Provided is a method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system. The method includes acquiring a first authentication key by performing an authentication procedure for the communication authentication in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS; and communicating with at least one member BS using a first encryption key that is generated using the first authentication key.
Description

Title of Invention: METHOD AND APPARATUS FOR MANAGING SECURITY KEYS FOR COMMUNICATION AUTHENTICATION WITH MOBILE STATION IN WIRELESS COMMUNICATION SYSTEM

Technical Field

[1] The present disclosure relates to a method and apparatus for managing security keys for communication authentication with a mobile station in a wireless communication system.

Background Art

[2] In order to support high-capacity data services, a wireless communication system that uses a high-frequency band such as, for example, a millimeter wave (mmW) is considered as the next-generation wireless communication system. In the case of the system that uses a high-frequency band, the available communication distance between a Mobile Station (MS) and a Base Station (BS) is short, so a cell radius of the BS is small, causing an increase in the number of BSs installed to secure the service area (or service coverage) for the MS. When the mobility of the MS is taken in consideration, if the cell radius of the BS is reduced and the number of BSs increases, the number of inter-cell handovers of the MS increases, and the system overhead may increase due to the frequent handovers of the MS.

Disclosure of Invention

Technical Problem

[3] In this wireless communication system using a high-frequency band, the number of BSs per unit area may increase. In this case, while an MS moves from place to place, the serving BS in communication with the MS may be changed or replaced frequently, and an authentication procedure for generating and allocating an authentication key or a security key for data exchange or data transmission/reception between the changed BS (to which the MS is handed over) and the MS is required whenever the serving BS is changed. Therefore, there is a need for a method for efficiently performing the authentication procedure in the wireless communication system that uses a high-frequency band.

Solution to Problem

[4] To address the above-discussed deficiencies, it is a primary object to provide a method and apparatus for managing security keys for authentication of an MS and data encryption in a cloud cell-based communication system.
In accordance with one aspect of the present disclosure, there is provided a method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system. The method includes acquiring a first authentication key by performing an authentication procedure for the communication authentication in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS; and communicating with at least one member BS using a first encryption key that is generated using the first authentication key.

In accordance with another aspect of the present disclosure, there is provided a method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system. The method includes acquiring an authentication context for the MS by performing an authentication procedure for the communication authentication with the MS in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS; and communicating with the MS using a first encryption key that is acquired from the authentication context.

In accordance with further another aspect of the present disclosure there is provided a method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system. The method includes performing a member Base Station (BS) subscription procedure for a cloud cell with a master BS in the cloud cell having member BSs that include the master BS and at least one slave BS for providing a service to the MS, and receiving an authentication context for an MS included in the cloud cell from the master BS; and if the authentication context includes a first authentication key, generating a first encryption key using the first authentication key and communicating with the MS using the first encryption key.

In accordance with yet another aspect of the present disclosure there is provided a Mobile Station (MS) for managing a security key for communication authentication with the MS in a communication system. The MS includes a communication unit for acquiring a first authentication key by performing an authentication procedure in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS, and communicating with at least one member BS using a first encryption key that is generated using the first authentication key.

In accordance with still another aspect of the present disclosure, there is provided a master Base Station (BS) for managing a security key for communication authentication with a Mobile Station (MS) in a communication system. The master BS includes a communication unit for acquiring an authentication context for the MS by performing an authentication procedure for the communication authentication with the
MS in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS, and communicating with the MS using a first encryption key that is acquired from the authentication context.

In accordance with still another aspect of the present disclosure, there is provided a slave Base Station (BS) for managing a security key for communication authentication with a Mobile Station (MS) in a communication system. The slave BS includes a communication unit for performing a member Base Station (BS) subscription procedure for a cloud cell with a master BS included in the cloud cell having member BSs that include the master BS and at least one slave BS for providing a service to the MS, and receiving an authentication context for the MS included in the cloud cell from the master BS; and a controller for, if the authentication context includes a first authentication key, controlling a security key generator to generate a first encryption key using the first authentication key, and controlling the communication unit to communicate with the MS using the first encryption key.

Before undertaking the DETAILED DESCRIPTION OF THE INVENTION below, it may be advantageous to set forth definitions of certain words and phrases used throughout this patent document: the terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation; the term "or," is inclusive, meaning and/or; the phrases "associated with" and "associated therewith," as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, or the like; and the term "controller" means any device, system or part thereof that controls at least one operation, such a device may be implemented in hardware, firmware or software, or some combination of at least two of the same. It should be noted that the functionality associated with any particular controller may be centralized or distributed, whether locally or remotely. Definitions for certain words and phrases are provided throughout this patent document, those of ordinary skill in the art should understand that in many, if not most instances, such definitions apply to prior, as well as future uses of such defined words and phrases.

**Brief Description of Drawings**

For a more complete understanding of the present disclosure and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, in which like reference numerals represent like parts:

FIG. 1 illustrates a schematic configuration of a general wireless communication system for handling authentication of an MS and data encryption;

FIG. 2a illustrates a configuration of a cloud cell according to an embodiment of the
present disclosure

[15] FIG. 2b illustrates an exemplary configuration of a wireless communication system for performing an authentication procedure such as authentication of an MS and data encryption in a cloud cell according to an embodiment of the present disclosure.

[16] FIG. 3 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a first embodiment of the present disclosure.

[17] FIGs. 4a and 4b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

[18] FIGs. 5a and 5b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

[19] FIG. 6 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

[20] FIG. 7 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

[21] FIG. 8 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a second embodiment of the present disclosure.

[22] FIGs. 9a and 9b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

[23] FIGs. 10a and 10b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

[24] FIG. 11 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

[25] FIG. 12 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

[26] FIG. 13 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a third embodiment of the present disclosure.

[27] FIGs. 14a and 14b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure.

[28] FIGs. 15a and 15b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure.

[29] FIG. 16 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure.

[30] FIG. 17 illustrates an operation of an authenticator in a cloud cell-based wireless...
communication system according to the third embodiment of the present disclosure

FIG. 18 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a fourth embodiment of the present disclosure.

FIGS. 19a and 19b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

FIGS. 20a and 20b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

FIG. 21 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

FIG. 22 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

FIG. 23 illustrates a signal flow diagram for managing security keys for an MS in a process of configuring a cloud cell in a cloud cell-based wireless communication system according to a fifth embodiment of the present disclosure.

FIG. 24 illustrates a signal flow diagram for managing security keys for an MS when a slave BS is added to a cloud cell, in a cloud cell-based wireless communication system according to the fifth embodiment of the present disclosure.

FIGS. 25a and 25b illustrate signal flow diagrams for managing security keys for an MS in a cloud cell-based wireless communication system according to a sixth embodiment of the present disclosure and

FIG. 26 illustrates an apparatus for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to embodiments of the present disclosure.

Throughout the drawings, the same drawing reference numerals will be understood to refer to the same elements, features and structures.

**Best Mode for Carrying out the Invention**

FIGURES 1 through 26, discussed below, and the various embodiments used to describe the principles of the present disclosure in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the disclosure. Those skilled in the art will understand that the principles of the present disclosure may be implemented in any suitably arranged system or device. In the following description, specific details such as detailed configuration and components are merely provided to assist the overall understanding of exemplary embodiments of the present invention. Therefore, it should be apparent to those skilled in the art that various changes and modifications of the embodiments described herein can be made.
without departing from the scope and spirit of the invention. In addition, descriptions of well-known functions and constructions are omitted for clarity and conciseness.

An embodiment of the present disclosure provides an authentication procedure for data transmission/reception in a cloud cell-based wireless communication system in which a plurality of BSs provide communication services to an MS in cooperation with each other. For a better understanding of the present disclosure, an authentication procedure for data transmission/reception performed in the general wireless communication system will be described first, and then, an authentication procedure performed in a cloud cell according to an embodiment of the present disclosure will be described.

FIG. 1 illustrates a schematic configuration of a general wireless communication system for handling authentication of an MS and data encryption.

Referring to FIG. 1, the general wireless communication system includes an MS 106, an access BS 104, an Access Service Network Gateway (hereinafter referred to as an "authenticator") 102, and an Authentication, Authorization and Accounting server (AAA) 100.

The MS 106 receives a service that an access service network provides via the access BS 104, and the access BS 104 controls wireless resources for the MS 106 and provides a wireless access point needed for communication of the MS 106.

The authenticator 102 manages security keys for authentication and data encryption for the data to be exchanged with the MS 106. The authenticator 102 controls an operation of the access service network for the MS 106, and also serves as a paging control station for managing an idle mode operation of the MS 106. The AAA 100 provides an access network authentication service for the MS 106.

As shown in FIG. 1, the general wireless communication system manages security keys for authentication and data encryption in a scenario where one MS receives a data service via one access BS.

An embodiment of the present disclosure provides a method for managing security keys for authentication and data encryption in a wireless communication system in which a plurality of BSs form a cloud cell in cooperation with each other and perform data exchange or data transmission/reception with an MS in the cloud cell.

A cloud cell will be described below, which is aimed to provide more efficient services to users taking into account the characteristics of high-frequency bands to be used in the wireless communication system to which the present disclosure is applicable. The cloud cell defined in the present disclosure refers to a virtual cell consisting of a plurality of BSs that are located around an MS and provide a service to the MS, and is assumed to operate, for example, in millimeter wave (mmW) bands that can provide broadband services, or in the general cellular bands (e.g., sub 1 GHz,
1.8-2.5 GHz, 3.5-3.6 GHz, etc.).

FIG. 2a illustrates a configuration of a cloud cell according to an embodiment of the present disclosure.

Referring to FIG. 2a, for convenience of description, a cloud cell 200 is assumed to include an MS 208 and, for example, three BSs 202, 204 and 206, which transmit data to the MS 208. It should be noted that the number of BSs constituting the cloud cell is subject to change.

The master BS 202 may transmit both a control signal and data to the MS 208, and manage the remaining BSs, i.e., a slave BS 204 and a slave BS 206. The slave BS 204 and the slave BS 206 may transmit only data to the MS 208 unless they receive special instructions from the master BS 202. The data that the master BS 202, the slave BS 204 and the slave BS 206 transmit to the MS 208 may be the same or different.

The master BS 202, the slave BS 204 and the slave BS 206 are directly connected to a core network 210, and are directly connected to each other in a wired or wireless manner.

The master BS 202, the slave BS 204 and the slave BS 206 may increase the reliability of low-power links in high-frequency bands as they all serve the MS 208, and may increase the throughput by providing a plurality of high-quality links to the MS 208. In addition, they may reduce the delay due to handover operations of the MS 208 located at the edge of their own cell.

In the cloud cell 200, the master BS 202, the slave BS 204 and the slave BS 206 may transmit data to the MS 208 at the same time or with a time difference. Similarly, the MS 208 may transmit data to the master BS 202, the slave BS 204 and the slave BS 206 at the same time or with a time difference. To this end, the MS 208 may have multiple Radio Frequency (RF) chains.

In the cloud cell-based wireless communication system, an MS perform data exchange with multiple BSs belonging to the cloud cell. When the MS moves between BSs belonging to the cloud cell, the handover operation in the general wireless communication system is not required. Therefore, the cloud cell-based wireless communication system may manage the boundless mobility for the MS.

In an embodiment of the present disclosure, an MS performs an operation of managing security keys including an authentication key and a data encryption key, which are for its authentication with multiple BSs and data encryption, respectively, in order to perform data exchange with multiple BSs belonging to the cloud cell.

FIG. 2b shows exemplary configuration of a wireless communication system for performing an authentication procedure such as authentication of an MS and data encryption in a cloud cell according to an embodiment of the present disclosure.

Referring to FIG. 2b, the cloud cell-based wireless communication system includes
an MS 232, a cloud cell 224, an authenticator 222, and an AAA 220. The authenticator 222 and the AAA 220 may be configured separately as shown in FIG. 2b, or may be configured in the form of a single block although not shown in the drawing.

[60] The cloud cell 224 includes a master BS 226 for providing a wireless access point of an access service network to the MS 232, and slave BSs 228 and 230. The master BS 226 provides a data service to the MS 232 by controlling the slave BSs 228 and 230 belonging to the cloud cell 224. In the cloud cell 224, the slave BSs 228 and 230 perform data exchange with the MS 232 by assisting the master BS 226. The authenticator 222 performs an authentication procedure such as managing security keys for authentication and data encryption for the data of the MS 232. The authenticator 222 controls an operation of the access service network for the MS 232, and also serves as a paging control station for managing an idle mode operation of the MS 232. The AAA 220 provides an access network authentication service for the MS 232.

[61] Exemplary embodiments of the present disclosure will be described below in brief.

[62] In a first embodiment of the present disclosure, a cloud seed is used as an input value for generation of an authentication key, and the authentication key is equally used during generation of a data encryption key needed for data exchange between the MS 232 and member BSs. The member BSs include the master BS 226 and the slave BSs 228 and 230 included in the cloud cell 224 to which the MS 232 belongs.

[63] In this specification, a master BS and slave BSs included in a cloud cell will be referred to as 'member BSs'.

[64] The cloud seed may be a value that is generated by the authenticator 222 or the AAA 220 and delivered to the MS 232, or may be a value that is selected by a rule that the MS 232 shares in advance with the authenticator 222 or the AAA 220. The cloud seed is changed when at least one of the member BSs in the cloud cell 224 is deleted. The deleted member BS may be the master BS 226 or one of the slave BSs 228 and 230 in the cloud cell 224.

[65] In a second embodiment of the present disclosure, an identifier of the master BS 226 in the cloud cell 224 to which the MS 232 belongs is used as an input value for generation of an authentication key, and the authentication key is equally used during generation of a data encryption key needed for data exchange between the MS 232 and the member BSs. The encryption key is generated by the authenticator 222, the AAA 220 or the MS 232, and may also be generated by the master BS 226 or each of the slave BSs 228 and 230 depending on the circumstances. If the master BS 226 of the cloud cell 224 is changed to (or replaced by) a new master BS, a new authentication key is generated using an identifier of the new master BS. Based on the new authentication key, a new data encryption key is generated, which is needed for data exchange between the MS and the member BSs including the new master BS added to the cloud.
cell 224. If any slave BS among the member BSs of the cloud cell is added or deleted, i.e., if there is no change in the master BS, the currently used security keys, i.e., the authentication key and the data encryption key are maintained.

[66] In a third embodiment of the present disclosure, an authentication key is generated individually for the master BS 226 and each of the slave BSs 228 and 230 among the member BSs of the cloud cell 224 to which the MS 232 belongs. In other words, an authentication key generated using an identifier of the master BS 226 is used during generation of a data encryption key between the MS and the master BS 226. An authentication key generated using an identifier of the slave BS 228 is used during generation of a data encryption key between the MS 232 and the slave BS 228 among the member BSs. Similarly, an authentication key generated using an identifier of the slave BS 230 is used during generation of a data encryption key between the MS 232 and the slave BS 230. If there is a deleted member BS among the member BSs of the cloud cell 224, the security keys (i.e., an authentication key and a data encryption key) generated by the deleted member BS are deleted. The deleted member BS may be the master BS or the slave BS.

[67] In a fourth embodiment of the present disclosure, an identifier of the master BS 226 of the cloud cell 224 to which the MS 232 belongs is used as an input value for generation of an authentication key, and the authentication key is used during generation of a data encryption key needed for data exchange between the MS 232 and the member BSs. The member BSs include the master BS 226 and the slave BSs 228 and 230 included in the cloud cell 224 to which the MS 232 belongs. The encryption key is generated by the authenticator 222, the AAA 220 or the master BS 226. The authentication key and the data encryption key may be managed or not be used by the slave BSs 228 and 230. If the master BS 226 of the cloud cell 224 is changed to a new master BS, a new authentication key is generated using an identifier of the new master BS. Based on the new authentication key, a data encryption key needed for data exchange between the MS 232 and the member BSs is generated.

[68] In a fifth embodiment of the present disclosure, the MS 232 generates a cloud seed as an input value for generation of an authentication key. The MS 232 delivers the cloud seed to its member BSs, i.e., the master BS 226 and the slave BSs 228 and 230 included in the cloud cell 224. If a member BS is added to the cloud cell 224, the MS 232 delivers the cloud seed to the added member BS. Each of the MS 232 and the member BSs having received the cloud seed from the MS 232 generates an authentication key by using the cloud seed as an input value. In addition, each of the MS 232 and the member BSs having received the cloud seed from the MS 232 generates a data encryption key using the authentication key. If any slave BS among the member BSs of the cloud cell 224 is deleted, the currently used cloud seed may be maintained, or
the MS 232 may generate a new cloud seed and deliver the new cloud seed to the member BSs.

In a sixth embodiment of the present disclosure, the MS 232 generates a cloud seed as an input value for generation of an authentication key. The master BS 226 delivers the cloud seed it has received from the MS 232, to its member BSs, i.e., the slave BSs 228 and 230. If a member BS is added to the cloud cell 224, the master BS 226 delivers the cloud seed to the added member BS. Each of the MS 232 and the member BSs having received the cloud seed from the MS 232 generates an authentication key by using the cloud seed as an input value. In addition, each of the MS 232 and the member BSs having received the cloud seed from the MS 232 generates a data encryption key using the authentication key. If any slave BS among the member BSs of the cloud cell 224 is deleted, the currently used cloud seed may be maintained, or the MS 232 may generate a new cloud seed. In this case, the master BS 226 delivers the new cloud seed to the member BSs.

First Embodiment

FIG. 3 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a first embodiment of the present disclosure.

Referring to FIG. 3, in step 302, an MS 300 performs an access and capability negotiation (also known as 'ranging and capability negotiation') procedure with a master BS 340.

In step 304, an access network authentication and data encryption procedure for the MS 300 is performed between the MS 300 and the master BS 340, an access network authentication and data encryption procedure for the MS 300 is performed between the master BS 340 and an authenticator 360, and an access network authentication and data encryption procedure for the MS 300 is performed between the authenticator 360 and an AAA 370. The authentication process information needed between the MS 300 and the master BS 340, between the master BS 340 and the authenticator 360, and between the authenticator 360 and the AAA 370 is transmitted using an authentication negotiation message exchanged between the MS 300 and the master BS 340, an access network authentication negotiation message exchanged between the master BS 340 and the authenticator 360, and an authentication message exchanged between the authenticator 360 and the AAA 370.

During the authentication procedure in step 304, the MS 300 and the authenticator 360 generate an authentication context, i.e., an authentication key based on a master key provided from the AAA 370. In the first embodiment of the present disclosure, the authentication key or the authentication context is generated using Equation (1) below.

MathFigure 1
[Math.l]

Authentication Key = Dot16KDF (PMK, MSID |Cloud Seed| "AK", AKJength)

[76] Equation (1)

[77] where PMK denotes a Pairwise Master Key (PMK), which is an example of the master key, MSID (Mobile Station IDentifier) denotes an identifier of an MS, Cloud Seed denotes an authentication seed for a cloud cell to which the MS belongs, "AK" denotes a character string indicating an authentication key for data encryption, and Dot16KDF denotes an algorithm that generates an authentication key with a length of AKJength bits by using PMK, MSID, Cloud Seed and "AK" as its input values.

[78] In the cloud cell to which the MS belongs, the cloud seed is used as an input value for generating the authentication key, and the same authentication key generated with the cloud seed is used in data encryption needed for data exchange between the MS and all BSs belonging to the cloud cell. The cloud seed may be a value that is generated by the authenticator 360 or the AAA 370 and delivered to the MS 300 by signaling, or may be a value that is selected by a rule that the MS 300 shares in advance with the authenticator 360 or the AAA 370.

[79] The cloud seed may be changed when any member BS is deleted from a cloud cell member BS list for managing member BSs in the cloud cell. In this case, the changed cloud seed may be a value that is newly generated by the authenticator 360 or the AAA 370, or may be a value that is selected again by a rule that the MS 300 shares in advance with the authenticator 360 or the AAA 370. Furthermore, in step 304, the authenticator 360 delivers the authentication key generated using Equation (1) to the master BS 340. Then, the master BS 340 generates a data encryption key used for data exchange with the MS 300, using the authentication key. Otherwise, using the authentication key, the authenticator 360 directly generates a data encryption key to be used by the MS 300 and the master BS 340, and delivers the generated data encryption key to the master BS 340. Thereafter, in step 306, the MS 300 performs a registration procedure through the master BS 340, and performs data exchange with the master BS 340.

[80] Thereafter, in step 308, the MS 300 and the master BS 340 perform a cloud cell update procedure for adding a slave BS 350 to the cloud cell member BS list. The cloud cell update procedure in this specification may include an operation in which a new BS is added to the cloud cell member BS list for managing member BSs of the cloud cell, an operation in which an existing member BS(s) is deleted from the cloud cell member BS list, an operation in which the existing master BS is changed to a slave BS, and an operation in which an existing slave BS is changed to a master BS.

[81] In step 310, the slave BS 350 performs a cloud cell member BS adding procedure
with the master BS 340. If the slave BS 350 is added to the cloud cell member BS list of the MS 300, the slave BS 350 is provided with a security key that the slave BS 350 will use for its communication with the MS 300. Then, if the slave BS 350 is provided only with the authentication key for the master BS 340 in step 312, or is provided only with the authentication key for the MS 300 from the authenticator 360 in step 314, the slave BS 350 directly generates a data encryption key for the MS 300 using the authentication key.

Thereafter, in step 316, the MS 300 and the master BS 340 perform a cloud cell update procedure for deleting any member BS from the cloud cell member BS list. In step 318, the master BS 340 notifies the authenticator 360 of the fact that an arbitrary member BS is deleted from the cloud cell member BS list. Then, in step 320, a security key update procedure for re-generating an authentication key for the MS 300 is performed. In the security key update procedure of step 320, a cloud seed for reconfiguring an authentication key of the MS 300 is newly generated, and a new authentication key is generated using the generated new cloud seed and Equation (1). In step 320, the authenticator 360 delivers a new authentication key generated using the new cloud seed to the master BS 340, or delivers a data encryption key for the MS 300, which is generated based on the new authentication key, to the master BS 340. If the master BS 340 is provided only with the new authentication key, the master BS 340 directly generates a new data encryption key that master BS 340 will use during data exchange with the MS 300.

In step 322, the master BS 340 notifies even the slave BS 350 of the fact that the member BS is deleted from the cloud cell member BS list. Then, based on the notification, the slave BS 350 performs a cloud cell update procedure for deleting the member BS from the cloud cell member BS list.

In step 324, the master BS 340 delivers the new authentication key or the new data encryption key to the slave BS 350. Otherwise, in step 326, the authenticator 360 delivers the new authentication key or the new data encryption key to the slave BS 350. If the slave BS 350 receives only the new authentication key from the master BS 340 or the authenticator 360, the slave BS 350 generates a new data encryption key using the new authentication key.

If the master BS 340 is deleted from the cloud cell member BS list by the cloud cell update procedure of step 316, a new master BS performs the procedures of steps 320 to 324.

FIGs. 4a and 4b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

Referring to FIG. 4a, the MS acquires synchronization for an access BS in step 400, and performs an access and capability negotiation procedure with the access BS in step
In step 404, the MS starts an authentication procedure with an authenticator and an AAA through the access BS. In step 406, the MS acquires a cloud seed. The cloud seed is a value that is received from the authenticator or the AAA, or a value that is selected by a rule that the MS shares in advance with the authenticator or the AAA.

In step 408, the MS generates an authentication key to be used for its data exchange with the access BS using the cloud seed and Equation (1), and generates a data encryption key using the generated authentication key. In step 410, the MS performs a registration procedure with the access BS, to set the access BS as a master BS of the cloud cell. In step 412, the MS performs data exchange with the master BS using the data encryption key.

In step 414, the MS performs a cloud cell update procedure for adding the master BS to a cloud cell member BS list, and then proceeds to step 416 in FIG. 4b.

Referring to FIG. 4b, the MS determines in step 416 whether a master BS of the cloud cell is changed. If the master BS is changed, the MS determines in step 418 whether the master BS is deleted from the cloud cell member BS list. If the master BS is not deleted, the MS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list in step 420. In step 422, the MS keeps the currently used authentication key and encryption key. In step 424, the MS exchanges data with the member BSs of the cloud cell using the currently used authentication key and data encryption key.

If it is determined in step 418 that the master BS is deleted, the MS terminates its communication with the master BS in step 426. In step 428, the MS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list. In step 430, the MS acquires a new cloud seed. In step 432, the MS generates new security keys using the new cloud seed and Equation (1). The security keys include an authentication key and a data encryption key. Thereafter, the MS performs data exchange with the member BSs of the cloud cell in step 424, using the new data encryption key generated in step 432.

If it is determined in step 416 that the master BS of the cloud cell is not changed, the MS determines in step 434 whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the MS performs a cloud cell update procedure for adding the new BS to the cloud cell member BS list in step 436. In step 438, the MS continues to use the currently used authentication key. In step 424, the MS performs data exchange with the member BSs of the cloud cell that includes the added new BS.

If it is determined in step 434 that there is a deleted member BS among the member BSs of the cloud cell, the MS performs a cloud cell update procedure for deleting the
deleted member BS from the cloud cell member BS list and terminates its communication with the deleted member BS in step 440. In step 422, the MS acquires a new cloud seed. In step 444, the MS generates a new authentication key using the acquired cloud seed and Equation (1), and generates a new data encryption key based on the new authentication key. Thereafter, in step 424, the MS performs data exchange with the remaining member BSs except for the deleted member BS using the new data encryption key.

If it is determined in step 524 that there is a deleted member BS among the member

FIGs. 5a and 5b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

Referring to FIG. 5a, the master BS performs an access and capability negotiation procedure for an MS in step 500. In step 502, the master BS starts an authentication procedure for the MS. In step 504, the master BS receives an authentication context for the MS from an authenticator. The authentication context is an authentication key for the MS or a data encryption key for the MS. If the authentication context received in step 504 is an authentication key for the MS, the master BS generates a data encryption key for the MS using the authentication key in step 506. In step 508, the master BS performs a registration procedure for the MS. In step 510, the master BS exchanges data with the MS using the data encryption key.

In step 512, the master BS performs a cloud cell update procedure for adding the master BS itself to a cloud cell member BS list, and then proceeds to step 514 in FIG. 5b.

Referring to FIG. 5b, the master BS determines in step 514 whether the master BS of the cloud cell is changed.

If the master BS is changed, the master BS determines in step 516 whether the master BS itself is deleted from the cloud cell member BS list. If the master BS is deleted from the cloud cell member BS list, the master BS terminates its communication with the MS in step 518.

If the master BS is not deleted from the cloud cell member BS list, the master BS continues to use the currently used authentication key and data encryption key for the MS in step 520, and performs data exchange with the MS in step 522.

If it is determined in step 514 that the master BS is not changed, the master BS determines in step 524 whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the master BS delivers the currently used authentication key or data encryption key to slave BSs as an authentication context for the MS in step 526. The master BS keeps the currently used data encryption key in step 528, and performs data exchange with the MS using the currently used data encryption key in step 522.

If it is determined in step 524 that there is a deleted member BS among the member
BSs of the cloud cell, the master BS receives a new authentication context for the MS from the authenticator in step 530. The new authentication context is assumed to include only a new authentication key for the MS.

[103] In step 532, the master BS generates a data encryption key for the MS using the new authentication key. If the new authentication context includes a new encryption key for the MS, step 532 is optional. In step 534, the master BS delivers the new authentication context for the MS, which is received in step 530, to the slave BSs. The new authentication context includes a new authentication key and a new encryption key.

Thereafter, in step 522, the master BS performs data exchange with the MS using the new data encryption key.

[104] FIG. 6 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

[105] Referring to FIG. 6, the slave BS performs a cloud cell member subscription procedure with a master BS in step 600. In step 602, the slave BS receives an authentication context for an MS from the master BS or an authenticator. The authentication context corresponds to an authentication key for the MS, or a data encryption key for the MS.

[106] If the authentication context received in step 602 includes only the authentication key for the MS, the slave BS generates a data encryption key for the MS using the authentication key in step 604. In step 606, the slave BS performs data exchange with the MS using the data encryption key.

[107] Thereafter, the slave BS determines in step 608 whether a new authentication context for the MS is received. If the new authentication context for the MS is not received, the slave BS returns to step 606.

[108] If it is determined in step 608 that the new authentication context for the MS is received, and the received new authentication context includes only the new authentication key, the slave BS generates a new data encryption key for the MS using the new authentication key in step 604, and then proceeds to step 606.

[109] If the received new authentication context includes a new data encryption key for the MS, the slave BS omits step 604, and performs data exchange with the MS using the data encryption key in step 606.

[110] FIG. 7 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the first embodiment of the present disclosure.

[III] Referring to FIG. 7, the authenticator starts an authentication procedure for an MS in step 700. In step 702, the authenticator generates a cloud seed for generating an authentication key for the MS. The cloud seed is generated by and received from an AAA, or corresponds to information that the authenticator generates by itself. In other words, the cloud seed is a value that is selected by a common rule shared with the MS,
or a value that is arbitrarily generated by the AAA or the authenticator.

[112] In step 704, the authenticator generates an authentication context for the MS. The authentication context for the MS includes an authentication key for the MS, or a data encryption key for the MS.

[113] Specifically, the authenticator generates an authentication key for the MS using the cloud seed and Equation (1). In step 706, the authenticator delivers the authentication key to a master BS of the MS as an authentication context. The authenticator may generate a data encryption key for the MS using the authentication key, and deliver it to the master BS as the authentication context.

[114] In step 708, the authenticator acquires the cloud cell update information through the master BS. Based on the cloud cell update information, the authenticator determines in step 710 whether there is any change in the member BSs constituting the cloud cell member BS list. If the cloud cell update information indicates the existence of an added new BS in the cloud cell member BS list, the authenticator delivers the authentication key or data encryption key for the MS to the new BS as an authentication context for the MS in step 712. If the master BS serves to deliver the authentication key or data encryption key for the MS to the new BS, the authenticator may skip step 712.

[115] If the cloud cell update information indicates the existence of a deleted member BS in the cloud cell member BS list, the authenticator newly acquires a cloud seed in step 714. In step 716, the authenticator generates only a new authentication key for the MS using Equation (1) based on the new cloud seed, or further generates a new data encryption key using the new authentication key. In step 718, the authenticator delivers a new authentication context including the new authentication key or the new data encryption key, to the master BS. If the master BS does not deliver the new authentication context to slave BSs, the authenticator may deliver the new authentication context to the slave BSs in step 718.

[116] If the master BS is not deleted from the cloud cell member BS list even though the cloud cell update information acquired in step 708 indicates a change in the master BS, the authenticator simply performs a cloud cell update procedure for setting the new master BS as a master BS.

[117] **Second Embodiment**

[118] FIG. 8 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a second embodiment of the present disclosure.

[119] Referring to FIG. 8, an MS 800 performs an access and capability negotiation procedure with a master BS 840 in step 802.

[120] In step 804, an access network authentication and data encryption procedure for the
MS 800 is performed between the MS 800 and the master BS 840, an access network authentication and data encryption procedure for the MS 800 is performed between the master BS 840 and an authenticator 860, and an access network authentication and data encryption procedure for the MS 800 is performed between the authenticator 860 and an AAA 870. The authentication process information needed between the MS 800 and the master BS 840, between the master BS 840 and the authenticator 860, and between the authenticator 860 and the AAA 870 is transmitted using an authentication negotiation message exchanged between the MS 800 and the master BS 840, an access network authentication negotiation message exchanged between the master BS 840 and the authenticator 860, and an authentication message exchanged between the authenticator 860 and the AAA 870.

[121] During the authentication procedure in step 804, the MS 800 and the authenticator 860 generate an authentication context, i.e., an authentication key based on a master key provided from the AAA 870. In the second embodiment of the present disclosure, the authentication key is generated using Equation (2) below.

[122] MathFigure 2

[Math.2]

\[
\text{Authentication Key} = \text{Dot16KDF} \ (\text{PMK, MSID [Master BSID]} \ "AK", \ AK\text{Length})
\]

[123] Equation (2)

[124] where PMK denotes a pairwise master key, MSID denotes an identifier of an MS, Master BSID denotes an identifier of a master BS of a cloud cell to which the MS belongs, "AK" denotes a character string indicating an authentication key for data encryption, and Dot16KDF denotes an algorithm that generates an authentication key with a length of AKLength bits by using PMK, MSID, Master BSID, and "AK" as its input values.

[125] In step 804, the authenticator 860 delivers the authentication key generated using an identifier of the master BS 840 and Equation (2) to the master BS840. The master BS 840 directly generates a data encryption key for data exchange with the MS 800 using the authentication key. Otherwise, using the authentication key, the authenticator 860 directly generates a data encryption key to be used by the MS 800 and the master BS 840, and delivers the generated data encryption key to the master BS 840.

[126] Thereafter, in step 806, the MS 800 performs a registration procedure through the master BS 840, and performs data exchange with the master BS 840.

[127] Thereafter, in step 808, the MS 800 and the master BS 840 perform a cloud cell update procedure for adding a slave BS 850 to a cloud cell member BS list.

[128] In step 810, the slave BS 850 performs a cloud cell member BS adding procedure with the master BS 840. If the slave BS 850 is added to the cloud cell member BS list
of the MS 800, the slave BS 850 is provided with a security key that the slave BS 850 will use for its communication with the MS 800. The security key corresponds to an authentication key or a data encryption key for the MS 800. If the slave BS 850 receives only the authentication key from the master BS 840 in step 812, or receives only the authentication key for the MS 800 from the authenticator 860 in step 814, the slave BS 850 directly generates a data encryption key using the authentication key.

Thereafter, in step 816, the MS 800 and the master BS 840 performs a procedure for changing or replacing a master BS of the cloud cell by performing a cloud cell update procedure. In other words, through the cloud cell update procedure, a new master BS 880 instead of the master BS 840 is changed to a master BS of the cloud cell. In step 818, the new master BS 880 notifies the authenticator 860 of the fact that the new master BS 880 itself is changed to a master BS of the cloud cell. Then, in step 820, the MS 800 and the authenticator 860 perform a security key update procedure for regenerating an authentication key using an identifier of the new master BS 880. In the security key update procedure of step 820, the new master BS 880 generates a new authentication key for the MS 800 using its own identifier and Equation (2). Thereafter, the authenticator 860 delivers the new authentication key to the new master BS 880, or delivers, to the new master BS 880, a data encryption key for the MS that the authenticator 860 has generated based on the new authentication key. If the new master BS 880 receives only the new authentication key for the MS 800, the new master BS 880 directly generates a new data encryption key for the MS using the new authentication key.

In step 822, the new master BS 880 notifies even the slave BS 850 in the cloud cell of the fact that the new master BS 880 itself is changed to a master BS of the cloud cell. Upon receiving the notification, the slave BS 850 performs a cloud cell update procedure for setting the new master BS 880 as (or instead of) the master BS 840.

In step 824, the new master BS 880 delivers the new authentication key for the MS 800 or the new data encryption key for the MS 800 to the slave BS 850. Otherwise, in step 826, the authenticator 860 delivers the new authentication key for the MS 800 or the new data encryption key for the MS 800 to the slave BS 850.

If the master BS 840 is maintained as a master BS of the cloud cell even though the slave BS 850 is deleted from the cloud cell member BS list in accordance with the cloud cell update procedure, the currently used security keys (i.e., the authentication key and the data encryption key) generated by the identifier of the master BS 840 are kept.

FIGs. 9a and 9b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

Referring to FIG. 9a, the MS acquires synchronization for an access BS in step 900,
and performs an access and capability negotiation procedure with the access BS in step 902.

[135] In step 904, the MS starts an authentication procedure with an authenticator and an AAA through the access BS. In step 906, the MS acquires an identifier of the access BS as a master BSID. In step 908, the MS generates an authentication key and a data encryption key to be used for its data exchange with the access BS, using Equation (2). In step 910, the MS performs a registration procedure with the access BS, and then sets the access BS as a master BS of the cloud cell. In step 912, the MS performs data exchange with the master BS.

[136] In step 914, the MS performs a cloud cell update procedure for adding the master BS to a cloud cell member BS list, and then proceeds to step 916 in FIG. 9b.

[137] Referring to FIG. 9b, the MS determines in step 916 whether the master BS is changed. If the master BS is not changed, the MS determines in step 918 whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the MS performs a cloud cell update procedure for adding the new BS to the cloud cell member BS list in step 920. In step 922, the MS keeps the currently used security keys, i.e., the authentication key and the data encryption key. In step 924, the MS exchanges data with the member BSs including the new BS, using the currently used data encryption key.

[138] If it is determined in step 918 that there is a deleted member BS among the member BSs of the cloud cell, the MS performs a cloud cell update procedure for deleting the deleted member BS from the cloud cell member BS list, and terminates its communication with the deleted member BS in step 926. The MS keeps the currently used security keys, i.e., the authentication key and the data encryption key in step 928, and performs data exchange with the remaining member BSs except for the deleted member BS using the currently used data encryption key in step 924.

[139] If it is determined in step 916 that the master BS is changed, the MS determines in step 930 whether the master BS is deleted from the cloud cell member BS list. If the master BS is deleted, the MS terminates its communication with the master BS in step 932. In step 934, the MS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list, and acquires an identifier of the new master BS through this procedure. In step 936, the MS generates new security keys for the new master BS. In other words, the MS generates a new authentication key using the identifier of the new master BS and Equation (2), and generates a new data encryption key using the new authentication key. Thereafter, in step 924, the MS performs data exchange with the member BSs of the cloud cell including the new master BS, using the new data encryption key.

[140] If it is determined in step 930 that the master BS is not deleted from the cloud cell
member BS list, the MS performs a cloud cell update procedure for adding the new master BS to the cloud cell member BS list, thereby acquiring an identifier of the new master BS, in step 938. In step 940, the MS generates new security keys for the new master BS. In other words, the MS generates a new authentication key using the identifier of the new master BS and Equation (2), and generates a new data encryption key using the new authentication key. In step 924, the MS performs data exchange with the member BSs of the cloud cell including the new master BS, using the new data encryption key.

FIGs. 10a and 10b illustrates an operation of a master BS in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

Referring to FIG. 10a, the master BS performs an access and capability negotiation procedure for an MS in step 1000. In step 1002, the master BS starts an authentication procedure for the MS. In step 1004, the master BS receives an authentication context for the MS from an authenticator. The authentication context is an authentication key for the MS, or a data encryption key to be used during data exchange with the MS. If the authentication context received in step 1004 includes only the authentication key, the master BS generates a data encryption key for the MS using the authentication key in step 1006, and performs a registration procedure for the MS in step 1008. Thereafter, in step 1010, the master BS exchanges data with the MS using the data encryption key.

In step 1012, the master BS performs a cloud cell update procedure for adding the master BS itself to the cloud cell member BS list, and then proceeds to step 1014 in FIG. 10b.

Referring to FIG. 10b, the master BS determines in step 1014 whether the master BS of the cloud cell is changed. If the master BS is changed, the master BS proceeds to step 1016. If the master BS of the cloud cell is not changed, the master BS proceeds to step 1026.

In step 1016, the master BS determines whether the master BS itself is deleted from the cloud cell member BS list. If the master BS itself is deleted from the cloud cell member BS list, the master BS terminates its communication with the MS in step 1018.

If it is determined in step 1016 that the master BS is not deleted from the cloud cell member BS list, the master BS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list and receives a new authentication context for the MS from the authenticator or the new master BS, in step 1020. A new authentication key included in the new authentication context is generated using an identifier of the new master BS and Equation (2). If the new authentication context received in step 1020 includes only the new authentication key, the master BS
generates a new data encryption key for the MS using the new authentication key in step 1022. Thereafter, in step 1024, the master BS, as a slave BS for the MS, exchanges data with the MS using the new data encryption key.

In step 1026, the master BS determines whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the master BS performs a cloud cell update procedure for adding the added new BS to the cloud cell member BS list and delivers an authentication context for the MS to the added new BS, in step 1028. The authentication context corresponds to the currently used security keys (i.e., the authentication key and the data encryption key) for the MS. In step 1030, the master BS keeps the currently used security keys. In step 1024, the master BS performs data exchange with the MS using the currently used data encryption key.

If it is determined in step 1026 that there is a deleted member BS, the master BS performs a cloud cell update procedure for deleting the deleted member BS from the cloud cell member BS list in step 1032, and performs data exchange with the MS in step 1024.

FIG. 11 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

Referring to FIG. 11, the slave BS performs a cloud cell member BS subscription procedure with a master BS in step 1100. In step 1102, the slave BS receives an authentication context for an MS. The authentication context may be received from the master BS or an authenticator, and corresponds to an authentication key for the MS and a data encryption key for the MS.

If the authentication context received in step 1102 includes only the authentication key for the MS, the slave BS generates a data encryption key for the MS using the authentication key in step 1104. In step 1106, the slave BS performs data exchange with the MS using the data encryption key. Thereafter, the slave BS determines in step 1108 whether a new authentication context for the MS is received. If the new authentication context is received and the received new authentication context includes only a new authentication key for the MS, the slave BS generates a new data encryption key for the MS using the new authentication key in step 1104, and then proceeds to step 1106.

However, if the new authentication context for the MS includes a new data encryption key for the MS, the slave BS skips step 1104, and performs data exchange with the MS using the new data encryption key in step 1106.

FIG. 12 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the second embodiment of the present disclosure.

Referring to FIG. 12, the authenticator starts an authentication procedure for an MS in step 1200. In step 1202, the authenticator generates an authentication key for the MS
using identification information of a master BS for the MS and Equation (2). In step 1204, the authenticator delivers the authentication key to the master BS for the MS. The authenticator may generate a data encryption key for the MS using the authentication key and deliver the data encryption key to the master BS.

[155] In step 1206, the authenticator acquires the cloud cell update information through the master BS. Based on the cloud cell update information, the authenticator determines in step 1208 whether the master BS of the cloud cell is changed. If the master BS of the cloud cell is changed, the authenticator generates a new authentication key for the MS using the identification information of the new master BS and Equation (2), and generates a new data encryption key for the MS using the new authentication key, in step 1210. In step 1212, the authenticator delivers the new authentication key or the new data encryption key to the master BS as a new authentication context for the MS. If the master BS does not deliver the new authentication key or the new data encryption key to the slave BS, the authenticator delivers the new authentication key or the new data encryption key to the slave BS in step 1212.

[156] If it is determined in step 1208 that the master BS is not changed, the authenticator determines in step 1214 whether there is any added new BS among the member BSs of the cloud cell. If there is no added new BS, the authenticator proceeds to step 1206. However, if there is an added new BS, the authenticator delivers, to the new BS, the authentication key or data encryption key which is generated by the identifier of the master BS and Equation (2), in step 1216. If the master BS delivers the authentication key or data encryption key for the MS to the new BS, the authenticator may skip step 1216.

[157] Third Embodiment

[158] FIG. 13 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a third embodiment of the present disclosure.

[159] Referring to FIG. 13, an MS 1300 performs an access and capability negotiation procedure with a master BS 1340 in step 1302. In step 1304, an access network authentication and data encryption procedure for the MS 1300 is performed between the MS 1300 and the master BS 1340, an access network authentication and data encryption procedure for the MS 1300 is performed between the master BS 1340 and an authenticator 1360, and an access network authentication and data encryption procedure for the MS 1300 is performed between the authenticator 1360 and an AAA 1370. The authentication process information needed between the MS 1300 and the master BS 1340, between the master BS 1340 and the authenticator 1360, and between the authenticator 1360 and the AAA 1370 is transmitted using an authentication negotiation message exchanged between the MS 1300 and the master BS 1340, an access network
authentication negotiation message exchanged between the master BS 1340 and the authenticator 1360, and an authentication message exchanged between the authenticator 1360 and the AAA 1370.

During the authentication procedure in step 1304, the MS 1300 and the authenticator 1360 generate an authentication key as an authentication context based on a master key provided from the AAA 1370. In the third embodiment of the present disclosure, the authentication key is generated using Equation (3) below.

\[
\text{Authentication Key} = \text{Dotl6KDF (PMK, MSID} \ [\text{Member BSID}] \ "AK", \ \text{AKLength})
\]

where PMK denotes a pairwise master key, MSID denotes an identifier of an MS, and Member BSID denotes an identifier of a member BS included in a cloud cell member BS list. In the third embodiment of the present disclosure, Member BSID indicates an identifier of the master BS 1340 during generation of an authentication key to be used between the MS 1300 and the master BS 1340. Also, Member BSID indicates an identifier of a slave BS 1350 during generation of an authentication key to be used between the MS 1300 and the slave BS 1350. In addition, "AK" denotes a character string indicating an authentication key for data encryption, and Dotl6KDF denotes an algorithm that generates an authentication key with a length of AKLength bits by using PMK, MSID, Member BSID, and "AK" as its input values.

Also, in step 1304, the authenticator 1360 delivers, to the master BS 1340, an authentication key that the authenticator 1360 generated using an identifier of the master BS 1340 and Equation (3). Then, the master BS 1340 generates a data encryption key for the MS 1300 using the received authentication key. Otherwise, using the authentication key, the authenticator 1360 directly generates a data encryption key to be used by the MS 1300 and the master BS 1340, and delivers the generated data encryption key to the master BS 1340.

Thereafter, in step 1306, the MS 1300 performs a registration procedure through the master BS 1340 and performs data exchange with the master BS 1340.

Thereafter, in step 1308, the MS 1300 and the master BS 1340 perform a cloud cell update procedure for adding the slave BS 1350 to a cloud cell member BS list.

In step 1310, the slave BS 1350 performs a cloud cell member BS adding procedure with the master BS 1340. The master BS 1340 delivers an identifier of the slave BS 1350 to the authenticator 1360 as cloud cell update information, together with information indicating the fact that the slave BS 1350 is added to the cloud cell member BS list. Otherwise, the slave BS 1350, together with the authenticator 1360, directly
performs a procedure for informing that slave BS 1350 itself is added as a cloud cell member BS. Using this procedure, the authenticator 1360 acquires an identifier of the slave BS 1350. If the cloud cell update procedure is completed in which the slave BS 1350 is added to the cloud cell member BS list for the MS 1300, a security key generation procedure between the slave BS 1350 and the MS 1300 is performed in step 1312. Specifically, the security key generation procedure includes a case in which the authenticator 1360 generates an authentication key between the MS 1300 and the slave BS 1350 using the identifier of the slave BS 1350 and Equation (3), and generates a data encryption key between the MS 1300 and the slave BS 1350 using the authentication key. In this case, the generated security key or data encryption key is delivered to the slave BS 1350 through the authenticator 1360 or the master BS 1340. If the security key that is delivered to the slave BS 1350 through the authenticator 1360 or the master BS 1340 includes only the authentication key, the slave BS 1350 directly generates a data encryption key for the MS 1300 using the authentication key.

If the master BS 1340 or the slave BS 1350 is deleted from the cloud cell member BS list in accordance with the cloud cell update procedure, the data encryption key and the authentication key, which were generated using the identifier of the deleted master BS or slave BS, are deleted.

FIGs. 14a and 14b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure. Referring to FIG. 14a, the MS acquires synchronization for an access BS in step 1400, and performs an access and capability negotiation procedure with the access BS in step 1402. In step 1404, the MS starts an authentication procedure with an authenticator and an AAA through the access BS. In step 1406, the MS acquires information about an identifier of the access BS. In step 1408, the MS generates, as security keys, an authentication key and a data encryption key to be used for its data exchange with the access BS, using the information about the identifier of the access BS and Equation (3). In step 1410, the MS performs a registration procedure with the access BS to set the access BS as a master BS of the cloud cell. In step 1412, the MS performs data exchange with the set master BS. In step 1414, the MS performs a cloud cell update procedure for adding the master BS to a cloud cell member BS list, and then proceeds to step 1416 in FIG. 14b.

Referring to FIG. 14b, the MS determines in step 1416 whether the master BS of the cloud cell is changed. If the master BS is changed, the MS proceeds to step 1418, and if the master BS is not changed, the MS proceeds to step 1432. In step 1418, the MS determines whether the master BS is deleted from the member BSs of the cloud cell. If the master BS is deleted, the MS performs a cloud cell update procedure for deleting the master BS from the cloud cell member BS list and deletes the security keys
including the authentication key and the data encryption key used for its data exchange with the master BS, in step 1420. In step 1422, the MS terminates communication with the master BS. Thereafter, in step 1424, the MS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list, generates a new authentication key using an identifier of the new master BS and Equation (3), and generates a data encryption key using the new authentication key. If the new master BS is one of the slave BSs included in the cloud cell member BS list for the MS, the MS does not need to additionally perform the procedure for generating a new authentication key and a data encryption key for the new master BS as in step 1424, because the MS is already using the authentication key and the data encryption key which were made using the identifier of the new master BS and Equation (3). In step 1426, the MS performs data exchange with the member BSs of the cloud cell including the new master BS.

If it is determined in step 1418 that the master BS is not deleted from the cloud cell member BS list, the MS performs a cloud cell update procedure for setting the master BS as a slave BS, maintains the security keys currently used for its communication with the master BS, and continues to perform data exchange with the master BS using the data encryption key currently used for its communication with the master BS, in step 1428. In step 1430, the MS performs a cloud cell update procedure for setting the new master BS as a master BS, and generates security keys to be used for its communication with the new master BS. In other words, the MS generates a new authentication key to be used for its communication with the new master BS, using an identifier of the new master BS and Equation (3), and generates a new encryption key using the new authentication key. In step 1426, the MS performs data exchange with the member BSs including the new master BS, using the new encryption key.

If the MS determines in steps 1424 and 1430 that the new master BS is a slave BS which was included in the cloud cell member BS list, the MS uses the currently used encryption key for its communication with the master BS, for data exchange with the new master BS, since the authentication key and the data encryption key, which were made using the identifier of the new master BS, are already being used.

If it is determined in step 1416 that the master BS of the cloud cell is not changed, the MS determines in step 1432 whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the MS performs a cloud cell update procedure for adding the new BS to the cloud cell member BS list and generates security keys to be used for its communication with the new BS, in step 1434. In other words, the MS generates an authentication key for the new BS using the identifier of the new BS and Equation (3), and generates a data encryption key to be used for its data exchange with the new BS, using the authentication key. Thereafter, in step 1426, the MS performs data exchange with the added new BS.
using the generated data encryption key.

If it is determined in step 1432 that there is a deleted member BS among the member BSs of the cloud cell, the MS deletes the deleted member BS from the cloud cell member BS list and deletes the security keys for the deleted member BS, in step 1436. The MS terminates its communication with the deleted member BS in step 1438, and performs data exchange with the remaining member BSs except for the deleted member BS in step 1426.

FIGs. 15a and 15b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure.

Referring to FIG. 15a, the master BS performs an access and capability negotiation procedure for an MS in step 1500. In step 1502, the master BS starts an authentication procedure for the MS. In step 1504, the master BS receives an authentication context for the MS from an authenticator. The authentication context may be an authentication key for the MS or a data encryption key for the MS. If the received authentication context includes only the authentication key, the master BS generates, as a security key, a data encryption key for the MS using the authentication key in step 1506. The master BS performs a registration procedure for the MS in step 1508 and exchanges data with the MS in step 1510.

Thereafter, in step 1512, the master BS performs a cloud cell update procedure for the MS to add the master BS itself to the cloud cell member BS list, and then proceeds to step 1514 in FIG. 15b.

Referring to FIG. 15b, the master BS determines in step 1514 whether the master BS of the cloud cell is changed. If the master BS is changed, the master BS proceeds to step 1516, and if the master BS of the cloud cell is not changed, the master BS proceeds to step 1524.

In step 1516, the master BS determines whether the master BS itself is detected from the cloud cell member BS list. If the master BS is deleted from the cloud cell member BS list, the master BS terminates communication with the MS in step 1518.

If the master BS is not deleted from the cloud cell member BS list, the master BS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list and keeps the currently used security keys (i.e., the authentication key and data encryption key for the MS) in step 1520. In step 1522, the master BS performs data exchange with the MS using the currently used authentication key and data encryption key for the MS.

In step 1524, the master BS determines whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the master BS performs a cloud cell update procedure for adding the new BS to the
cloud cell member BS list and keeps the currently used security keys (i.e., the authentication key and data encryption key for the MS) in step 1526. In step 1522, the master BS performs data exchange with the MS using the current used data encryption key for the MS.

[183] If it is determined in step 1524 that there is a deleted member BS, the master BS performs a cloud cell update procedure for deleting the deleted member BS from the cloud cell member BS list, and keeps the currently used security keys (i.e., the authentication key and data encryption key for the MS) in step 1528. In step 1522, the master BS performs data exchange with the MS using the data encryption key for the MS.

[184] FIG. 16 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure.

[185] Referring to FIG. 16, the slave BS performs a cloud cell member subscription procedure with a master BS in step 1600. In step 1602, the slave BS receives an authentication context for an MS from the master BS or an authenticator. The authentication context corresponds to an authentication key for the MS or a data encryption key for the MS. If the authentication context received in step 1602 includes only the authentication key for the MS, the slave BS generates a data encryption key for the MS as a security key, using its own identifier and Equation (3), in step 1064. In step 1606, the slave BS performs data exchange with the MS using the data encryption key.

[186] Thereafter, the slave BS determines in step 1608 whether a new authentication context for the MS is received. If the new authentication context for the MS is not received, the slave BS performs data exchange with the MS using the currently used data encryption key in step 1606.

[187] However, if the new authentication context for the MS is received, and the new authentication context corresponds to a new encryption key for the MS, the slave BS generates a new data encryption key for the MS using the new authentication key in step 1604. On the other hand, if the new authentication context for the MS includes a new data encryption key for the MS, the slave BS skips step 1604, and performs data exchange with the MS using the received new data encryption key in step 1606.

[188] FIG. 17 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the third embodiment of the present disclosure.

[189] Referring to FIG. 17, the authenticator starts an authentication procedure for an MS in step 1700. In step 1702, the authenticator generates an authentication key for the MS using identification information of a master BS of the cloud cell to which the MS belongs, and Equation (3).

[190] In step 1704, the authenticator delivers the authentication key to the master BS of the MS as an authentication context for the MS. The authenticator may generate a data encryption key for the MS using the authentication key and deliver it to the master BS. In
step 1706, the authenticator acquires the cloud cell update information through the master BS.

Based on the cloud cell update information, the authenticator determines in step 1708 whether a new BS is added to a cloud cell member BS list. If a new BS is added, the authenticator delivers to the new BS, a new authentication key generated using an identifier of the new BS and Equation (3) or a new data encryption key generated using the new authentication key, in step 1710. The new authentication key or the new data encryption key to be used by the new BS and the MS may be delivered to the new BS through the master BS.

Fourth Embodiment

FIG. 18 illustrates a signal flow diagram for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to a fourth embodiment of the present disclosure.

Referring to FIG. 18, an MS 1800 performs an access and capability negotiation procedure with a master BS 1840 in step 1802. In step 1804, an access network authentication and data encryption procedure for the MS 1800 is performed between the MS 1800 and the master BS 1840, an access network authentication and data encryption procedure for the MS 1800 is performed between the master BS 1840 and an authenticator 1860, and an access network authentication and data encryption procedure for the MS 1800 is performed between the authenticator 1860 and an AAA 1870. The authentication process information needed between the MS 1800 and the master BS 1840, between the master BS 1840 and the authenticator 1860, and between the authenticator 1860 and the AAA 1870 is transmitted using an authentication negotiation message exchanged between the MS 1800 and the master BS 1840, an access network authentication negotiation message exchanged between the master BS 1840 and the authenticator 1860, and an authentication message exchanged between the authenticator 1860 and the AAA 1870.

During the authentication procedure in step 1804, the MS 1800 and the authenticator 1860 generate an authentication context or an authentication key based on a master key provided from the AAA 1870. In the fourth embodiment of the present disclosure, the authentication key is generated using Equation (2) above.

Further, in step 1804, the authenticator 1860 delivers the authentication key generated using Equation (2), to the master BS 1840. Using the received authentication key, the master BS 1840 generates a data encryption key used for its data encryption with the MS 1800. Otherwise, the authenticator 1860 directly generates a data encryption key to be used by the MS 1800 and the master BS 1840 using the authentication key, and delivers the data encryption key to the master BS 1840. Thereafter, in step 1806, the MS performs a registration procedure through the master BS 1840, and
performs data exchange with the master BS 1840.

[197] Thereafter, in step 1808, the MS 1800 and the master BS 1840 perform a cloud cell update procedure for adding a slave BS 1850 to a cloud cell member BS list. Further, in step 1810, the slave BS 1850 performs a cloud cell member BS adding procedure with the master BS 1840.

[198] Thereafter, in step 1812, the MS 1800 and the master BS 1840 perform a cloud cell update procedure for changing the master BS of the cloud cell. It is assumed that a new master BS 1880 instead of the master BS 1840 is set as a master BS of the cloud cell. Then, in step 1814, the new master BS 1880 provides the authenticator 1860 with information indicating the change in the master BS of the cloud cell.

[199] Thereafter, in step 1816, the MS 1800 and the authenticator 1860 perform a security key update procedure for the MS 1800 using an identifier of the new master BS 1880. In other words, the MS 1800 and the authenticator 1860 generate a new authentication key for the MS 1800 using the identifier of the new master BS 1880 and Equation (2). Further, in step 1816, the authenticator 1860 delivers, as a new authentication context for the MS 1800, the generated new authentication key or a new data encryption key for the MS 1800, which is generated based on the authentication key, to the new master BS 1880. If the new master BS 1880 receives only the new authentication key, the new master BS 1880 directly generates a new data encryption key for the MS 1800 using the new authentication key.

[200] In step 1818, the new master BS 1880 notifies even the slave BS 1850 in the cloud cell that the master BS of the cloud cell is changed to the new master BS 1880, thereby updating the cloud cell member BS list by which the slave BS 1850 may set the new master BS 1880 as a master BS of the cloud cell.

[201] In FIG. 18, in a case where a member BS included in the cloud cell member BS list is deleted or added, if the master BS is not changed, the currently used security keys for the MS 1880 are maintained unchanged.

[202] FIGs. 19a and 19b illustrate an operation of an MS in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

[203] Referring to FIG. 19a, the MS acquires synchronization for an access BS in step 1900, and performs an access and capability negotiation procedure with the access BS in step 1902. In step 1904, the MS starts an authentication procedure with an authenticator and an AAA through the access BS. In step 1906, the MS acquires information about an identifier of the access BS. In step 1908, the MS generates an authentication key to be used for its data exchange with the access BS using the acquired identifier of the access BS and Equation (2), and generates a data encryption key using the authentication key. The authentication key and the data encryption key may be referred to as 'security keys'. Thereafter, in step 1910, the MS performs a registration
procedure with the access BS, to set the access BS as a master BS of the cloud cell.

[204] Thereafter, in step 1912, the MS performs data exchange with the master BS. In step 1914, the MS performs a cloud cell update procedure for adding the master BS to the cloud cell member BS list, and then proceeds to step 1916 in FIG. 19b.

[205] In step 1916, the MS determines whether a master BS of the cloud cell is changed.

[206] If the master BS is changed, the MS proceeds to step 1918, and if the master BS is not changed, the MS proceeds to step 1932.

[207] In step 1918, the MS determines whether the master BS among the member BSs of the cloud cell is detected. If the master BS is deleted, the MS deletes the master BS from the cloud cell member BS list and deletes the currently used security keys used for its communication with the master BS, in step 1920. In step 1922, the MS terminates its communication with the master BS. In step 1924, the MS performs a cloud cell update procedure for adding a new master BS to the cloud cell member BS list, and generates security keys to be used for its communication with the new master BS. In other words, the MS generates a new authentication key using an identifier of the new master BS and Equation (2), and generates a new data encryption key using the new authentication key. Thereafter, in step 1926, the MS performs data exchange with the member BSs including the new master BS, using the new data encryption key.

[208] Even if the master BS is not deleted in step 1918, the MS deletes the currently used security keys used for its communication with the master BS in step 1928, because the master BS is changed to the new master BS. In step 1930, the MS performs a cloud cell update procedure for adding the new master BS to the cloud cell member BS list, and generates security keys to be used for its communication with the new master BS. In other words, the MS generates a new authentication key using an identifier of the new master BS and Equation (2), and generates a new data encryption key using the new authentication key. In step 1926, the MS performs data exchange with the member BSs of the cloud cell including the new master BS, using the new data encryption key.

[209] If it is determined in step 1916 that the master BS of the cloud cell is not changed, the MS determines in step 1932 whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell. If there is an added new BS, the MS performs a cloud cell update procedure for adding the new BS to the cloud cell member BS list in step 1934. In step 1936, the MS keeps the currently used security keys. In other words, in step 1926, the MS performs data exchange with the member BSs of the cloud cell including the new BS, using the data encryption key currently used for its communication with the master BS.

[210] If it is determined in step 1932 that there is a deleted member BS, the MS performs a cloud cell update procedure for deleting the deleted member BS from the cloud cell member BS list and terminates its communication with the deleted member BS, in step
1938. In step 1940, the MS keeps the security keys currently used for its communication with the master BS. In other words, in step 1926, the MS performs data exchange with the remaining member BSs except for the deleted member BS, using the data encryption key currently used for its communication with the master BS.

[211] FIGs. 20a and 20b illustrate an operation of a master BS in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

[212] Referring to FIG. 20a, the master BS performs an access and capability negotiation procedure for an MS in step 2000, and starts an authentication procedure for the MS in step 2002. In step 2004, the master BS receives an authentication context for the MS from an authenticator. The authentication context is an authentication key for the MS or a data encryption key for the MS. If the authentication context received in step 2004 is the authentication key, the master BS generates a data encryption key for the MS using the authentication key in step 2006. The authentication key and the data encryption key may be referred to as 'security keys'. Thereafter, the master BS performs a registration procedure for the MS in step 2008, and performs data exchange with the MS using the generated data encryption key in step 2010.

[213] Thereafter, in step 2012, the master BS performs a cloud cell update procedure for adding the master BS itself to a cloud cell member BS list, and then proceeds to step 2014 in FIG. 20b.

[214] Referring to FIG. 20b, the master BS determines in step 2014 whether the master BS of the cloud cell is changed. If the master BS is changed, the master BS proceeds to step 2016, and if the master BS is not changed, the master BS proceeds to step 2024.

[215] In step 2016, the master BS determines whether the master BS itself is deleted from the cloud cell member BS list. If the master BS is deleted from the cloud cell member BS list, the master BS terminates its communication with the MS in step 2018.

[216] If it is determined in step 2016 that the master BS is not deleted from the cloud cell member BS list, the master BS performs a cloud cell update procedure for adding the new master BS to the cloud cell member BS list and deletes its currently used security keys (i.e., the authentication key and data encryption key for the MS), in step 2020, and then proceeds to step 2022.

[217] In step 2024, the master BS determines whether there is an added new BS or a deleted member BS among the member BSs of the cloud cell, the master BS. If there is an added new BS, the master BS performs a cloud cell update procedure for adding the new BS to the cloud cell member BS list and keeps the security keys (i.e., the authentication key and data encryption key for the MS) currently used for its communication with the MS, in step 2026. In step 2022, the master BS performs data communication with the MS using the currently used data encryption key for the MS.
[218] If it is determined in step 2024 that there is a deleted member BS, the master BS performs a cloud cell update procedure for deleting the deleted member BS from the cloud cell member BS list and keeps the security keys (i.e., the authentication key and data encryption key for the MS) currently used for its communication with the MS, in step 2028. Thereafter, in step 2210, the master BS performs data communication with the MS using the currently used data encryption key for the MS.

[219] FIG. 21 illustrates an operation of a slave BS in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

[220] Referring to FIG. 21, the slave BS performs a cloud cell member subscription procedure with a master BS in step 2100, and performs data exchange with an MS in step 2102.

[221] In step 2104, the slave BS determines whether the slave BS itself is changed to the master BS of the cloud cell. If the slave BS is changed to the master BS, the slave BS operates as the changed master BS in step 2016. In other words, the slave BS receives an authentication context for the MS. The authentication context may be received from an authenticator, and corresponds to an authentication key or data encryption key for the MS, which is generated by an identifier of the slave BS and Equation (2). If the authentication context includes only the authentication key, the slave BS or the changed master BS generates a data encryption key for the MS using the received authentication key, in step 2018. From this time on, the slave BS serves as a master BS for the MS in the cloud cell.

[222] FIG. 22 illustrates an operation of an authenticator in a cloud cell-based wireless communication system according to the fourth embodiment of the present disclosure.

[223] Referring to FIG. 22, the authenticator starts an authentication procedure for an MS in step 2200, and generates an authentication key for the MS using identification information of a master BS of the cloud cell to which the MS belongs, and Equation (2), in step 2202.

[224] In step 2204, the authenticator delivers the authentication key to the master BS for the MS. The authenticator may generate a data encryption key for the MS using the authentication key and deliver the data encryption key to the master BS.

[225] Thereafter, in step 2206, the authenticator acquires the cloud cell update information through the master BS. Based on the cloud cell update information, the authenticator determines in step 2208 whether the master BS of the cloud cell is changed. If the master BS of the cloud cell is changed to a new master BS, the authenticator generates a new authentication key for the MS using Equation (2) and the identification information of the new master BS, which is acquired from the cloud cell update information, and generates a new data encryption key based on the new authentication key, in step 2210. The authenticator delivers the new authentication key or the new
data encryption key to the new master BS as a new authentication context for the MS.

Fifth Embodiment

FIG. 23 illustrates a signal flow diagram for managing security keys for an MS in a process of configuring a cloud cell in a cloud cell-based wireless communication system according to a fifth embodiment of the present disclosure.

Referring to FIG. 23, in step 2302, an MS 2300 performs a procedure for selecting a BS that provides a communication service. In the BS selection process, the MS 2300 selects a candidate BS for a slave BS constituting a cloud cell centered on the MS 2300. In step 2304, the MS 2300 sends an access request message to a master BS 2350 which was selected in step 2302. If information about the candidate BS is included in the access request message, the master BS 2350 performs a cloud cell member BS negotiation procedure for negotiating the slave BS corresponding to the candidate BS, as a member BS constituting the cloud cell, in step 2306. For example, a slave BS 2360 is assumed to be selected as the candidate BS by the MS 2300. The master BS 2350 adds the slave BS 2360 to a cloud cell member BS list through the cloud cell member BS negotiation procedure performed in step 2306. Thereafter, in step 2308, the master BS 2350 sends an access response message to the MS 2300 in response to the access request message from the MS 2300. The access response message includes information indicating that the slave BS 2360 is added to the cloud cell member BS list for the MS. Upon receiving the access response message, the MS 2300 adds the slave BS 2360 to the cloud cell member BS list for the MS 2300 in step 2310.

Thereafter, in step 2312, the MS 2300 performs an access network authentication and security key generation procedure with the master BS 2350 and an authenticator/AAA 2370. Specifically, the authenticator/AAA 2370 performs authentication for the MS 2300, and generates a security key for an access link, which is used to authenticate and encrypt the access link between the MS 2300 and the master BS 2350 under the involvement of the authenticator/AAA 2370.

In step 2314, the MS 2300 generates a cloud seed, which is an input value for generating a communication security key to be used for data exchange with member BSs in the cloud cell. In step 2316, the MS 2300 sends a cloud cell security context message including the cloud seed to the master BS 2350. The cloud cell security context message is encrypted using the security key for an access link between the master BS 2350 and the MS 2300, which is generated in step 2312.

Thereafter, in step 2318, the MS 2300 generates a communication security key to be used for data exchange with the member BSs in the cloud cell, by using the cloud seed as an input value. In other words, the MS 2300 generates a communication authentication key to be used for data exchange with the member BSs in the cloud cell, in accordance with Equation (1) by using the cloud seed as an input value, and generates a
communication data encryption key using the generated communication authentication key. Similarly, in step 2320, the master BS 2350 generates a communication authentication key to be used for data exchange in the cloud cell in accordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key.

[232] In step 2322, the master BS 2350 sends a cloud cell security context response message to the MS 2300. The cloud cell security context response message is encrypted using the communication security key generated in step 2320.

[233] In step 2324, the MS 2300 performs an access network authentication and security key generation procedure with the authenticator/AAA 2370 and the slave BS 2360. Specifically, in step 2324, a security key for an access link is generated, which is used to authenticate and encrypt the access link between the MS 2300 and the slave BS 2360. In step 2326, the MS 2300 sends a cloud cell security context message to the slave BS 2360. The cloud cell security context message includes the cloud seed that the MS 2300 generated in step 2318, and is encrypted using the security key for an access link, which was generated in step 2324. In step 2328, the slave BS 2360 generates a communication security key to be used for its data exchange with the member BSs in the cloud cell, by using the cloud seed as an input value. In other words, the slave BS 2360 generates a communication authentication key to be used for its data exchange in the cloud cell in accordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key. In step 2330, the slave BS 2360 sends a cloud cell security context response message to the MS 2300. The cloud cell security context response message is encrypted using the communication security key that is generated in step 2328.

[234] Thereafter, in step 2332, the MS 2300 performs data exchange with the member BSs in the cloud cell. The member BSs of the cloud cell, which handle the data exchanged with the MS 2300 by using the communication security key, may correspond to the master BS 2350, or to both the master BS 2350 and the slave BS 2360.

[235] FIG. 24 illustrates a signal flow diagram for managing security keys for an MS when a slave BS is added to a cloud cell, in a cloud cell-based wireless communication system according to the fifth embodiment of the present disclosure.

[236] Referring to FIG. 24, an MS 2400 performs data exchange with member BSs (i.e., a master BS 2440 and a first slave BS 2450) of the cloud cell in step 2402. In step 2404, the master BS 2440 is assumed to determine to add another adjacent BS, e.g., a second slave BS 2460, as a slave BS of the cloud cell. The criteria for determining to add a slave BS of the cloud cell corresponds to the signal strength measurement results for the MS 2400, and the cell loads for the master BS 2440 and the first slave BS 2450.
These are out of the scope of the present disclosure, so a detailed description thereof will be omitted. In step 2406, the master BS 2440 performs a cloud cell member BS negotiation procedure with the second slave BS 2460. Specifically, if the second slave BS 2460 is determined as a slave BS of the cloud cell for the MS 2400, the master BS 2440 sends a cloud cell update message to the MS 2400 in step 2408. In other words, the cloud cell update message includes information indicating that the second slave BS 2460 is added to the cloud cell member BS list for the MS 2400.

In step 2410, the master BS 2440 sends a cloud cell update message including information indicating that the second slave BS 2460 is added to the cloud cell member BS list for the MS 2400, to the first slave BS 2450 or a member BS of the cloud cell for the MS 2400. Then, in step 2412, the MS 2400 adds the second slave BS 2460 to its own cloud cell member BS list.

Thereafter, in step 2414, the MS 2400 performs an access network authentication and security key generation procedure with an authenticator/AAA 2470 and the second slave BS 2460. Specifically, in step 2414, a security key for an access link is generated, which is used to authenticate and encrypt the access link between the MS 2400 and the second slave BS 2460. In step 2416, the MS 2400 sends a cloud cell security context message including a cloud seed used in the cloud cell, to the second slave BS 2460. As an example, the cloud seed delivered to the second slave BS 2460 is assumed to be the previously generated cloud seed. However, as another example, if there is a deleted member BS among the member BSs of the cloud cell for the MS 2400, the MS 2400 generates a new cloud seed and delivers the new cloud seed to the member BSs.

The cloud cell security context message is encrypted using the security key for an access link, which is generated in step 2414.

In step 2418, the second slave BS 2460 generates a communication security key to be used for its data exchange in the cloud cell. In other words, the second slave BS 2460 generates a communication authentication key to be used for its data exchange in the cloud cell in accordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key. In step 2420, the second slave BS 2460 sends a cloud cell security context response message to the MS 2400. The cloud cell security context response message is encrypted using the communication security key generated in step 2418.

Thereafter, in step 2422, the MS 2400 exchanges data with the member BSs of the cloud cell. The member BSs of the cloud cell, which handle the data exchanged with the MS 2400 by using the communication security key, may correspond to the master BS 2440, or to all of the master BS 2440, the first slave BS 2450, and the second slave...
Sixth Embodiment

FIGs. 25a and 25b illustrate signal flow diagrams for managing security keys for an MS in a cloud cell-based wireless communication system according to a sixth embodiment of the present disclosure.

[Referring to FIGs. 25a and 25b, in step 2502, an MS 2500 performs a procedure for selecting a BS that provides a communication service. In the BS selection process, the MS 2500 selects a candidate BS for a slave BS constituting a cloud cell centered on the MS 2500. In step 2504, the MS 2500 sends an access request message to a master BS 2550 which was selected in step 2502. If information about the candidate BS is included in the access request message, the master BS 2550 performs a cloud cell member BS negotiation procedure for negotiating the slave BS corresponding to the candidate BS, as a member BS constituting the cloud cell, in step 2506. For example, a first slave BS 2560 is assumed to be selected as the candidate BS by the MS 2500. The master BS 2550 adds the first slave BS 2560 to a cloud cell member BS list through the cloud cell member BS negotiation procedure performed in step 2506. Thereafter, in step 2508, the master BS 2550 sends an access response message to the MS 2500 in response to the access request message from the MS 2500. The access response message includes information indicating that the first slave BS 2560 is added to the cloud cell member BS list for the MS. Upon receiving the access response message, the MS 2500 adds the first slave BS 2560 to the cloud cell member BS list for the MS 2500 in step 2510.

Thereafter, in step 2512, the MS 2500 performs an access network authentication and security key generation procedure with the master BS 2550 and an authenticator/AAA 2580. Specifically, the authenticator/AAA 2580 performs authentication for the MS 2500, and generates a security key for an access link, which is used to authenticate and encrypt the access link between the MS 2500 and the master BS 2550 under the involvement of the authenticator/AAA 2580.

In step 2514, the MS 2500 generates a cloud seed, which is an input value for generating a communication security key to be used for data exchange with member BSs in the cloud cell. In step 2516, the MS 2500 sends a cloud cell security context message including the cloud seed to the master BS 2550. The cloud cell security context message is encrypted using the security key for an access link between the master BS 2550 and the MS 2500, which is generated in step 2512.

Thereafter, in step 2518, the MS 2500 generates a communication security key to be used for data exchange with the member BSs in the cloud cell, by using the cloud seed as an input value. In other words, the MS 2500 generates a communication authentication key to be used for data exchange with the member BSs in the cloud cell, in ac-
cordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key. Similarly, in step 2520, the master BS 2550 generates a communication authentication key to be used for data exchange in the cloud cell in accordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key.

In step 2522, the master BS 2550 sends a cloud cell security context response message to the MS 2500. The cloud cell security context response message is encrypted using the communication security key generated in step 2520.

In step 2524, the master BS 2550 delivers the cloud seed received in step 2516 to the first slave BS 2560. The cloud seed is encrypted using the security key for an access link between the master BS 2550 and the first slave BS 2560. Then, in step 2526, the first slave BS 2560 generates a communication security key for data exchange in the cloud cell, by using the cloud seed as an input value. In other words, the first slave BS 2560 generates a communication authentication key to be used for its data exchange in the cloud cell in accordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key.

In step 2528, the first slave BS 2560 sends a cloud cell security context response message to the MS 2500. The cloud cell security context response message is encrypted using the communication security key that is generated in step 2526.

It is assumed that thereafter, during data transmission of the MS 2500, the master BS 2550 and the first slave BS 2560, the master BS 2550 determines to add another adjacent BS (i.e., a second slave BS 2570) as a slave BS of the cloud cell for the MS 2500. The criteria for determining to add a slave BS of the cloud cell corresponds to the signal strength measurement results for the MS 2500, and the cell loads for the master BS 2550 and the first slave BS 2560. These are out of the scope of the present disclosure, so a detailed description thereof will be omitted. In step 2530, the master BS 2550 performs a cloud cell member BS negotiation procedure with the second slave BS 2570. While performing step 2530, the master BS 2550 delivers the cloud seed received in step 2516 to the second slave BS 2570. In step 2532, the master BS 2550 sends a cloud cell update message to the MS 2500. In other words, the cloud cell update message includes information indicating that the second slave BS 2570 is added to the cloud cell member BS list for the MS.

In step 2534, the MS 2500 adds the second slave BS 2570 to its own cloud cell member BS list, and sends a cloud cell update response message to the master BS 2550. Then, in step 2536, the master BS 2550 sends a cloud cell update message including information indicating that the second slave BS 2570 is added to the cloud cell member BS list for the MS.
cell member BS list for the MS, to the first slave BS 2560 which is now a member BS of the cloud cell of the MS 2500.

[253] Thereafter, in step 2538, the second slave BS 2570 generates a communication security key to be used for data exchange in the cloud cell. In other words, the second slave BS 2570 generates a communication authentication key to be used for its data exchange in the cloud cell in accordance with Equation (1) by using the cloud seed as an input value, and generates a communication data encryption key using the generated communication authentication key. In step 2540, the second slave BS 2570 sends a cloud cell security context response message to the MS 2500. The cloud cell security context response message is encrypted using the communication security key generated in step 2538.

[254] The member BSs of the cloud cell, which handle the data exchanged with the MS 2500 by using the communication security key, may correspond to the master BS 2550, or to all of the master BS 2550, the first slave BS 2560, and the second slave BS 2570.

[255] In the fifth and six embodiments of the present disclosure, if a member BS constituting the cloud cell of an MS is deleted, the MS generates a new cloud seed, and may re-generate a communication security key to be used for its communication with the remaining cloud cell member BSs.

[256] Specifically, any member BS is assumed to be deleted. Then, a master BS sends a member BS deletion message to a MS, and the MS generates a new cloud seed. The MS transmits the new cloud seed to the master BS. The cloud seed is encrypted using a security key for an access link between the MS and the master BS. Upon receiving the new cloud seed, the master BS also re-generates a communication security key using the new cloud seed. Also, while performing a member BS update procedure with a slave BS, the master BS delivers the new cloud seed to the slave BS. The slave BS also re-generates a communication security used for its communication with the MS, using the new cloud seed.

[257] FIG. 26 illustrates a structure of an apparatus for managing security keys for authentication and data encryption in a cloud cell-based wireless communication system according to embodiments of the present disclosure.

[258] Referring to FIG. 26, a security key management apparatus 2600 for authentication and data encryption may include a communication unit 2610, a security key generator 2620, a cloud cell member BS update unit 2630, and a controller 2640.

[259] The security key management apparatus 2600 is included in at least one of an MS, a master BS, a slave BS and an authenticator provided by the first to sixth embodiments of the present disclosure, and performs the above-described authentication procedure.

[260] An operation of the security key management apparatus 2600 according to em-
bodiments of the present disclosure will be described below.

First, the security key management apparatus 2600 is assumed to operate as an MS based on the first to sixth embodiments of the present disclosure.

If the security key management apparatus 2600 operates in accordance with the first embodiment of the present disclosure, the communication unit 2610 receives a cloud seed from an authenticator oran AAA. The cloud seed is a value that is selected by a rule shared between the MS and the authenticator or the AAA. If the controller 2640 detects the reception of the cloud seed, the security key generator 2620 generates an authentication key using the cloud seed and Equation (1) under control of the controller 2640.

The cloud cell member BS update unit 2630 manages a cloud cell member BS list that includes member BSs in the cloud cell to which the MS belongs. If a member BS in the cloud cell is deleted or added, a procedure for updating the cloud cell member BS list is performed. Also, if a master BS in the cloud cell is changed, information about the master BS in the cloud cell member BS list is updated.

If there is a member BS deleted from the cloud cell member BS list, the controller 2640 controls the communication unit 2610 to receive a new cloud seed. The controller 2640 controls the security key generator 2620 to generate an authentication key using the new cloud seed and Equation (1).

If the security key management apparatus 2600 operates in accordance with the second or fourth embodiment of the present disclosure, the security key generator 2620 generates an authentication key using an identifier of the master BS and Equation (2). The communication unit 2610 exchanges data with (i.e., transmits and receives data to/from) the master BS and slave BSs using a data encryption key that is generated based on the authentication key.

If the master BS is changed or replaced, the communication unit 2610 receives an identifier of the changed or replaced master BS. Upon detecting the change, the controller 2640 controls the security key generator 2620 to generate a new authentication key using the identifier of the changed master BS and Equation (2). Further, the controller 2640 controls the communication unit 2610 to exchange data with the member BSs including the new master BS, using a new data encryption key generated based on the new authentication key.

The cloud cell member BS update unit 2630 operates as it does in the first embodiment.

If the security key management apparatus 2600 operates in accordance with the third embodiment of the present disclosure, the controller 2640 controls the security key generator 2620 to generate an authentication key individually for each of the master BS and the slave BSs of the current cloud cell. In other words, under control of the
controller 2640, the security key generator 2620 generates an authentication key to be used for communication with the master BS, using an identifier of the master BS and Equation (3). Further, the security key generator 2620 generates an authentication key to be used for communication with a pertinent slave BS, using an identifier of each of slave BSs and Equation (3).

Thereafter, during communication with the master BS under control of the controller 2640, the communication unit 2610 exchanges data with the master BS using an encryption key that is generated based on the authentication key which is generated using an identifier of the master BS. Further, during communication with a slave BS, the communication unit 2610 exchanges data with the slave BS using an encryption key that is generated based on the authentication key which is generated using an identifier of the slave BS.

If a master BS or a slave BS, an identifier of which was used for generation of an encryption key, is deleted, the controller 2640 deletes the encryption key. The cloud cell member BS update unit 2630 operates as it does in the first embodiment.

If the security key management apparatus 2600 operates in accordance with the fifth or sixth embodiment of the present disclosure, the security key generator 2620 generates a cloud seed. Further, the security key generator 2620 generates a communication security key using the cloud seed. In the fifth embodiment of the present disclosure, the communication unit 2610 delivers the cloud seed to member BSs. If a particular member BS is deleted from the current member BSs, the security key generator 2620 generates a new cloud seed. Then, the security key generator 2620 generates a communication security key using the new cloud seed.

Second, the security key management apparatus 2600 is assumed to operate as a master BS based on the first to sixth embodiments of the present disclosure.

If the security key management apparatus 2600 operates in accordance with the first embodiment of the present disclosure, and the master BS is changed, then the controller 2640 determines whether the master BS itself is deleted from the cloud cell member BS list. If the master BS is deleted from the cloud cell member BS list, the controller 2640 terminates its communication with an MS, and the remaining operations are the same as those of the controller of the MS. The cloud cell member BS update unit 2630 and the communication unit 2610 are the same in operation as those of the MS, except that the communication unit 2610 communicates with the MS.

If the security key management apparatus 2600 operates in accordance with the second to fourth embodiments of the present disclosure, the security key management apparatus 2600 operates the same as that of the MS, except that the communication unit 2610 communicates with the MS.
If the security key management apparatus 2600 operates in accordance with the fifth embodiment of the present disclosure, the communication unit 2610 receives a cloud seed that is generated by and provided from an MS. Then, the security key generator 2620 generates a communication security key using the cloud seed.

If the security key management apparatus 2600 operates in accordance with the sixth embodiment of the present disclosure, the communication unit 2610 receives a cloud seed that is generated by and provided from an MS, and delivers the cloud seed to other member BSs. Then, the security key generator 2620 generates a communication security key using the cloud seed.

Third, the security key management apparatus 2600 is assumed to operate as a slave BS based on the first to sixth embodiments of the present disclosure.

If the security key management apparatus 2600 operates in accordance with the first to sixth embodiments of the present disclosure, the cloud cell member BS update unit 2630 further performs a subscription procedure to the current master BS and cloud cell member BSs, and its operation of managing a cloud cell member BS list including the member BSs in the cloud cell is the same as that of the MS and the master BS.

The controller 2640 also operates the same as that of the MS and the master BS. However, in the case of the third embodiment, if the controller 2640 recognizes that the slave BS itself is set as a master BS, the controller 2640 controls the security key generator 2620 to generate a security key, using a new authentication context received through the communication unit 2610.

If the security key management apparatus 2600 operates in accordance with the fifth and embodiments of the present disclosure, the controller 2640 controls the security key generator 2620 to generate a communication security key using a cloud seed received from an MS.

Fourth, if the security key management apparatus 2600 operates as an authenticator based on the first to fourth embodiments of the present disclosure, the security key management apparatus 2600 is the same in operation as that of the MS and the master BS based on the first to fourth embodiments of the present disclosure, except that the communication unit 2610 delivers an authentication key or a data encryption key generated in accordance with the pertinent embodiment, to the master BS.

If the security key management apparatus 2600 operates in accordance with the fifth and sixth embodiment of the present disclosure, the security key management apparatus 2600 involves only in generation of a security key for an access link between an MS and a member BS, without involving in generation of a communication security key like in other embodiments.

As is apparent from the foregoing description, the present disclosure provides a method for managing security keys for authentication and data encryption in a cloud
cell-based wireless communication system supporting data transmission and reception between an MS and multiple BSs serving the MS, thereby ensuring reliable and seamless communication between the MS and the BSs.

Although the present disclosure has been described with an exemplary embodiment, various changes and modifications may be suggested to one skilled in the art. It is intended that the present disclosure encompass such changes and modifications as fall within the scope of the appended claims.
Claims

[Claim 1] A method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system, the method comprising:
acquiring a first authentication key by performing an authentication procedure for the communication authentication in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS; and
communicating with at least one member BS using a first encryption key that is generated using the first authentication key.

[Claim 2] The method of claim 1, wherein the acquiring a first authentication key includes generating the first authentication key using a first seed;
wherein the first seed is a value that is selected by a rule predefined between the MS and an Authentication, Authorization and Accounting server (AAA), selected by a rule predefined between the MS and an authenticator for managing an authentication procedure, or received from the AAA or the authenticator.

[Claim 3] The method of claim 2, further comprising:
if there is a deleted member BS among the member BSs, selecting a second seed by a rule predefined between the MS and the AAA or the authenticator, or receiving the second seed from the AAA or the authenticator;
generating a second authentication key using the second seed; and
generating a second encryption key using the second authentication key.

[Claim 4] The method of claim 1, wherein acquiring the first authentication key comprises:
generating a seed for generating the first authentication key
delivering the seed to the master BS;
generating the first authentication key using the seed; and
generating a new seed, if there is a deleted member BS among the member BSs.

[Claim 5] A method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system, the method comprising:
acquiring an authentication context for the MS by performing an authentication procedure for the communication authentication with the
MS in a cloud cell having member Base Stations (BSs) that include a master BS and at least one slave BS for providing a service to the MS; and communicating with the MS using a first encryption key that is acquired from the authentication context.

[Claim 6] The method of claim 5, further comprising: if the authentication context includes a first authentication key, generating the first encryption key using the first authentication key, wherein the first authentication key is generated using a first seed by the MS and an Authentication, Authorization and Accounting server (AAA) or an authenticator for managing the authentication procedure, and the first seed is a value that is selected by a rule predefined between the MS and the AAA, selected by a rule predefined between the MS and the authenticator, or a value that is received from the MS.

[Claim 7] The method of claim 6, further comprising: if there is a deleted member BS among the member BSs, receiving a second authentication key from the authenticator; and generating a second encryption key using the second authentication key, and delivering the second encryption key to remaining slave BSs except for the deleted member BS, wherein the second authentication key is generated using a second seed by the MS and the AAA or the authenticator, and the second seed is a value that is selected to be different from the first seed by a rule predefined between MS and the AAA or the authenticator, or a value that is newly generated by and received from the MS.

[Claim 8] A method for managing a security key for communication authentication with a Mobile Station (MS) in a communication system, the method comprising: performing a member Base Station (BS) subscription procedure for a cloud cell with a master BS in the cloud cell having member BSs that include the master BS and at least one slave BS for providing a service to the MS, and receiving an authentication context for an MS included in the cloud cell from the master BS; and in response to the authentication context including a first authentication key, generating a first encryption key using the first authentication key and communicating with the MS using the first encryption key.

[Claim 9] The method of claim 8, further comprising: if the authentication context includes a seed generated by the MS,
generating the first authentication key using the seed, wherein the seed is received directly from the MS or received from the master BS and wherein if there is a deleted member BS among the member BSs, a new seed value is generated by and received from the MS.

[Claim 10]  A Mobile Station (MS) configured to manage a security key for communication authentication with the MS in a communication system, the MS implemented by the method described in any one of claims 1 to 4.

[Claim 11]  A master Base Station (BS) configured to manage a security key for communication authentication with a Mobile Station (MS) in a communication system, the master BS implemented by the method described in any one of claims 5 to 7.

[Claim 12]  A slave Base Station (BS) configured to manage a security key for communication authentication with a Mobile Station (MS) in a communication system, the slave implemented by the method described in any one of claims 8 to 9.
[Fig. 4a]

START

ACQUIRE SYNCHRONIZATION FOR ACCESS BS

PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE

START AUTHENTICATION PROCEDURE

ACQUIRE CLOUD SEED

GENERATE SECURITY KEY

PERFORM REGISTRATION PROCEDURE

EXCHANGE DATA WITH MASTER BS

UPDATE CLOUD CELL

A
[Fig. 4b]
[Fig. 5a]

1. START
2. PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE FOR MS
3. START AUTHENTICATION PROCEDURE FOR MS
4. ACQUIRE AUTHENTICATION CONTEXT FOR MS
5. GENERATE SECURITY KEY FOR MS
6. PERFORM REGISTRATION PROCEDURE FOR MS
7. EXCHANGE DATA WITH MS
8. PERFORM CLOUD CELL UPDATE PROCEDURE

End of process
[Fig. 5b]

- Acquire new authentication context for MS
- Generate new encryption key for MS
- Deliver new authentication context for MS to slave BSS
- Exchange data with MS
- Continue to use currently used security key
- DELIVER AUTHENTICATION CONTEXT FOR MS TO SLAVE BSS
- CONTINUE TO USE CURRENTLY USED SECURITY KEY
- TERMINATE COMMUNICATION WITH MS
- DELETE MEMBERS OF CLOUD CELL DELETED OR MODIFIED
- DELETION OF MASTER BS IS CLOUD CELL IS CHANGED
- YES
- NO
- MEMBER BS OF CLOUD CELL ADDED OR MODIFIED
- DELETION OF MASTER BS IS CLOUD CELL IS CHANGED
- YES
- NO
- Master BS is deleted from cloud
- Master BS is changed
[Fig. 9a]

START

ACQUIRE SYNCHRONIZATION FOR ACCESS BS

PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE

START AUTHENTICATION PROCEDURE

ACQUIRE MASTER BS INFORMATION

GENERATE SECURITY KEY

PERFORM REGISTRATION PROCEDURE

PERFORM DATA EXCHANGE WITH MASTER BS

CLOUD CELL UPDATE PROCEDURE

A
[Fig. 14a]

START

ACQUIRE SYNCHRONIZATION FOR ACCESS BS

PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE

START AUTHENTICATION PROCEDURE

ACQUIRE INFORMATION ABOUT IDENTIFICATION OF ACCESS BS

GENERATE SECURITY KEY

PERFORM REGISTRATION PROCEDURE

PERFORM DATA EXCHANGE WITH MASTER BS

CLOUD CELL UPDATE PROCEDURE

A
[Fig. 15a]

START

PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE FOR MS

START AUTHENTICATION PROCEDURE FOR MS

ACQUIRE AUTHENTICATION CONTEXT FOR MS

PERFORM REGISTRATION PROCEDURE FOR MS

PERFORM REGISTRATION PROCEDURE FOR MS

PERFORM DATA EXCHANGE WITH MS

CLOUD CELL UPDATE PROCEDURE
[Fig. 19a]

START

ACQUIRE SYNCHRONIZATION FOR ACCESS BS

PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE

START AUTHENTICATION PROCEDURE

ACQUIRE IDENTIFIER INFORMATION OF ACCESS BS

GENERATE SECURITY KEY

PERFORM REGISTRATION PROCEDURE

PERFORM COMMUNICATION WITH MASTER BS

CLOUD CELL UPDATE PROCEDURE

A
[Fig. 20a]

START

PERFORM ACCESS AND CAPABILITY NEGOTIATION PROCEDURE FOR MS

START AUTHENTICATION PROCEDURE FOR MS

ACQUIRE AUTHENTICATION CONTEXT FOR MS

GENERATE DATA ENCRYPTION KEY FOR MS

PERFORM REGISTRATION PROCEDURE FOR MS

PERFORM DATA EXCHANGE WITH MS

CLOUD CELL UPDATE PROCEDURE

A
[Fig. 21]

START

PERFORM CLOUD CELL MEMBER SUBSCRIPTION PROCEDURE WITH MASTER BS

PERFORM COMMUNICATION WITH MS

MASTER BS OF CLOUD CELL IS CHANGED?

NO

YES

ACQUIRE AUTHENTICATION CONTEXT

USE ENCRYPTION KEY FOR MS

[Fig. 22]

START

START AUTHENTICATION PROCEDURE FOR MS

GENERATE AUTHENTICATION CONTEXT FOR MS

DELIVER AUTHENTICATION CONTEXT TO MASTER BS

ACQUIRE CLOUD CELL UPDATE INFORMATION

MASTER BS OF CLOUD CELL IS CHANGED?

NO

YES

DELIVER AUTHENTICATION CONTEXT FOR NEW MS TO MASTER BS
[Fig. 23]

2300  2350  2360  2370

MS  MASTER BS  SLAVE BS  AUTHENTICATOR / AAA

BS SELECTION PROCEDURE

2304  ACCESS REQUEST  MEMBER BS NEGOTIATION PROCEDURE

2308  ACCESS RESPONSE

ADD SLAVE BS 2360 TO MEMBER BS LIST  

2310  AUTHENTICATION AND SECURITY KEY GENERATION PROCEDURE

2312  ACCESS LINK

2314  CLOUD CELL SECURITY CONTEXT

2316  GENERATE CLOUD SEED

2318  CLOUD CELL SECURITY CONTEXT RESPONSE

2320  GENERATE COMMUNICATION SECURITY KEY

2322  CLOUD CELL SECURITY CONTEXT

2324  AUTHENTICATION AND SECURITY GENERATION PROCEDURE

2326  ACCESS LINK

2328  GENERATE COMMUNICATION SECURITY KEY

2330  CLOUD CELL SECURITY CONTEXT RESPONSE

2332  DATA EXCHANGE WITH MEMBER BSS OF CLOUD CELL
A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04(2009.01)i, H04W 12/06(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W 12/04; H04L 9/14; H04L 9/08; H04W 4/08; H04L 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: communication authentication, group/member, encryption key, generate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>KR 10-2011-0055866 A (AJOU UNIVERSITY INDUSTRY-ACADEMIC COOPERATION FOUNDATION) 26 May 2011</td>
<td>1,5,8,10-12</td>
</tr>
<tr>
<td>A</td>
<td>See the abstract; paragraphs [0017]-[0024]; claims 1-5 and figure 1.</td>
<td>2-4,6-7,9</td>
</tr>
<tr>
<td>A</td>
<td>US 2008-0130902 A1 (F00 KUNE DENIS et al.) 05 June 2008</td>
<td>1-12</td>
</tr>
<tr>
<td>A</td>
<td>KR 10-2010-0047099 A (LG ELECTRONICS INC.) 07 May 2010</td>
<td>1-12</td>
</tr>
<tr>
<td></td>
<td>See the abstract; paragraphs [0091]-[0110]; claims 1-7 and figure 3.</td>
<td></td>
</tr>
</tbody>
</table>

Date of the actual completion of the international search 28 March 2013 (28.03.2013)

Date of mailing of the international search report 28 March 2013 (28.03.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
BOK, Sang Moon
Telephone No. 82-42-481-8345

Form PCT/ISA/210 (second sheet) (July 2009)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>KR 10-20 11-0055866 A</td>
<td>26.05.2011</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>US 2008-0 130902 A1</td>
<td>05.06.2008</td>
<td>GB 24496 17 A</td>
<td>26.11.2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 7936878 B2</td>
<td>03.05.2011</td>
</tr>
<tr>
<td>KR 10-20 10-0047099 A</td>
<td>07.05.2010</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>