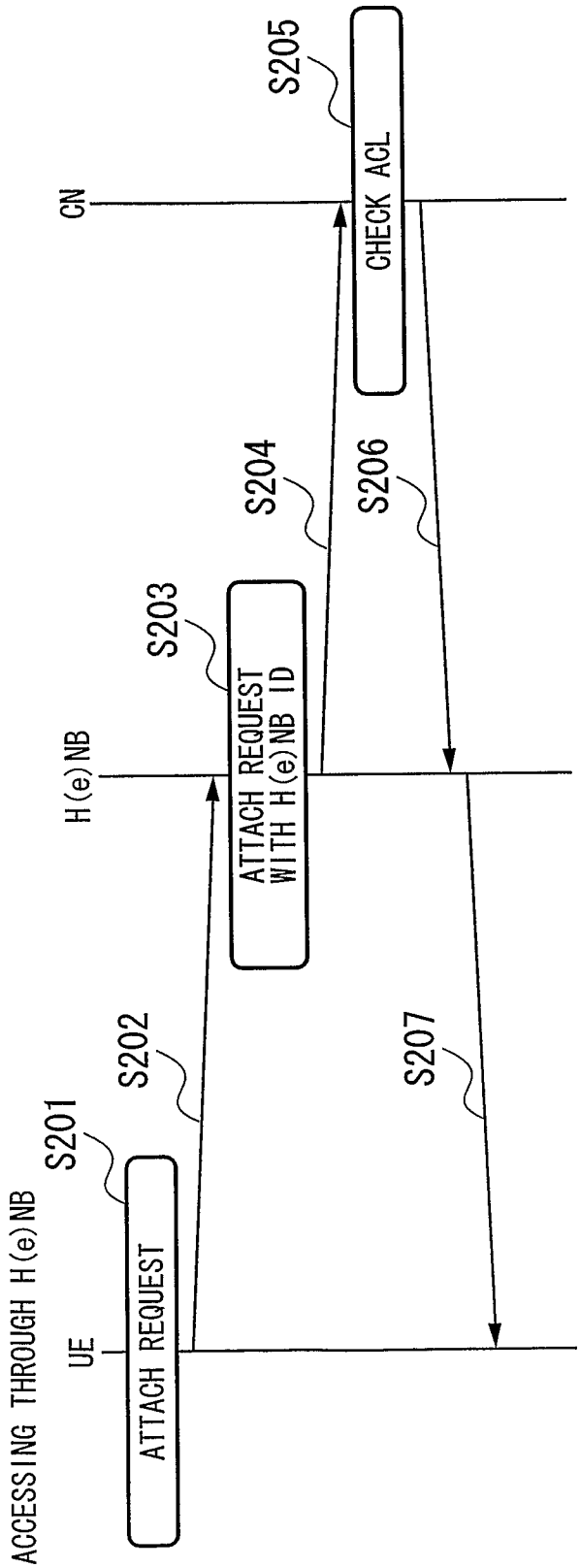

ACCESSING THROUGH H(e)NB
UE
H(e)NB
CN
S201
ATTACH REQUEST
S202
S203
ATTACH REQUEST WITH H(e)NB ID
S204
S205
CHECK ACL
S206
S207

FIG. 8

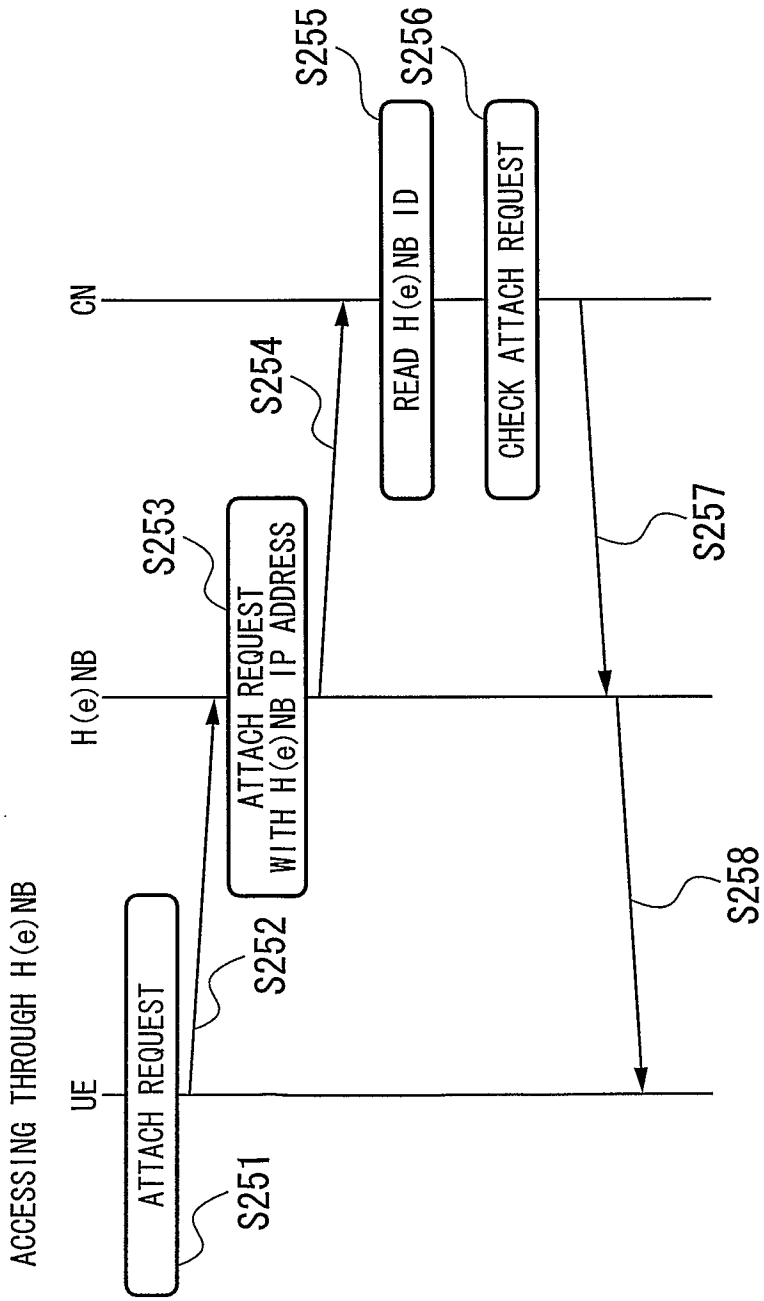

ACCESSING THROUGH H(e)NB
UE
H(e)NB
CN
ATTACH REQUEST
ATTACH REQUEST WITH H(e)NB IP ADDRESS
READ H(e)NB ID
CHECK ATTACH REQUEST
S251
S252
S253
S254
S255
S256
S257
S258

FIG. 9

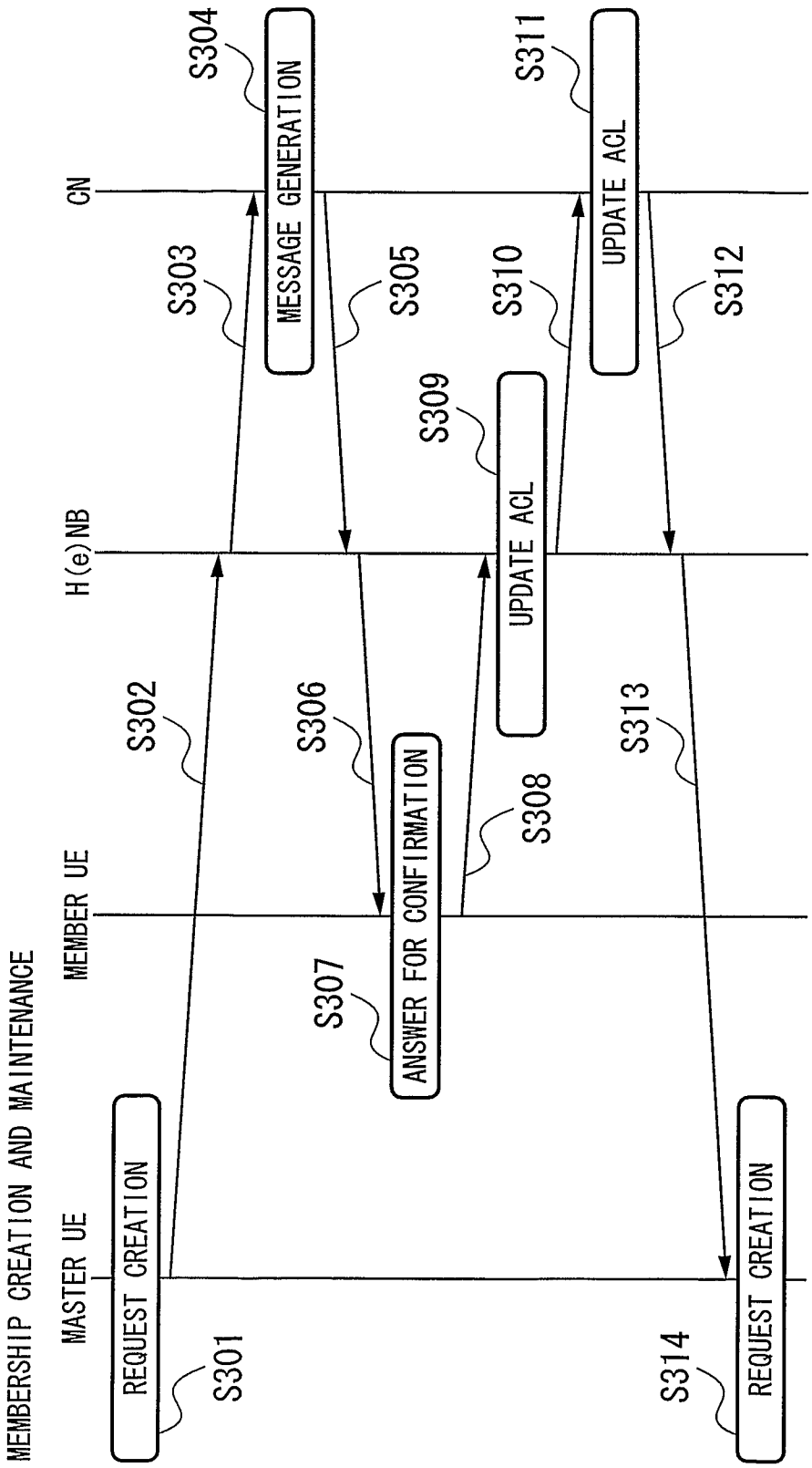

MEMBERSHIP CREATION AND MAINTENANCE
MASTER UE
MEMBER UE
H(e)NB
CN
REQUEST CREATION
S301
S302
S303
MESSAGE GENERATION
S304
S305
S306
ANSWER FOR CONFIRMATION
S307
S308
UPDATE ACL
S309
S310
UPDATE ACL
S311
S312
S313
REQUEST CREATION
S314

FIG. 10

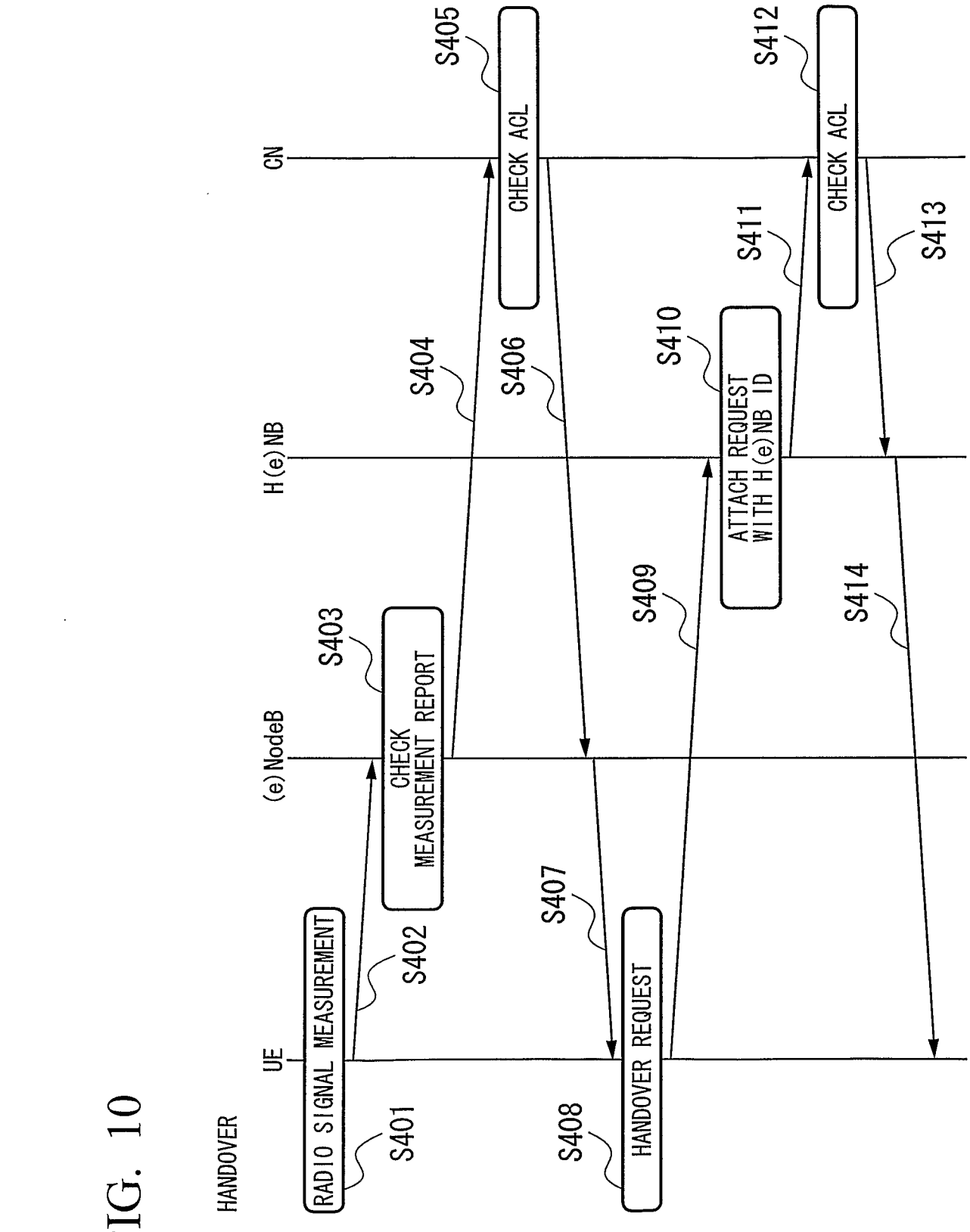

HANDOVER
UE
(e)NodeB
H(e)NB
CN
RADIO SIGNAL MEASUREMENT
S401
S402
CHECK MEASUREMENT REPORT
S403
S404
CHECK ACL
S405
S406
S407
HANDOVER REQUEST
S408
S409
ATTACH REQUEST WITH H(e)NB ID
S410
S411
CHECK ACL
S412
S413
S414

FIG. 11

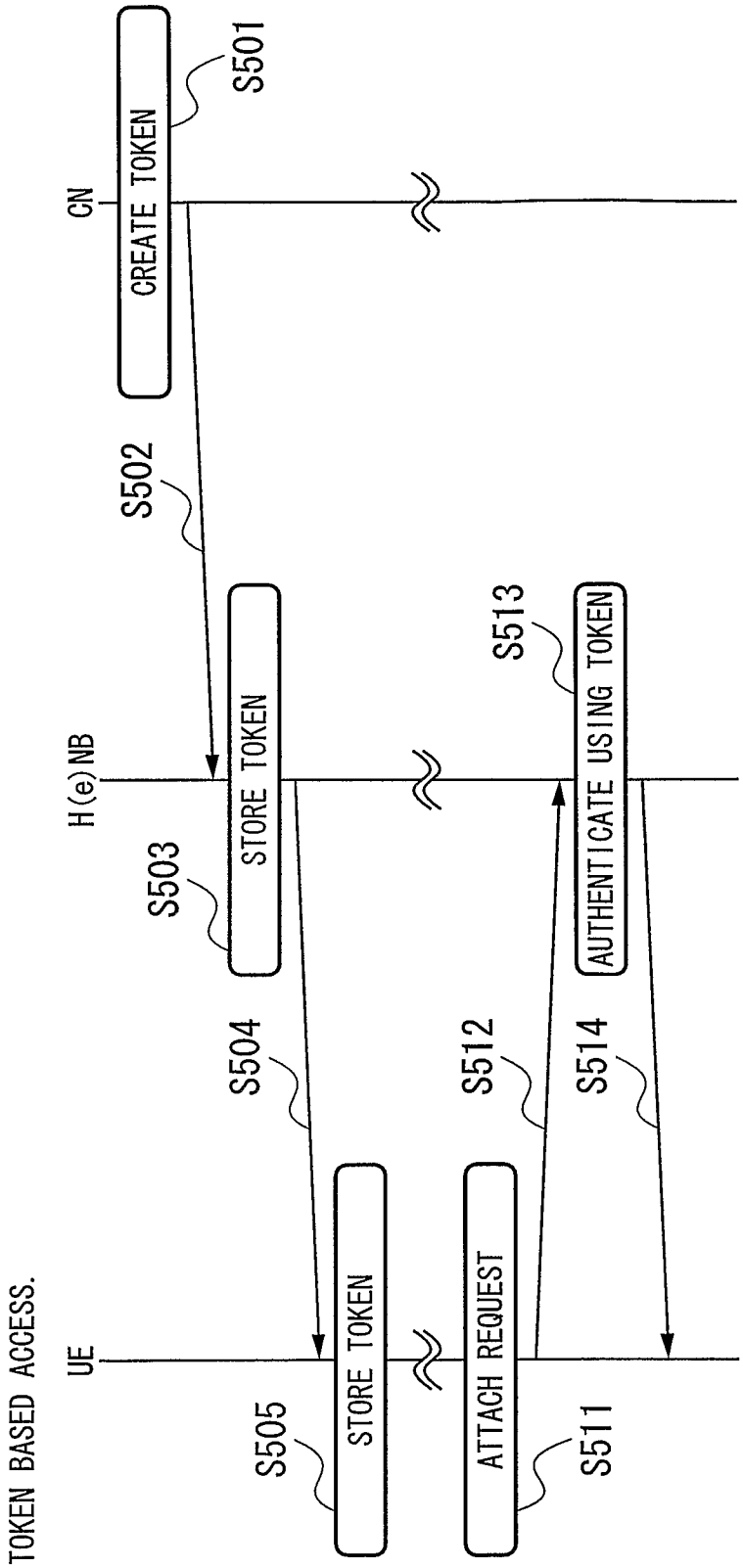

TOKEN BASED ACCESS.
UE
H(e)NB
CN
CREATE TOKEN
S501
S502
STORE TOKEN
S503
S504
STORE TOKEN
S505
ATTACH REQUEST
S511
S512
AUTHENTICATE USING TOKEN
S513
S514

FIG. 12

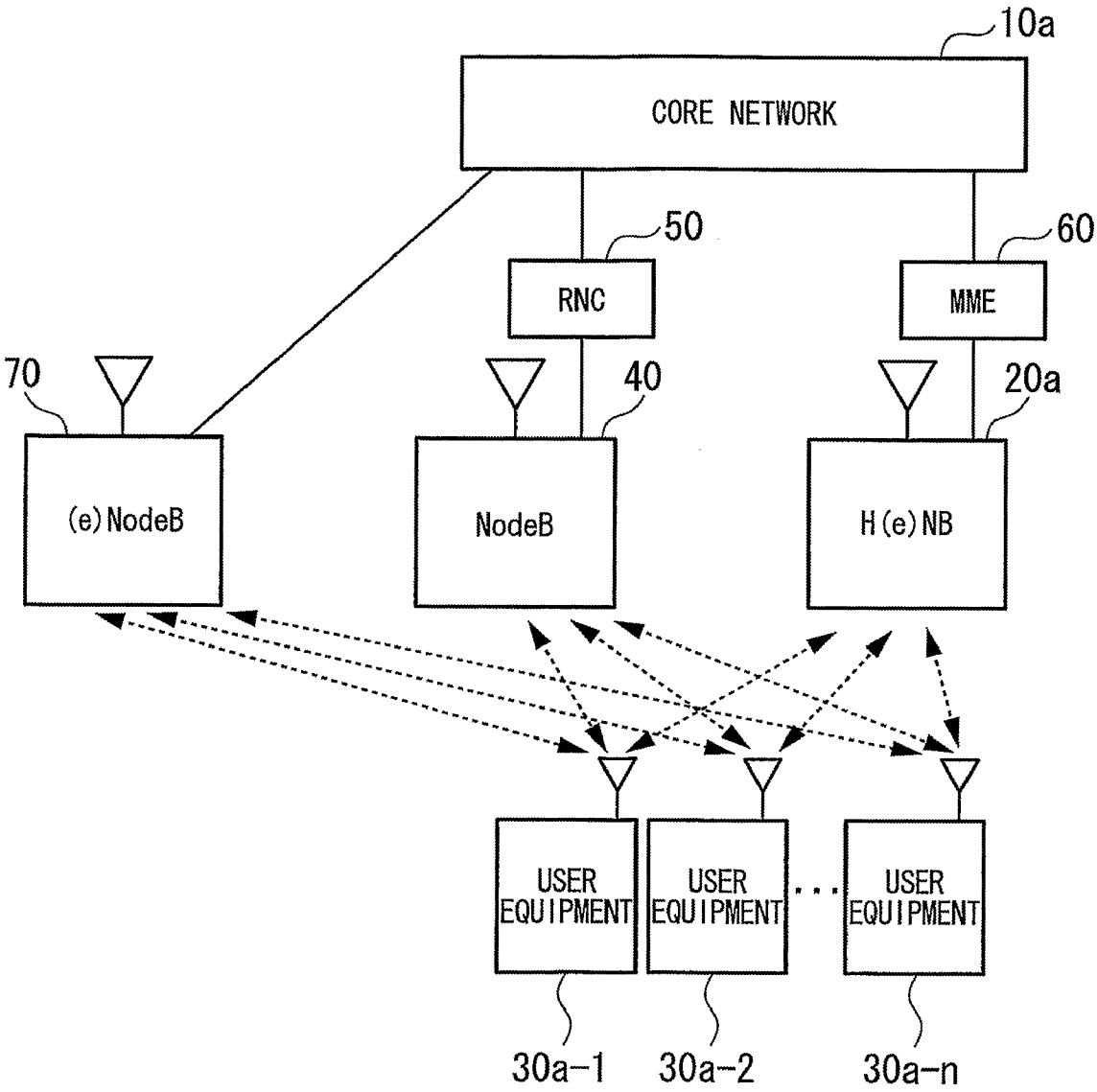
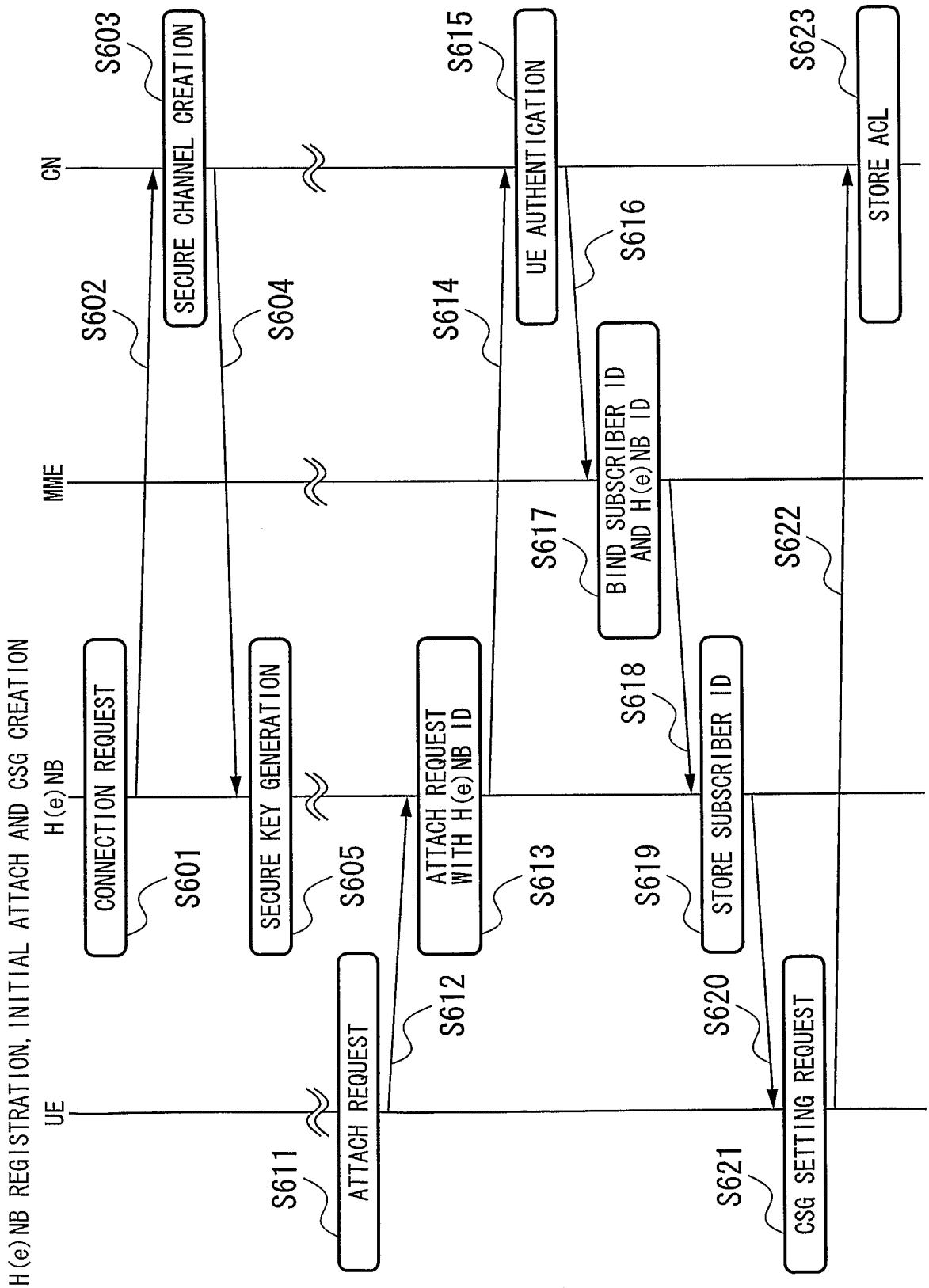

10a
CORE NETWORK
50
60
RNC
MME
70
40
20a
(e)NodeB
NodeB
H(e)NB
USER EQUIPMENT
USER EQUIPMENT
USER EQUIPMENT
30a-1
30a-2
30a-n

FIG. 13


H(e)NB REGISTRATION, INITIAL ATTACH AND CSG CREATION
UE
H(e)NB
MME
CN
CONNECTION REQUEST
S601
ATTACH REQUEST
S611
SECURE CHANNEL CREATION
S602
S603
SECURE KEY GENERATION
S604
S605
ATTACH REQUEST WITH H(e)NB ID
S612
S613
UE AUTHENTICATION
S614
S615
BIND SUBSCRIBER ID AND H(e)NB ID
S616
S617
STORE SUBSCRIBER ID
S618
S619
CSG SETTING REQUEST
S620
S621
STORE ACL
S622
S623