

DESCRIPTION

MOBILE COMMUNICATION METHOD, MOBILE STATION AND RADIO BASE
STATION

5 Technical Field

[0001]

The present invention relates to a mobile communication method, a mobile station and a radio base station.

10 Background Art

[0002]

In the LTE (Long Term Evolution) type mobile communication system specified by the 3GPP, a mobile station UE is configured to perform a connection re-establishment procedure, when detecting a radio link failure (RLF) in an RRC connection. Specifically, in the connection re-establishment procedure, the mobile station is configured to perform cell selection processing and to transmit an "RRC Connection Re-establishment Request" through a common control channel (CCCH) to the selected cell.

[0003]

Here, the mobile station UE is configured to select, in the cell selection processing, a cell which meets a certain propagation level and to which the mobile station UE has an access right.

Summary of the Invention**Problems to be Solved by the Present Invention**

[0004]

In the connection re-establishment procedure, a radio base station eNB that manages the selected cell is configured to verify an "RRC Connection Re-establishment Request" on the basis of "second verification information (short MAC-I)" contained in the "RRC Connection Re-establishment Request" to avoid the following problems.

[0005]

- The radio base station eNB cannot distinguish "RRC Connection Re-establishment Requests" from each other, when the mobile stations UE that have detected an RLF in different cells transmit the "RRC Connection Re-establishment Requests" containing the same C-RNTI (Cell-Radio Network Temporary Identifier) and the same PCI (Physical Cell ID) to the selected cell.

[0006]

- The radio base station eNB cannot distinguish an "RRC Connection Re-establishment Request" from others, when a mobile station UE of a malicious user transmits the "RRC Connection Re-establishment Request" containing a C-RNTI and a PCI which are randomly set.

[0007]

The "short MAC-I" can be used to verify the credibility of the "RRC Connection Re-establishment Request". In other words, the "short MAC-I" can serve as a checksum for performing a tampering check of the "RRC Connection Re-establishment Request".

[0008]

In the LTE type mobile communication system, a tampering check of an RRC message on a dedicated control channel (DCCH)

is provided by a PDCP layer function. Specifically, the system is configured to generate a checksum (MAC-I) for the RRC message in a PDCP layer, and to transmit the checksum attached to the PDCP header.

5 [0009]

Meanwhile, the LTE type mobile communication system is configured to transmit an "RRC Connection Re-establishment Request" through the common control channel (CCCH).

[0010]

10 Furthermore, the LTE type mobile communication system has no PDCP layer function for the common control channel (CCCH).

[0011]

In consideration of the above circumstances, it is
15 apparent that the "short MAC-I" to be contained in the "RRC Connection Re-establishment Request" cannot be generated under the current LTE specifications.

[0012]

The present invention was made in consideration of the
20 foregoing problem. It is an object of the present invention to provide a mobile communication method, a mobile station and a radio base station which are capable of generating "short MAC-I" to be contained in an "RRC Connection Re-establishment Request".

25

Means for Solving the Problems

[0013]

A first aspect of the present invention is summarized as a mobile communication method including the steps of:

generating, at a mobile station, first verification information by use of a first key, a first parameter and an algorithm for "Integrity Protection"; generating, at the mobile station, second verification information by extracting
5 predetermined bits of the first verification information; and performing, at the mobile station, cell selection processing, and transmitting, from the mobile station to a radio base station that manages the selected cell, an RRC-PDU for RRC connection re-establishment request through a common control
10 channel, upon detection of a radio link failure in an RRC connection, the second verification information being set in the RRC-PDU for RRC connection re-establishment request.

[0014]

In the first aspect, the first parameter can be "COUNT",
15 "bearer ID" and "direction (DL/UL)"; and a physical cell ID and a C-RNTI can be set in the RRC-PDU for RRC connection re-establishment request.

[0015]

A second aspect of the present invention is summarized
20 as a mobile communication method including the steps of: generating, at a radio base station, first verification information using a first key, a first parameter and an algorithm for "Integrity Protection"; generating, at the radio base station, second verification information by extracting
25 predetermined bits of the first verification information; performing, at the mobile station, cell selection processing, and transmitting, from the mobile station to the radio base station that manages the selected cell, an RRC-PDU for RRC connection re-establishment request through a common control

channel, upon detection of a radio link failure in an RRC connection, the second verification information being set in the RRC-PDU for RRC connection re-establishment request; and verifying, at the radio base station, the RRC-PDU for RRC connection re-establishment request received from the mobile station by use of the second verification information.

[0016]

In the second aspect, the first parameter can be "COUNT", "bearer ID" and "direction (DL/UL)".

10 [0017]

A third aspect of the present invention is summarized as a mobile station including: a first verification information generator unit configured to generate first verification information by use of a first key, a first parameter and an algorithm for "Integrity Protection"; a second verification information generator unit configured to generate second verification information by extracting predetermined bits of the first verification information; and a transmitter unit configured to, upon detection of a radio link failure in an RRC connection, perform cell selection processing and transmit an RRC-PDU for RRC connection re-establishment request through a common control channel to a radio base station that manages the selected cell, the second verification information being set in the RRC-PDU for RRC connection re-establishment request.

25 [0018]

In the third aspect, the first parameter can be "COUNT", "bearer ID" and "direction (DL/UL)"; and a physical cell ID and a C-RNTI can be set in the RRC-PDU for RRC connection re-establishment request.

[0019]

In the third aspect, the transmitter unit can be configured to set, as the physical cell ID, a physical cell ID of a cell in which a radio link failure has occurred during the RRC connection, and to set, as the C-RNTI, a C-RNTI used by the mobile station UE in the cell in which the radio link failure has occurred.

[0020]

In the third aspect, the first verification information generator unit can be configured to generate the first verification information for a PDU in which a physical cell ID of a cell in which a radio link failure has occurred during the RRC connection, a C-RNTI used by the mobile station UE in the cell in which the radio link failure has occurred, and a cell ID of the selected cell are set.

[0021]

A fourth aspect of the present invention is summarized as a radio base station including: a first verification information generator unit configured to generate first verification information by use of a first key, a first parameter and an algorithm for "Integrity Protection"; a second verification information generator unit configured to generate second verification information by extracting predetermined bits of the first verification information; and a verification unit configured to verify, by use of the second verification information, an RRC-PDU for RRC connection re-establishment request received from a mobile station through a common control channel.

[0022]

In the fourth aspect, the first parameter can be "COUNT", "bearer ID" and "direction (DL/UL)".

[0023]

In the fourth aspect, the radio base station can further
5 include: a notification unit configured to notify, to an neighbor radio base station, the second verification information by use of a handover preparation signal.

[0024]

In the fourth aspect, the first verification information
10 generator unit can be configured to extract a physical cell ID and a C-RNTI from the RRC-PDU for RRC connection re-establishment request received from the mobile station, to generates a PDU containing the extracted physical cell ID and C-RNTI as well as a (notification) cell ID of a cell that has
15 received the RRC-PDU, and to generate the first verification information for the PDU.

[0025]

In the fourth aspect, the radio base station can be configured to verify the RRC-PDU for RRC connection
20 re-establishment request, by determining whether or not the second verification information held after being received through the handover preparation signal from an neighbor radio base station corresponds to second verification information contained in the RRC-PDU for RRC connection re-establishment
25 request.

Effect of the Invention

[0026]

As described above, the present invention can provide a

mobile communication method, a mobile station and a radio base station, which are capable of generating "short MAC-I" contained in an "RRC Connection Re-establishment Request".

5 Brief Description of the Drawings

[0027]

[Fig.1] Fig. 1 is an overall configuration diagram of a mobile communication system according to a first embodiment of the present invention.

10 [Fig.2] Fig. 2 is a diagram showing a protocol stack between a mobile station and a radio base station according to the first embodiment of the present invention.

[Fig.3] Fig. 3 is a sequence diagram showing an operation of generating "short MAC-I" in the mobile station according to
15 the first embodiment of the present invention.

[Fig.4] Fig. 4 is a sequence diagram showing a connection re-establishment procedure in the mobile communication system according to the first embodiment of the present invention.

[Fig.5] Fig. 5 is a sequence diagram showing a connection
20 re-establishment procedure in the mobile communication system according to the first embodiment of the present invention.

[Fig.6] Fig. 6 is a sequence diagram showing a connection re-establishment procedure in the mobile communication system according to the first embodiment of the present invention.

25

Embodiment Mode for carrying out the Invention

[0028]

(Mobile communication system according to the first embodiment of the present invention)

With reference to Figs. 1 to 6, a mobile communication system according to a first embodiment of the present invention will be described. The LTE system is applied to the mobile communication system according to this embodiment.

5 [0029]

As shown in Fig. 1, the mobile communication system according to this embodiment includes an exchange MME and multiple radio base stations eNB#1 to eNB#n.

[0030]

10 Fig. 2 shows a protocol stack between a mobile station UE and the radio base station eNB according to this embodiment.

[0031]

Specifically, each of the mobile station UE and the radio base station eNB according to this embodiment includes an RRC layer function, a PDCP layer function, an RLC layer function, a MAC layer function and a physical layer function.

15 [0032]

Moreover, in the LTE type mobile communication system, three kinds of radio bearers for C-plane called "SRBs: Signalling Radio Bearers" (SRB0, SRB1 and SRB2) are specified.

20 [0033]

The "SRB0" is a radio bearer for a common control channel (CCCH). In an uplink, the "SRB0" is used for transmitting the "RRC Connection Establishment Request" and the "RRC Connection Re-establishment Request". In a downlink, the "SRB0" is used for transmitting "RRC Connection Establishment", "RRC Connection Reject", "RRC Connection Re-establishment" and "RRC Connection Re-establishment Reject".

25 [0034]

In general, "C-RNTI", "PCI" and "short MAC-I" are specified as information elements contained in the "RRC Connection Re-establishment Request".

[0035]

5 Here, the "C-RNTI" includes 16 bits, and is specified as a "UE-ID" used by the mobile station UE in a serving cell until just before detection of an RLF. Moreover, the "PCI" includes 9 bits, and is specified as an ID of a serving cell connected to the mobile station UE until just before detection of an RLF.
10 Furthermore, the "short MAC-I" is assumed to include 15 or 16 bits.

[0036]

Specifically, the "SRB0" is used for transmitting a message in a situation where a sender and a receiver cannot be
15 uniquely specified.

[0037]

Moreover, since the "SRB0" is the radio bearer for the common control channel (CCCH), the "SRB0" has no PDCP layer. Therefore, neither an "Integrity Protection" function nor a
20 "Ciphering" function can be applied to the "SRB0".

[0038]

Furthermore, the "SRB1" is a radio bearer for a dedicated control channel (DCCH), and is used for transmitting all RRC messages (including NAS messages connected to the RRC messages)
25 which are not transmitted by the "SRB0".

[0039]

Note that the "Integrity Protection" function and the "Ciphering" function can be applied to the "SRB1".

[0040]

Moreover, the "SRB2" is a radio bearer for a dedicated control channel (DCCH), and is applied to "NAS Direct Transfer".

[0041]

5 The "SRB2" has lower priority than the "SRB1", and the "Integrity Protection" function and the "Ciphering" function can be applied to the "SRB2".

[0042]

10 Moreover, in the LTE type mobile communication system, a radio bearer for U-plane called a "DRB: Data Radio Bearer" is specified.

[0043]

15 The "DRB" is a radio bearer for a dedicated traffic channel (DTCH), and a necessary number of DRBs are provided depending on communication services. Note that, since the "DRB" has a PDCP layer, the "Ciphering" function can be applied to the "DRB" within the PDCP layer.

[0044]

20 With reference to Fig. 3, a description will be given below of an operation of generating the "short MAC-I (second verification information)" in the mobile station UE and the radio base station eNB.

[0045]

25 As shown in Fig. 3, in Step S1001, the RRC layer function generates an RRC-PDU for "RRC Connection Re-establishment Request" containing a predetermined "short MAC-I".

[0046]

For example, the RRC layer function may set, as the predetermined "short MAC-I", a "short MAC-I" in which all bits

have a value of "0".

[0047]

Moreover, the RRC layer function is configured to set a "C-RNTI" and a "PCI", which are known to both the mobile station
5 UE and the radio base station eNB, in the RRC-PDU for "RRC Connection Re-establishment Request".

[0048]

For example, the RRC layer function may set values currently used by the mobile station UE as the "C-RNTI" and the
10 "PCI" in the RRC-PDU for "RRC Connection Re-establishment Request".

[0049]

Moreover, the RRC layer function may set a predetermined number of higher order or lower order bits in the "short MAC-I" to a "PCI" of a target cell and pad the rest with "0" in the
15 RRC-PDU for "RRC Connection Re-establishment Request".

[0050]

In the case of the mobile station UE, a "PCI" of a cell selected by cell selection after an RLF detection (i.e., a cell
20 to which the mobile station UE actually transmits the "RRC Connection Re-establishment Request") can be set as the "PCI" of the target cell.

[0051]

On the other hand, in the case of the radio base station eNB, a "PCI" of a cell which performs "HO preparation" (i.e., a cell which is likely to receive the "RRC Connection Re-establishment Request" from the mobile station UE) can be
25 set as the "PCI" of the target cell.

[0052]

In Step S1002, the RRC layer function transmits the generated RRC-PDU for "RRC Connection Re-establishment Request" to the PDCP layer function.

[0053]

5 In Step S1003, the PDCP layer function generates "MAC-I (first verification information)" from the received RRC-PDU for "RRC Connection Re-establishment Request" by using a predetermined algorithm (e.g., an algorithm for "Integrity Protection" that is currently in use)

10 [0054]

To be more specific, the PDCP layer function calculates the "MAC-I" by inputting a first key $K_{\text{RRC_IP}}$ and three parameters "COUNT (32 bits)", "bearer ID (8 bits)" and "direction (DL/UL)" to the currently-used algorithm for "Integrity Protection".

15 [0055]

Here, the first key $K_{\text{RRC_IP}}$ is calculated by use of an incremented master key $K_{\text{eNB}}[n+1]$.

[0056]

20 The master key K_{eNB} is updated at the time of handover from the current master key $K_{\text{eNB}}[n]$ to the next master key $K_{\text{eNB}}[n+1]$ to be used after the handover. The incremented master key $K_{\text{eNB}}[n+1]$ to be used after the next handover can be used to calculate the first key $K_{\text{RRC_IP}}$ used for calculation of the "short MAC-I".

25 [0057]

Moreover, the PDCP layer function uses a "bearer ID" for the "SRB1" or the "SRB0" as the "bearer ID". Note that, since the "SRB0" is the radio bearer for the common control channel (CCCH), the "SRB0" normally has no "bearer ID". However, for

the above purpose, the "bearer ID" is also specified for the "SRB0".

[0058]

In terms of security, the PDCP layer function needs to
5 avoid securing multiple RRC-PDUs by use of the same master key K_{eNB} and the same parameters (particularly, "COUNT"). In this regard, the PDCP layer function can use the "bearer ID" for the "SRB0" as the "bearer ID" to avoid complexity. When the PDCP layer function uses the "bearer ID" for the "SRB1" as the
10 "bearer ID", there occurs a trouble such that "COUNT=0" can not be used in the original RRC-PDU of the "SRB1".

[0059]

In addition, the PDCP layer function sets the "COUNT" to "0". However, the PDCP layer function need not increment the
15 "COUNT" by the "MAC-I" calculation operation.

[0060]

The "COUNT" may be expressed by being divided into "HFN" representing higher order bits and "SN" representing lower order bits.

20 [0061]

The PDCP layer function inserts only the "SN" portion into an actual header, and only manages the "HFN" portion.

[0062]

Furthermore, the PDCP layer function sets the
25 "direction" to "UL".

[0063]

In Step S1004, the PDCP layer function transmits the generated "MAC-I" to the RRC layer function.

[0064]

In Step S1005, the RRC layer function extracts predetermined bits (e.g., 16 LSBs, 16 MSBs or the like) of the received "MAC-I", and sets the bits as the "short MAC-I" in the RRC-PDU for "RRC Connection Re-establishment Request".

5 [0065]

Next, with reference to Figs. 4 to 6, a description will be given of a connection re-establishment procedure in the mobile communication system according to this embodiment.

[0066]

10 Firstly, with reference to Fig. 4, a description will be given of an example where the connection re-establishment procedure is successfully performed.

[0067]

As shown in Fig. 4, an RRC connection is established
15 between the mobile station UE and the radio base station eNB and an S1 connection is established between the radio base station eNB and the exchange MME. Here, the mobile station UE and the radio base station eNB calculate "short MAC-I" by performing the operations shown in Fig. 3, in Steps S2001 and
20 S2002.

[0068]

The mobile station UE and the radio base station eNB may calculate the "short MAC-I" upon completion of a handover procedure, upon completion of a connection re-establishment
25 procedure, upon detection of an RLF, or the like.

[0069]

In Step S2003, the mobile station UE detects an RLF during the RRC connection described above. For example, the mobile station UE detects the RLF in any of the following cases.

[0070]

- When an RSRP (Reference Signal Received Power) in the RRC connection falls below a predetermined threshold for a predetermined period of time

5 • When a random access procedure is not successfully performed

- When the handover procedure fails

Thereafter, the mobile station UE performs cell selection processing in Step S2004, and sends the selected cell
10 (or to the radio base station eNB that manages the selected cell) the "RRC Connection Re-establishment Request" containing the "C-RNTI", "PCI" and "short MAC-I" through the common control channel.

[0071]

15 The radio base station eNB manages a serving cell of the mobile station UE, and previously holds "UE context (short MAC-I)" of the mobile station UE. For this reason, in Step S2006, the radio base station eNB verifies the received "RRC Connection Re-establishment Request" by comparing the
20 previously-held "short MAC-I" with the "short MAC-I" contained in the "RRC Connection Re-establishment Request".

[0072]

In the example of Fig. 4, since the validity of the "RRC Connection Re-establishment Request" is successful, the radio
25 base station eNB transmits "RRC Connection Re-establishment" to the mobile station UE in Step S2007.

[0073]

In Step S2008, the mobile station UE transmits "RRC Connection Re-establishment Complete" to the radio base

station eNB.

[0074]

In Step S2009, the radio base station eNB transmits "RRC Connection Reconfiguration" to the mobile station UE. In Step
5 S2010, the mobile station UE transmits "RRC Connection Reconfiguration Complete" to the radio base station eNB.

[0075]

Secondly, with reference to Fig. 5, a description will be given of an example where the connection re-establishment
10 procedure fails.

[0076]

As shown in Fig. 5, an RRC connection is established between the mobile station UE and the radio base station eNB#1 and an S1 connection is established between the radio base
15 station eNB#1 and the exchange MME. Here, the mobile station UE and the radio base station eNB#1 calculate "short MAC-I" by performing the operations shown in Fig. 3, in Steps S3001 and S3002.

[0077]

20 In Step S3003, the mobile station UE detects an RLF during the RRC connection described above.

[0078]

Thereafter, the mobile station UE performs cell selection processing in Step S3004, and sends the selected cell
25 (or the radio base station eNB#2 that manages the selected cell) the "RRC Connection Re-establishment Request" containing the "C-RNTI", "PCI" and "short MAC-I" through the common control channel.

[0079]

The radio base station eNB#2 does not manage a serving cell of the mobile station UE, and does not previously hold "UE context (short MAC-I)" of the mobile station UE. For this reason, in Step S3006, the radio base station eNB#2 is unable
5 to verify the "RRC Connection Re-establishment Request".
[0080]

As a result, in Step S3007, the radio base station eNB#2 transmits "RRC Connection Re-establishment Reject" to the mobile station UE.
10 [0081]

In Step S3008, the RRC connection between the mobile station UE and the radio base station eNB#1 is released, so that the mobile station UE transits to an idle state.
[0082]

15 As described above, to succeed in the connection re-establishment procedure, the radio base station eNB that manages the cell selected by the mobile station UE needs to previously hold the "UE context" of the mobile station UE.
[0083]

20 Here, if the cell selected by the mobile station UE is an original serving cell of the mobile station UE, the connection re-establishment procedure is successfully performed since the radio base station eNB previously holds the "UE context" of the mobile station UE (see Fig. 4).
[0084]

25 On the other hand, in order to successfully carry out the connection re-establishment procedure even if the cell selected by the mobile station UE is not an original serving cell of the mobile station UE, the radio base station eNB that

manages the cell needs to prepare the "UE context" of the mobile station UE in advance.

[0085]

The "UE context" can be prepared by carrying out an "HO
5 Preparation procedure".

[0086]

In the handover procedure, a handover-source radio base station S-eNB can transfer the "UE context" of the mobile station UE to a handover-target radio base station T-eNB by the
10 "HO Preparation".

[0087]

Moreover, in case of an RLF detection, the handover-source radio base station S-eNB can transmit the "HO Preparation" containing the "UE context" of the mobile station
15 UE to one or more neighbor radio base stations any time, even when the handover procedure is not intended.

[0088]

Thirdly, with reference to Fig. 6, a description will be given of operations of the mobile communication system
20 according to this embodiment in the case described above.

[0089]

As shown in Fig. 6, an RRC connection is established between the mobile station UE and the radio base station eNB#1 and an S1 connection is established between the radio base station eNB#1 and the exchange MME. Here, the mobile station
25 UE and the radio base station eNB#1 calculate "short MAC-I" by performing the operations shown in Fig. 3, in Steps S4001 and S4002.

[0090]

Here, in Step S4003, the radio base station eNB#1 transmits "H0 Preparation" containing "UE context (short MAC-I)" of the mobile station UE to the neighbor radio base station eNB#2.

5 [0091]

In Step S4004, after acquisition of the "UE context (short MAC-I)" of the mobile station UE, the radio base station eNB#2 transmits "H0 Preparation Ack" showing that effect to the mobile station UE.

10 [0092]

In Step S4005, the mobile station UE detects an RLF during the RRC connection described above.

[0093]

Thereafter, the mobile station UE performs cell selection processing in Step S4006, and sends the selected cell (or the radio base station eNB#2 that manages the selected cell) the "RRC Connection Re-establishment Request" containing the "C-RNTI", "PCI" and "short MAC-I" through the common control channel.

20 [0094]

The radio base station eNB#2 previously holds the "UE context (short MAC-I)" of the mobile station UE. For this reason, in Step S4008, the radio base station eNB#2 verifies the received "RRC Connection Re-establishment Request" by comparing the previously-held "short MAC-I" with the "short MAC-I" contained in the "RRC Connection Re-establishment Request".

[0095]

In the example of Fig. 6, since the validity of the "RRC

Connection Re-establishment Request" is successful, the radio base station eNB#2 transmits "RRC Connection Re-establishment" to the mobile station UE in Step S4009.

[0096]

- 5 In Step S4010, the mobile station UE transmits "RRC Connection Re-establishment Complete" to the radio base station eNB#2.

[0097]

- The radio base station eNB#2 transmits "S1 Path Switch" to the exchange MME in Step S4011, and also transmits "RRC Connection Reconfiguration" to the mobile station UE in Step S4012.

[0098]

- In Step S4013, the mobile station UE transmits "RRC Connection Reconfiguration Complete" to the radio base station eNB#2. In Step S4014, the exchange MME transmits "S1 Path Switch Ack" to the radio base station eNB#2.

[0099]

- As a result, the connection re-establishment procedure described above is successfully performed, so that an RRC connection is established between the mobile station UE and the radio base station eNB#2, and an S1 connection is established between the radio base station eNB#2 and the exchange MME.

[0100]

- 25 (Advantageous effect of the mobile communication system according to the first embodiment of the present invention)

 The mobile communication system according to the first embodiment of the present invention enables calculation of the "short MAC-I" contained in the "RRC Connection

Re-establishment Request" transmitted through the common control channel having no PDCP layer function.

[0101]

Moreover, according to the mobile communication system
5 according to the first embodiment of the present invention, the radio base station eNB that has received "short MAC-I" by the "HO Preparation" does not need to calculate the "short MAC-I". Therefore, the radio base station eNB can verify the "RRC Connection Re-establishment Request" by simply comparing the
10 "short MAC-I" using the RRC layer function.

[0102]

Furthermore, according to the mobile communication system according to the first embodiment of the present invention, the validity of the "RRC Connection
15 Re-establishment Request" can be successful even when the algorithm for "Integrity Protection" to be used (in the LTE system, it is possible to select between two types, AES and Snow3G) varies between the handover-source radio base station S-eNB and the handover-target radio base station T-eNB during
20 handover.

[0103]

(Modified Example)

The radio base station eNB#1 may also be configured not to transmit "HO Preparation" that does not contain "short
25 MAC-I". However, note that such "HO Preparation" contains "C-RNTI" and "PCI".

[0104]

In such a case, firstly, the RRC layer function of the neighbor radio base station eNB#2 extracts the "C-RNTI" and

"PCI" contained in the "RRC Connection Re-establishment Request" received from the mobile station UE, and temporarily creates an RRC-PDU for "RRC Connection Re-establishment Request" on the basis of the extracted "C-RNTI" and "PCI".

5 [0105]

Here, the RRC layer function of the neighbor radio base station eNB#2 sets all values of the "short MAC-I" to "0" in the RRC-PDU for "RRC Connection Re-establishment Request".

[0106]

10 Alternatively, the RRC layer function of the neighbor radio base station eNB#2 sets higher order or lower order bits in the "short MAC-I" to a "PCI" (a "PCI" under the radio base station eNB#2 that has received the "RRC Connection Re-establishment Request" from the mobile station UE) and sets
15 the rest to "0" in the RRC-PDU for "RRC Connection Re-establishment Request".

[0107]

Secondly, the RRC layer function of the neighbor radio base station eNB#2 transmits the generated RRC-PDU for "RRC
20 Connection Re-establishment Request" to the PDCP layer function of the neighbor radio base station eNB#2.

[0108]

Thirdly, the PDCP layer function of the neighbor radio base station eNB#2 calculates "MAC-I (which may also be called
25 X-MAC due to "MAC-I" on the receiving side)". Here, the first key $K_{\text{RRC_IP}}$, "COUNT", "bearer ID" and "direction" are handled in the same manner as the calculation operation in the mobile station UE.

[0109]

Fourthly, the RRC layer function of the neighbor radio base station eNB#2 extracts 16 LSBs or 16 MSBs of the "MAC-I" received from the PDCP function (which is called "short X-MAC").

5 [0110]

The RRC layer function of the neighbor radio base station eNB#2 checks if the "short X-MAC" corresponds to the "short MAC-I" contained in the "RRC Connection Re-establishment Request" received from the mobile station UE. Thus, the RRC layer function evaluates the credibility of the "RRC Connection Re-establishment Request".

[0111]

Note that, if a "Prepare procedure" is not performed for the neighbor radio base station eNB#2, the neighbor radio base station eNB#2 does not have the first key K_{RRC_IP} since the neighbor radio base station eNB#2 does not previously hold "UE context". Therefore, the neighbor radio base station eNB#2 transmits "RRC Connection Re-establishment Reject" without calculating "short X-MAC".

20 [0112]

Note that operation of the above described mobile station UE and the radio base station eNB may be implemented by means of hardware, a software module executed by a processor, or a combination of both.

25 [0113]

The software module may be provided in any type of storage medium such as an RAM (Random Access Memory), a flash memory, a ROM (Read Only Memory), an EPROM (Erasable Programmable ROM), an EEPROM (Electrically Erasable and Programmable ROM), a

register, a hard disk, a removable disk, or a CD-ROM.

[0114]

The storage medium is connected to the processor so that the processor can read and write information from and to the storage medium. Also, the storage medium may be integrated into the processor. Also, the storage medium and the processor may be provided in an ASIC. The ASIC may be provided in the mobile station UE and the radio base station eNB. Also, the storage medium and the processor may be provided in the mobile station UE and the radio base station eNB as a discrete component.

[0115]

Hereinabove, the present invention has been described in detail using the above embodiment; however, it is apparent to those skilled in the art that the present invention is not limited to the embodiment described herein. Modifications and variations of the present invention can be made without departing from the spirit and scope of the present invention defined by the description of the scope of claims. Thus, what is described herein is for illustrative purpose, and has no intention whatsoever to limit the present invention.

CLAIMS

1. A mobile communication method comprising the steps of:
generating, at a mobile station, first verification
5 information by use of a first key, a first parameter and an
algorithm for "Integrity Protection";
generating, at the mobile station, second verification
information by extracting predetermined bits of the first
verification information; and
10 performing, at the mobile station, cell selection
processing, and transmitting, from the mobile station to a
radio base station that manages the selected cell, an RRC-PDU
for RRC connection re-establishment request through a common
control channel, upon detection of a radio link failure in an
15 RRC connection, the second verification information being set
in the RRC-PDU for RRC connection re-establishment request.
2. The mobile communication method according to claim 1,
wherein
20 the first parameter is "COUNT", "bearer ID" and
"direction (DL/UL)"; and
a physical cell ID and a C-RNTI are set in the RRC-PDU
for RRC connection re-establishment request.
- 25 3. A mobile communication method comprising the steps of:
generating, at a radio base station, first verification
information using a first key, a first parameter and an
algorithm for "Integrity Protection";
generating, at the radio base station, second

21
verification information by extracting predetermined bits of the first verification information;

performing, at the mobile station, cell selection processing, and transmitting, from the mobile station to the radio base station that manages the selected cell, an RRC-PDU for RRC connection re-establishment request through a common control channel, upon detection of a radio link failure in an RRC connection, the second verification information being set in the RRC-PDU for RRC connection re-establishment request; and
10 verifying, at the radio base station, the RRC-PDU for RRC connection re-establishment request received from the mobile station by use of the second verification information.

4. The mobile communication method according to claim 3,
15 wherein
the first parameter is "COUNT", "bearer ID" and "direction (DL/UL)".

5. A mobile station comprising:
20 a first verification information generator unit configured to generate first verification information by use of a first key, a first parameter and an algorithm for "Integrity Protection";
a second verification information generator unit
25 configured to generate second verification information by taking out predetermined bits of the first verification information; and
a transmitter unit configured to, upon detection of a radio link failure in an RRC connection, perform cell selection

processing and transmit an RRC-PDU for RRC connection re-establishment request through a common control channel to a radio base station that manages the selected cell, the second verification information being set in the RRC-PDU for RRC
5 connection re-establishment request.

6. The mobile station according to claim 5, wherein
the first parameter is "COUNT", "bearer ID" and
"direction (DL/UL)"; and
10 a physical cell ID and a C-RNTI are set in the RRC-PDU
for RRC connection re-establishment request.

7. The mobile station according to any one of claims 5 and
6, wherein
15 the transmitter unit is configured to set, as the
physical cell ID, a physical cell ID of a cell in which a radio
link failure has occurred during the RRC connection, and to set,
as the C-RNTI, a C-RNTI used by the mobile station UE in the
cell in which the radio link failure has occurred.

20

8. A radio base station comprising:
a first verification information generator unit
configured to generate first verification information by use
of a first key, a first parameter and an algorithm for
25 "Integrity Protection";
a second verification information generator unit
configured to generate second verification information by
extracting predetermined bits of the first verification
information; and

a verification unit configured to verify, by use of the second verification information, an RRC-PDU for RRC connection re-establishment request received from a mobile station through a common control channel.

5

9. The radio base station according to claim 8, wherein the first parameter is "COUNT", "bearer ID" and "direction (DL/UL)".

10 10. The radio base station according to any one of claims 8 and 9, further comprising:

a notification unit configured to notify, to an neighbor radio base station, the second verification information by use of a handover preparation signal.

15

11. The mobile station according to any one of claims 5 to 7, wherein

the first verification information generator unit is configured to generate the first verification information for a PDU in which a physical cell ID of a cell in which a radio link failure has occurred during the RRC connection, a C-RNTI used by the mobile station UE in the cell in which the radio link failure has occurred, and a cell ID of the selected cell are set.

25

12. The radio base station according to any one of claims 8 to 10, wherein

the first verification information generator unit is configured to extract a physical cell ID and a C-RNTI from the

RRC-PDU for RRC connection re-establishment request received from the mobile station, to generates a PDU containing the extracted physical cell ID and C-RNTI as well as a (notification) cell ID of a cell that has received the RRC-PDU,
5 and to generate the first verification information for the PDU.

13. The radio base station according to claim 10, wherein the radio base station is configured to verify the RRC-PDU for RRC connection re-establishment request, by
10 determining whether or not the second verification information held after being received through the handover preparation signal from an neighbor radio base station corresponds to second verification information contained in the RRC-PDU for RRC connection re-establishment request.