Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2725461 C 2013/10/08

(11)(21) 2 725 461

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2009/06/19
(87) Date publication PCT/PCT Publication Date: 2009/12/23
(45) Date de délivrance/Issue Date: 2013/10/08
(85) Entrée phase nationale/National Entry: 2010/11/02
(86) N° demande PCT/PCT Application No.: JP 2009/061227
(87) N° publication PCT/PCT Publication No.: 2009/154277
(30) Priorité/Priority: 2008/06/20 (JP2008-162617)

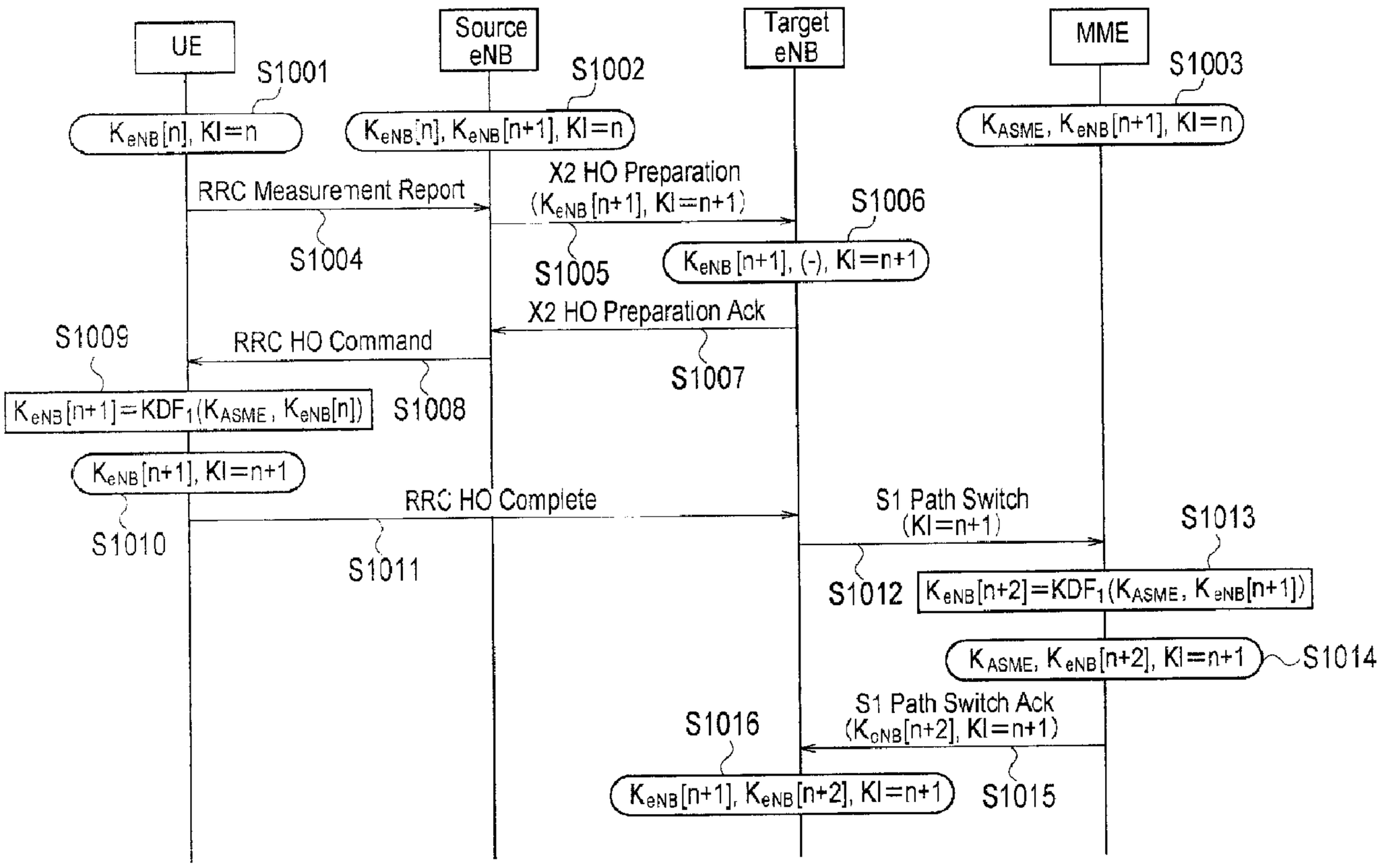
(51) Cl.Int./Int.Cl. *H04W 12/04* (2009.01), *H04L 9/08* (2006.01), *H04W 36/08* (2009.01), *H04W 36/10* (2009.01)

(72) Inventeurs/Inventors:
HAPSARI, WURI ANDARMAWANTI, JP;
IWAMURA, MIKIO, JP;
ZUGENMAIER, ALF, JP

(73) Propriétaire/Owner:
NTT DOCOMO, INC., JP

(74) Agent: OYEN WIGGS GREEN & MUTALA LLP

(54) Titre : PROCEDE DE COMMUNICATION MOBILE ET STATION MOBILE
(54) Title: MOBILE COMMUNICATION METHOD AND MOBILE STATION



(57) Abrégé/Abstract:
The present invention relates to a mobile communication method in which a mobile station performs a handover from a handover source radio base station to a handover target radio base station. The mobile communication method includes the steps of: (A) acquiring, at the handover target radio base station, from the handover source radio base station or a switching center, a key for calculating a first key for generating a certain key used in a communication between the handover target radio base station and the mobile station; and (B) acquiring, at the handover target radio base station, from the switching center, a second key for calculating a first key for generating a certain key used in a communication between a next handover target radio base station and the mobile station.

Abstract

The present invention relates to a mobile communication method in which a mobile station performs a handover from a handover source radio base station to a handover target radio base station. The mobile communication method includes the steps of: (A) acquiring, at the handover target radio base station, from the handover source radio base station or a switching center, a key for calculating a first key for generating a certain key used in a communication between the handover target radio base station and the mobile station; and (B) acquiring, at the handover target radio base station, from the switching center, a second key for calculating a first key for generating a certain key used in a communication between a next handover target radio base station and the mobile station.

DESCRIPTION

Title of the invention: MOBILE COMMUNICATION METHOD AND MOBILE STATION

Technical Field

[0001]

The present invention relates to a mobile communication method for communicating between a mobile station and a radio base station using a certain key.

Background Art

[0002]

A conventional mobile communication system of the LTE (Long Term Evolution) scheme specified by the 3GPP is configured to communicate between a mobile station UE and a radio base station eNB, by using a certain key.

[0003]

The certain key includes, for example, a key K_{RRC_Ciph} used for "Ciphering" in an RRC protocol, which is a C-plane protocol between the mobile station UE and the radio base station eNB (Access Stratum, AS), a key K_{RRC_IP} used for "Integrity Protection" in the RRC protocol, and a key K_{UP_Ciph} used for "Ciphering" in a U-plane protocol between the mobile station UE and the radio base station eNB (Access Stratum, AS) and the like. These certain keys are generated using a first key K_{eNB}.

[0004]

Using the same key as any of the certain keys and the first key K_{eNB} for a long time is not preferable, because it makes the

system's security vulnerable. For this reason, a procedure for updating such a certain key or a first key K_{eNB} during handover is devised by the 3GPP.

[0005]

Here, operations of a handover target radio base station (Target eNB) acquiring a first key K_{eNB}** used for generating a certain key in the handover procedure of the mobile station UE are described referring to Fig. 12.

[0006]

As shown in Fig. 12, first, a handover source radio base station (Source eNB) generates an intermediate key K_{eNB}* based on a stored first key K_{eNB}, a parameter "Next Hop", a parameter "Handover Type" representing the parameter type and a parameter "Target PCI" representing the identification information of a handover target cell.

[0007]

Secondly, the handover source radio base station (Source eNB) transmits the generated intermediate key K_{eNB}* to the handover target radio base station (Target eNB).

[0008]

Thirdly, the handover target radio base station (Target eNB) generates, based on the the received intermediate key K_{eNB}* and "C-RNTI (Cell Radio Network Temporay ID)" allocated by the handover target cell, a first key K_{eNB}** used for generating a certain key in the handover target radio station (Target eNB).

Disclosure of the Invention

Problem to be Solved by the Invention

[0009]

However, as described above, in the handover procedure of the conventional mobile communication system, there is a problem that both handover source radio base station (Source eNB) and handover target radio base station (Target eNB) have to use a plurality of parameters and functions to generate a first key K_{eNB}** used in the handover target radio station (Target eNB).

[0010]

In particular, there is a problem that the handover source radio base station (Source eNB) and the handover target radio base station (Target eNB) have to use K_{eNB} conversion functions (Key Derivation Function, KDF) different in parameters for each of the stations, and the mobile station UE also has be provided with the KDFs, whereby the procedure is complicated.

[0011]

Furthermore, it is cumbersome that K_{eNB} needs to be updated according to PCI (Physical Cell ID) of the handover target radio base station.

[0012]

Furthermore, there is a restriction in flexibly changing the allocation of C-RNTI, since K_{eNB} needs to be updated according to C-RNTI.

[0013]

Accordingly, the present invention has been made in view of the above-described problems, and an object of the present invention is to provide a mobile communication method with which a first key used in a handover target radio base station (Target eNB) can be generated through a simplified procedure.

Solution to Problem

[0014]

A first aspect of the present invention is summarized as a mobile communication method in which a mobile station performs a handover from a handover source radio base station to a handover target radio base station, the mobile communication method including the steps of: (A) acquiring, at the handover target radio base station, from the handover source radio base station or a switching center, a key for calculating a first key for generating a certain key used in a communication between the handover target radio base station and the mobile station; and (B) acquiring, at the handover target radio base station, from the switching center, a second key for calculating a first key for generating a certain key used in a communication between a next handover target radio base station and the mobile station.

[0015]

In the first aspect, the mobile communication method can further include the step of: (C) updating, at the mobile station, upon receiving a handover command signal from the handover source radio base station, a first key for generating a certain key used in a communication between the handover source radio base station and the mobile station, to the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station.

[0016]

In the first aspect, in the step (C), the mobile station can update the first key for generating the certain key used in the communication between the handover source radio base

station and the mobile station, to the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station, based on a parameter included in the handover command signal.

[0017]

In the first aspect, the step (C) can include the steps of: (C1) generating, at the mobile station, the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station based on the parameter included in the handover command signal, when the parameter is incremented; and (C2) generating, at the mobile station, the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station based on the first key for generating the certain key used in the communication between the handover source radio base station and the mobile station, when the parameter included in the handover command signal is not incremented.

[0018]

In the first aspect, in the step (C1), when the parameter included in the handover command signal is incremented, the mobile station can update, based on the parameter, a second key for calculating the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station, and can generate the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station based on the updated second key.

[0019]

In the first aspect, the parameter can be a key index (KI)

[0020]

In the first aspect, the mobile communication method car further include the step of: (D) storing, at the mobile station, the received parameter.

[0021]

A second aspect of the present invention is summarizec as a radio base station which functions as a handover target radio base station when a mobile station performs a handover from a handover source radio base station to the handover target radio base station, the radio base station including: a first acquiring unit configured to acquire, from the handover source radio base station, a key for calculating a first key for generating a certain key used in a communication between the handover target radio base and the mobile station; and a second acquiring unit configured to acquire, from a switching center a second key for calculating a first key for generating a certain key used in a communication between a next handover target radio base station and the mobile station.

[0022]

A third aspect of the present invention is summarized as a mobile station which performs a handover from a handover source radio base station to a handover target radio base station, the mobile station including: a key updating unit configured to update, upon receiving a handover command signal from the handover source radio base station, a first key for generating a certain key used in a communication between the handover source radio base station and the mobile station, to a first key for generating a certain key used in a communicatio

between the handover target radio base station and the mobile station.

[0023]

In the third aspect, the key updating unit can be configured to update, based on a parameter included in the handover command signal, the first key for generating the certain key used in the communication between the handover source radio base station and the mobile station, to the first key for generating the certain key used in the communication between the handover target radio base and the mobile station.

[0024]

In the third aspect, the key updating unit can be configured to generate, when the parameter included in the handover command signal is incremented, the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station, based on the parameter; and the key updating unit can be configured to generate, when the parameter included in the handover command signal is not incremented, the first key for generating the certain key used in the communication between the handover target radio base station and the mobile station, based on the first key for generating the certain key used in the communication between the handover source radio base station and the mobile station.

[0025]

In the third aspect, the key updating unit can be configured to update, when a parameter included in the handover command signal is incremented, a second key for calculating the first key for generating the certain key used in the

communication between the handover target radio base station and the mobile station, based on the parameter, and to generate the first key for generating certain keys used in the communication between the handover target radio base station and the mobile station, based on the updated second key.

[0026]

In the third aspect, the parameter can be KI.

[0027]

In the third aspect, the key updating unit can be configured to store the received parameter.

EFFECT OF THE INVENTION

[0028]

As described above, according to the present invention, it is possible to provide a mobile communication method with which a first key used in a handover target radio base station (Target eNB) can be generated through a simplified procedure.

Brief Description of the Drawings

[0029]

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

[Fig. 2] Fig. 2 is a diagram showing an example of a hierarchical structure and a calculation procedure of a key used in the mobile communication system according to the first embodiment of the present invention.

[Fig. 3] Fig. 3 is a sequence diagram showing an initial establishment procedure in the mobile communication system

according to the first embodiment of the present invention.

[Fig. 4] Fig. 4 is a sequence diagram showing an X2 handover procedure in the mobile communication system according to the first embodiment of the present invention.

[Fig. 5] Fig. 5 is a sequence diagram showing an S1 handover procedure in the mobile communication system according to the first embodiment of the present invention.

[Fig. 6] Fig. 4 is a sequence diagram showing an Intra-eNB handover procedure in the mobile communication system according to the first embodiment of the present invention.

[Fig. 7] Fig. 7 is a sequence diagram showing an S1 handover procedure in a mobile communication system according to a second embodiment of the present invention.

[Fig. 8] Fig. 8 is a diagram showing an exemplary hierarchical structure and calculation procedure of keys used in a mobile communication system according to a third embodiment of the present invention.

[Fig. 9] Fig. 9 is a sequence diagram showing an X2 handover procedure in the mobile communication system according to the third embodiment of the present invention.

[Fig. 10] Fig. 10 is a sequence diagram showing an S1 handover procedure in the mobile communication system according to the third embodiment of the present invention.

[Fig. 11] Fig. 11 is a sequence diagram showing an Intra-eNB handover procedure in the mobile communication system according to the third embodiment of the present invention.

[Fig. 12] Fig. 12 is a diagram showing an exemplary calculation procedure of keys used in a mobile communication system according to a conventional technique.

Best Modes for Carrying Out the Invention

[0030]

(Mobile Communication System According to First Embodiment of the Present Invention)

A mobile communication system according to a first embodiment of the present invention is described referring to Fig. 1 to Fig. 6.

[0031]

The mobile communication system according to this embodiment is a mobile communication system to which the LTE scheme is applied, and includes a plurality of switching centers MME#1, MME#2, ... and a plurality of radio base stations eNB#11, eNB#12, eNB#21, eNB#22, ...

[0032]

For example, a mobile station UE is configured to communicate, in the cell #111 under the control of the radio base station eNB#11, with the radio base station eNB#11 using a certain key described above.

[0033]

Furthermore, in the handover procedure of the mobile station UE, the handover target radio base station (for example, the radio base station eNB#12) is configured to acquire first keys $K_{eNB}[n+1]$, $K_{eNB}[n+2]$ and the like for generating certain keys used in a communication with the mobile station UE, without using an intermediate key K_{eNB}^* generated by the handover source radio base station (for example, the radio base station eNB#11).

[0034]

Fig. 2 shows an example of the hierarchical structure and

the calculation procedure of a key used in the mobile communication system according to this embodiment (that is, a key used to calculate the certain key).

[0035]

As shown in Fig. 2, a key K_{RRC_IP} used for "Integrity Protection" in the RRC protocol, a key K_{RRC_Ciph} used for "Ciphering" in the RRC protocol, and a key K_{UP_Ciph} used for "Ciphering" in the U-plane of AS are generated using a first key $K_{eNB}[n]$.

[0036]

The first key $K_{eNB}[n]$ is calculated by using a master key K_{ASME} from the formulas given below.

[0037]

$$K_{eNB}[0]=KDF_0\ (K_{ASME},\ NAS\ SN)$$

$$K_{eNB}[n+1]=KDF_1\ (K_{ASME},\ K_{eNB}[n]),\ (n\geq 0)$$

Here, the master key K_{ASME} is known only to the mobile station UE and the switching center MME, but must not be known to the radio base station eNB.

[0038]

Furthermore, the NAS SN is a sequence number (SN) of a NAS protocol which is the C-plane protocol between the mobile station UE and the switching center MME (Non Access Stratum, NAS).

[0039]

Hereafter, operations of the mobile communication system according to this embodiment are described referring to Fig. 3 to Fig. 6.

[0040]

First, an initial establishment procedure in the mobile

communication system according to this embodiment is described referring to Fig. 3.

[0041]

As shown in Fig. 3, before starting the initial establishment procedure, the mobile station UE holds K_{ASME} (in step S101), the radio base station eNB holds no keys used for generating certain keys (in step S102), and the switching center MME holds K_{ASME} (in step S103).

[0042]

In step S104, the mobile station UE transmits "RRC Connection Request (RRC connection request signal)" to the radio base station eNB, and in step S105, the radio base station eNB transmits "RRC Connection Setup (RRC connection setup signal)" to the mobile station UE.

[0043]

In step S106, the mobile station UE transmits "RRC Connection Setup Complete (RRC connection setup complete signal)" to the radio base station eNB and "NAS Service Request (NAS service request signal)" including "NAS SN (sequence number of NAS)".

[0044]

In step S107, the radio base station eNB transmits "S1 Initial UE Message" and "NAS Service Request (NAS service request signal)" including "NAS SN" to the switching center MME.

[0045]

In step S108, the switching center MME calculates $K_{eNB}[0]$ and $K_{eNB}[1]$ from the formulas given below.

[0046]

$$K_{eNB}[0]=KDF_0\ (K_{ASME},\ NAS\ SN)$$

$K_{eNB}[1]=KDF_1\ (K_{ASME},\ K_{eNB}[0])$

In step S109, the switching center MME transmits "S1 Initial UE Context Setup (initial UE context setup signal)" including $K_{eNB}[0]$, $K_{eNB}[1]$ and "NAS SN" to the radio Base station eNB. Furthermore, "KI (=0)" may or may not be included in this message.

[0047]

In step S110, the radio base station eNB transmits "RRC Security Mode Command (RRC security mode command signal)" including "NAS SN" to the mobile station UE.

[0048]

In step S111, the mobile station UE calculates $K_{eNB}[0]$ from the formula given below.

[0049]

$K_{eNB}[0]=KDF_0\ (K_{ASME},\ NAS\ SN)$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[0]$, and uses them in subsequent AS communications.

[0050]

In this stage, the mobile station UE holds $K_{eNB}[0]$, and "KI (=0)" (in step S114), the radio base station eNB holds $K_{eNB}[0]$, $K_{eNB}[1]$ and "KI (=0)" (in step S113), and the switching center MME holds K_{ASME}, $K_{eNB}[1]$ and "KI (=0)" (in step S112).

[0051]

If "KI (=0)" is not included in the "S1 Initial UE Context Setup (initial UE context setup signal)" in step S109, the radio base station eNB may initialize "KI (=0)" automatically by receiving the above message.

[0052]

Furthermore, the radio base station eNB calculates K_{RRC_IP}, K_{RRC_ciph} and K_{UP_ciph} based on $K_{eNB}[0]$, and uses them in subsequent AS communications.

[0053]

In step S115, the radio base station eNB transmits "RRC Connection Reconfiguration (RRC connection reconfiguration signal)" to the mobile station UE.

[0054]

In steps S116 and S117, the mobile station UE respectively transmits "RRC Security Mode Command Complete (RRC security mode command complete signal)" and "RRC Connection Reconfiguration Complete (RRC connection reconfiguration complete signal)" to the radio base station eNB.

[0055]

In step S118, the radio base station eNB transmits "S1 Initial UE Context Setup Complete (initial UE context setup complete signal)" to the switching center MME.

[0056]

Through the above procedure, all keys necessary for protection of AS communication (integrity protection and ciphering) are prepared at the mobile station UE, the radio base station eNB and the switching center MME.

[0057]

Secondly, an X2 handover procedure (handover procedure between different radio base stations) in the mobile communication system according to this embodiment is described referring to Fig. 4.

[0058]

As shown in Fig. 4, before starting the X2 handover

procedure, the mobile station UE holds $K_{eNB}[n]$ and "KI (=n)" (in step S1001), the handover source radio base station (Source eNB) holds $K_{eNB}[n]$, $K_{eNB}[n+1]$ and "KI (=n)" (in step S1002), and the switching center MME holds K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n)" (in step S1003).

[0059]

In step S1004, if predetermined conditions are satisfied, the mobile station UE transmits "RRC Measurement Report (measurement report signal)" to the handover source radio base station (Source eNB).

[0060]

In step S1005, the handover source radio base station (Source eNB) transmits "X2 HO Preparation (handover preparation signal)" including $K_{eNB}[n+1]$ and "KI (=n+1)" to the handover target radio base station (Target eNB).

[0061]

In step S1006, the handover target radio base station (Target eNB) stores the received $K_{eNB}[n+1]$ and "KI (=n+1)", and in step S1007, transmits "X2 HO Preparation Ack (handover preparation acknowledge signal)" to the handover source radio base station (Source eNB).

[0062]

Furthermore, the radio base station eNB calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1]$ and uses them in subsequent AS communications.

[0063]

In step S1008, the handover source radio base station (Source eNB) transmits "RRC HO Command (handover command signal)" to the mobile station UE.

[0064]

In step S1009, the mobile station UE calculates $K_{eNB}[n+1]$ from the formula given below, and in step S1010, stores $K_{eNB}[n+1]$ and "KI (=n+1)".

[0065]

$$K_{eNB}[n+1] = KDF_1 (K_{ASME}, K_{eNB}[n])$$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1]$ and uses them in subsequent AS communications.

[0066]

In step S1011, the mobile station UE transmits "RRC HO Complete (handover complete signal)" to the handover target radio base station (Target eNB).

[0067]

In step S1012, the handover target radio base station (Target eNB) transmits "S1 Path Switch (path switch signal)" including "KI (=n+1)" to the switching center MME.

[0068]

In step S1013, the switching center MME calculates $K_{eNB}[n+2]$ from the formula given below, and in step S1014, stores $K_{eNB}[n+2]$ and "KI (=n+1)".

[0069]

$$K_{eNB}[n+2] = KDF_1 (K_{ASME}, K_{eNB}[n+1])$$

In step S1015, the switching center MME transmits "S1 Patch Switch Ack (path switch acknowledge signal)" including $K_{eNB}[n+2]$ and "KI (=n+1)" to the handover target radio base station (Target eNB).

[0070]

In step S1016, the handover target radio base station

(Target eNB) stores $K_{eNB}[n+1]$, $K_{eNB}[n+2]$ and "KI (=n+1)".

[0071]

Through the above procedure, K_{eNB} and certain keys are updated in the X2 handover.

[0072]

Thirdly, an S1 handover procedure (handover procedure between different switching centers) in the mobile communication system according to this embodiment is described referring to Fig. 5.

[0073]

As shown in Fig. 5, before starting the S1 handover procedure, the mobile station UE holds $K_{eNB}[n]$ and "KI (=n)" (in step S2001), the handover source radio base station (Source eNB) holds $K_{eNB}[n]$, $K_{eNB}[n+1]$ and "KI (=n)" (in step S2002), and the switching center MME holds K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n)" (in step S2003).

[0074]

In step S2004, if predetermined conditions are satisfied, the mobile station UE transmits "RRC Measurement Report (measurement report signal)" to the handover source radio base station (Source eNB).

[0075]

In step S2005, the handover source radio base station (Source eNB) transmits "S1 HO Required (handover request receipt signal)" including $K_{eNB}[n+1]$ and "KI (=n+1)" to the handover source switching center (source MME).

[0076]

In step S2006, the handover source switching center (Source MME) transmits "Relocation Request (relocation request

signal)" including K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n+1)" to the handover target switching center (Target MME).

[0077]

In step S2007, the handover target switching center (Target MME) calculates $K_{eNB}[n+2]$ from the formula given below, and in step S2008, stores $K_{eNB}[n+2]$ and "KI (=n+1)".

[0078]

$$K_{eNB}[n+2] = KDF_1 (K_{ASME}, K_{eNB}[n+1])$$

In step S2009, the handover target switching center (Target MME) transmits "S1 HO Request (handover request signal)" including $K_{eNB}[n+1]$, $K_{eNB}[n+2]$ and "KI (=n+1)" to the handover target radio base station (Target eNB).

[0079]

In step S2010, the handover target radio base station (Target eNB) transmits "S1 HO Request Ack (handover request acknowledge signal)" to the handover target switching center (Target MME).

[0080]

In step S2011, the handover target switching center (Target MME) transmits "Relocation Request Ack (relocation request acknowledge signal)" including "KI (=n+1)" to the handover source switching center (Source MME).

[0081]

In step S2012, the handover source switching center (Source MME) transmits "S1 HO Required Ack (handover request receipt acknowledge signal)" including "KI (=n+1)" to the handover source radio base station (Source eNB).

[0082]

In step S2013, the handover source radio base station

(Source eNB) transmits "RRC HO Command (handover command signal)" to the mobile station UE.

[0083]

In step S2014, the mobile station UE calculates $K_{eNB}[n+1]$ from the following formula, and in step S2015, stores $K_{eNB}[n+1]$ and "KI (=n+1)".

[0084]

$$K_{eNB}[n+1] = KDF_1 (K_{ASME}, K_{eNB}[n])$$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} on the basis of $K_{eNB}[n+1]$ and uses them in subsequent AS communications.

[0085]

At this stage, the handover target radio base station (Target eNB) holds $K_{eNB}[n+1]$, $K_{eNB}[n+2]$ and "KI (=n+1)" (in step S2016). The radio base station eNB calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1]$, and uses them in subsequent AS communications.

[0086]

In step S2017, the mobile station UE transmits "RRC HO Complete (handover complete signal)" to the handover target radio base station (Target eNB).

[0087]

In step S2018, the handover target radio base station (Target eNB) transmits "S1 HO Complete (handover complete signal)" to the handover target switching center (Target MME).

[0088]

In step S2019, the handover target switching center (Target MME) transmits "Relocation Complete (relocation complete signal)" to the handover source switching center

(Source MME), and in step S2020, the handover source switching center (Source MME) transmits "Relocation Complete Ack (relocation complete acknowledge signal)" to the handover target switching center (Target MME).

[0089]

Through the above procedure, K_{eNB} and certain keys are updated in the S1 handover.

[0090]

Operations of the mobile station UE in the S1 handover procedure are same as operations in the X2 handover procedure shown in Fig. 3. Based on the same processing, the mobile station UE is capable of performing both X2 and S1 handover procedures. That is, the mobile station UE is capable of performing a handover regardless of whether the handover type is "X2 handover" or "S1 handover".

[0091]

Fourthly, an Intra-eNB handover procedure (inter-radio base station handover procedure) in the mobile communication system according to this embodiment is described referring to Fig. 6.

[0092]

As shown in Fig. 6, before starting the Intra-eNB handover procedure, the mobile station UE holds $K_{eNB}[n]$ and "KI (=n)" (in step S4001), the radio base station (Source eNB) holds $K_{eNB}[n]$, $K_{eNB}[n+1]$ and "KI (=n)" (in step S4002), and the switching center MME holds K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n)" (in step S4003).

[0093]

In step S4004, if predetermined conditions are satisfied, the mobile station UE transmits "RRC Measurement Repo

(measurement report signal)" to the radio base station (Source eNB).

[0094]

In step S4005, the radio base station (Source eNB) transmits "RRC HO Command (handover command signal)" to the mobile station UE.

[0095]

In step S4006, the mobile station UE calculates $K_{eNB}[n+1]$ from the formula given below, and in step S4007, stores $K_{eNB}[n+1]$ and "KI (=n+1)".

[0096]

$$K_{eNB}[n+1] = KDF_1 (K_{ASME}, K_{eNB}[n])$$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1]$ and uses them in subsequent AS communications.

[0097]

At this stage, the radio base station (Source eNB) holds $K_{eNB}[n+1]$ and "KI (=n+1)" (in step S4008). The radio base station eNB calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1]$ and uses them in subsequent AS communications.

[0098]

In step S4009, the mobile station UE transmits "RRC HO Complete (handover complete signal)" to the radio base station (Source eNB).

[0099]

In step S4010, the radio base station (Source eNB) transmits "S1 Path Switch (path switch signal)" including "KI (=n+1)" to the switching center MME.

[0100]

In step S4011, the switching center MME calculates $K_{eNB}[n+2]$ from the formula given below, and in step S4012, stores K_{ASME}, $K_{eNB}[n+2]$ and "KI (=n+1)".

[0101]

$$K_{eNB}[n+2]=KDF_1\ (K_{ASME},\ K_{eNB}[n+1])$$

In step S4013, the switching center MME transmits "S1 Path Switch Ack (path switch acknowledge signal)" including $K_{eNB}[n+2]$ and "KI (=n+1)" to the radio base station (Source eNB).

[0102]

In step S4014, the radio base station (Source eNB) stores $K_{eNB}[n+1]$, $K_{eNB}[n+2]$ and "KI (=n+1)". At this stage, the mobile station UE holds $K_{eNB}[n+1]$ and "KI (=n+1)" (in step S4015).

[0103]

Through the above procedure, K_{eNB} and certain keys are updated in the Intra-NB handover.

[0104]

Operations of the mobile station UE in the Intra-eNB handover procedure are same as operations in the X2 handover procedure shown in Fig. 3 and in the S1 handover procedure shown in Fig. 4. Based on the same processing, the mobile station UE is capable of performing all of X2, S1 and Intra-eNB handover procedures. That is, the mobile station UE is capable of performing a handover with regardless of whether the handover type is "X2 handover", "S1 handover" or "Intra-eNB handover".

[0105]

(Advantageous Effects of Mobile Communication System According to First Embodiment of the Present Invention)

In the mobile communication system according to the first embodiment of the present invention, $K_{eNB}[n+1]$ and the like us

in the handover target radio base station (Target eNB) can be generated through a simplified procedure.

[0106]

Furthermore, in the mobile communication system according to the first embodiment of the present invention, there is no need to change operations of the mobile station UE in a handover procedure regardless of the handover type (X2 handover, S1 handover or Intra-eNB handover).

[0107]

(Mobile Communication System According to Second Embodiment of the Present Invention)

Referring to Fig. 7, a mobile communication system according to a second embodiment of the present invention is described by focusing on differences from the above described mobile communication system according to the first embodiment of the present invention.

[0108]

Specifically, the S1 handover procedure (handover procedure between different switching centers) in the mobile communication system according to this embodiment is described referring to Fig. 7.

[0109]

As shown in Fig. 7, operations in step S3001 to step S3006 are same as operations in step S2001 to step S2006 shown in Fig. 5.

[0110]

In step S3007, the handover target switching center (Target MME) calculates $K_{eNB}[n+3]$ from the formulas given below, and in step S3008, stores $K_{eNB}[n+3]$ and "KI (=n+2)".

[0111]

$K_{eNB}[n+2]=KDF_1\ (K_{ASME},\ K_{eNB}[n+1])$

$K_{eNB}[n+3]=KDF_1\ (K_{ASME},\ K_{eNB}[n+2])$

In step S3009, the handover target switching center (Target MME) transmits "S1 HO Request (handover request signal)" including $K_{eNB}[n+2]$, $K_{eNB}[n+3]$ and "KI (=n+2)" to the handover target radio base station (Target eNB).

[0112]

In step S3010, the handover target radio base station (Target eNB) transmits "S1 HO Request Ack (handover request acknowledge signal)" to the handover target switching center (Target MME).

[0113]

In step S3011, the handover target switching center (Target MME) transmits "Relocation Request Ack (relocation request acknowledge signal)" including "KI (=n+2)" to the handover source switching center (Source MME).

[0114]

In step S3012, the handover source switching center (Source MME) transmits "S1 HO Required Ack (handover request receipt acknowledge signal)" including "KI (=n+2)" to the handover source radio base station (Source eNB).

[0115]

In step S3013, the handover source radio base station (Source eNB) transmits "RRC HO Command (handover command signal)" to the mobile station UE. This message may include information indicating "KI (=n+2)".

[0116]

In step S3014, the mobile station UE calculates $K_{eNB}[n+2]$

from the formulas given below, and in step S3015, stores $K_{eNB}[n+2]$ and "KI (=n+2)".

[0117]

$$K_{eNB}[n+1]=KDF_1\ (K_{ASME},\ K_{eNB}[n])$$

$$K_{eNB}[n+2]=KDF_1\ (K_{ASME},\ K_{eNB}[n+1])$$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+2]$ and uses them in subsequent AS communications.

[0118]

At this stage, the handover target radio base station (Target eNB) holds $K_{eNB}[n+2]$, $K_{eNB}[n+3]$ and "KI (=n+1)" (in step S3016). The radio base station eNB calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+2]$ and uses them in subsequent AS communications.

[0119]

Hereafter, operations in step S3017 to step S3020 are same as operations in step S2017 to step S2020 shown in Fig. 5.

[0120]

Through the above procedure, certain keys and K_{eNB} used in the AS communication in the handover target radio base station (Target eNB) becomes unidentifiable to the handover source radio base station (Source eNB), whereby system's security is improved.

[0121]

(Mobile Communication System According to Third Embodiment of the Present Invention)

Referring to Fig. 8 to Fig. 11, a mobile communication system according to a third embodiment of the present invention is described by focusing on differences from the above described

mobile communication system according to the first embodiment of the present invention.

[0122]

Fig. 8 shows an example of the hierarchical structure and the calculation procedure of a key used in the mobile communication system according to this embodiment (that is, a key used to calculate the certain key).

[0123]

As shown in Fig. 8, a key K_{RRC_IP} used for "Integrity Protection" in the RRC protocol, a key K_{RRC_Ciph} used for "Ciphering" in the RRC protocol, and a key K_{UP_Ciph} used for "Ciphering" in the U-plane of AS are generated using $K_{eNB}[n][m]$.

[0124]

$K_{eNB}[n][m]$ is calculated by using $K_{eNB}[n]$ from the formulas given below.

[0125]

$$K_{eNB}[n][0] = K_{eNB}[n]$$

$$K_{eNB}[n][m+1] = KDF_2\ (K_{eNB}[n][m])\quad (m \geq 0)$$

Furthermore, $K_{eNB}[n]$ is calculated from the formulas given below using K_{ASME}.

[0126]

$$K_{eNB}[0] = KDF_0\ (K_{ASME},\ NAS\ SN)$$

$$K_{eNB}[n+1] = KDF_1\ (K_{ASME},\ K_{eNB}[n]),\quad (n \geq 0)$$

Hereafter, operations of the mobile communication system according to this embodiment are described referring to Fig. 9 to Fig. 11.

[0127]

Firstly, an X2 handover procedure (handover procedure between different radio base stations) in the mobile

communication system according to this embodiment is described referring to Fig. 9.

[0128]

As shown in Fig. 9, before starting the X2 handover procedure, the mobile station UE holds $K_{eNB}[n]$, $K_{eNB}[n][m]$, "KI (=n)" and "RC (=m)" (in step S6001), the handover source radio base station (Source eNB) holds $K_{eNB}[n]$, $K_{eNB}[n+1]$, $K_{eNB}[n][m]$, "KI (=n)" and "RC (=m)" (in step S6002), and the switching center MME holds K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n)" (in step S6003).

[0129]

In step S6004, if predetermined conditions are satisfied, the mobile station UE transmits "RRC Measurement Report (measurement report signal)" to the handover source radio base station (Source eNB).

[0130]

In step S6005, the handover source radio base station (Source eNB) transmits "X2 HO Preparation (handover preparation signal)" including $K_{eNB}[n+1]$ and "KI (=n+1)" to the handover target radio base station (Target eNB).

[0131]

In steps S6006 and S6007, the handover target radio base station (Target eNB) stores $K_{eNB}[n+1]$, $K_{eNB}[n+1][0]$, "KI (=n+1)" and "RC (=0)". Here, it is assumed that $K_{eNB}[n+1][0]=K_{eNB}[n+1]$.

[0132]

In step S6008, the handover target radio base station (Target eNB) transmits "X2 HO preparation Ack (handover preparation acknowledge signal)" to the handover source radio base station (Source eNB).

[0133]

In step S6009, the handover source radio base station (Source eNB) transmits "RRC HO Command (handover command signal)" including "KI (=n+1)" and "RC (=0)" to the mobile station UE.

[0134]

In step S6010, the mobile station UE calculates $K_{eNB}[n+1]$ and $K_{eNB}[n+1][0]$ from the formulas given below, and in step S6011 stores $K_{eNB}[n+1]$, $K_{eNB}[n+1][0]$, "KI (=n+1)" and "RC (=0)".

[0135]

$$K_{eNB}[n+1] = KDF_1 (K_{ASME}, K_{eNB}[n])$$

$$K_{eNB}[n+1][0] = K_{eNB}[n+1]$$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1][0]$ and uses them in subsequent AS communications.

[0136]

Hereafter, operations in step S6012 to step S6017 are same as operations in step S1011 to step S1016 shown in Fig. 4.

[0137]

Secondly, an S1 handover procedure (handover procedure between different switching centers) in the mobile communication system according to this embodiment is described referring to Fig. 10.

[0138]

As shown in Fig. 10, before starting the S1 handover procedure, the mobile station UE holds $K_{eNB}[n]$, $K_{eNB}[n][m]$, "KI (=n)" and "RC (=m)" (in step S7001), the handover source radio base station (Source eNB) holds $K_{eNB}[n]$, $K_{eNB}[n+1]$, $K_{eNB}[n][m]$, "KI (=n)" and "RC (=m)" (in step S7002), and the switching center MME holds K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n)" (in step S7003).

[0139]

Hereafter, operations in step S7004 to step S7012 are same as operations in step S2004 to step S2012 shown in Fig. 4.

[0140]

In step S7013, the handover source radio base station (Source eNB) transmits "RRC HO Command (handover command signal)" including "KI (=n+1)" and "RC (=0)" to the mobile station UE.

[0141]

Here, in step S7014, the handover target radio base station (Target eNB) calculates $K_{eNB}[n+1][0]$ from the formula given below and stores it.

[0142]

$$K_{eNB}[n+1][0]=K_{eNB}[n+1]$$

At this stage, it is assumed that the handover target radio base station (Target eNB) stores $K_{eNB}[n+1]$, $K_{eNB}[n+2]$, $K_{eNB}[n+1][0]$, "KI (=n+1)", and "RC (=0)" (in step S7015). The radio base station eNB calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1][0]$ and uses them in subsequent AS communications.

[0143]

In step S7016, the mobile station UE calculates $K_{eNB}[n+1]$ and $K_{eNB}[n+1][0]$ from the formulas given below, and in step S7017, stores $K_{eNB}[n+1]$, $K_{eNB}[n+1][0]$, "KI (=n+1)" and "RC (=0)"

[0144]

$$K_{eNB}[n+1]=KDF_1\ (K_{ASME},\ K_{eNB}[n])$$

$$K_{eNB}[n+1][0]=K_{eNB}[n+1]$$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n+1][0]$ and uses them to subsequent AS communications.

[0145]

Hereafter, operations in step S7018 to step S7021 are same as operations in step S2017 to step S2020 shown in Fig. 5.

[0146]

Thirdly, an Intra-eNB handover procedure (inter-radio base station handover procedure) in the mobile communication system according to this embodiment is described referring to Fig. 11.

[0147]

As shown in Fig. 11, before starting the Intra-eNB handover procedure, the mobile station UE holds $K_{eNB}[n]$, $K_{eNB}[n][m]$, "KI (=n)" and "RC (=m)" (in step S5001), the radio base station (Source eNB) holds $K_{eNB}[n]$, $K_{eNB}[n+1]$, $K_{eNB}[n][m]$, "KI (=n)" and "RC (=m)" (in step S5002), and the switching center MME holds K_{ASME}, $K_{eNB}[n+1]$ and "KI (=n)" (in step S5003).

[0148]

In step S5004, if predetermined conditions are satisfied, the mobile station UE transmits "RRC Measurement Report (measurement report signal)" to the radio base station (Source eNB).

[0149]

In step S5005, the radio base station (Source eNB) transmits "RRC HO Command (handover command signal)" including "KI (=n)" and "RC (=m+1)" to the mobile station UE.

[0150]

In step S5006, the radio base station (Source eNB) calculates $K_{eNB}[n][m+1]$ from the formula given below, and in step S5007, stores $K_{eNB}[n]$, $K_{eNB}[n+1]$, $K_{eNB}[n][m+1]$, "KI (=n+1)" and "RC (=m+1)".

[0151]

$K_{eNB}[n][m+1]=KDF_2\ (K_{eNB}[n][m])$

Furthermore, the radio base station eNB calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n][m+1]$ and uses them to subsequent AS communications.

[0152]

At the same time, in step S5008, the mobile station UE calculates $K_{eNB}[n][m+1]$ from the formula given below, and in step S5009, stores $K_{eNB}[n]$, $K_{eNB}[n][m+1]$, "KI (=n+1)" and "RC (=m+1)".

[0153]

$K_{eNB}[n][m+1]=KDF_2\ (K_{eNB}[n][m])$

Furthermore, the mobile station UE calculates K_{RRC_IP}, K_{RRC_Ciph} and K_{UP_Ciph} based on $K_{eNB}[n][m+1]$ and uses them in subsequent AS communications.

[0154]

In step S5010, if predetermined conditions are satisfied, the mobile station UE transmits "RRC HO Complete (handover complete signal)" to the radio base station (Source eNB).

[0155]

According to this embodiment, "Path Switch" in the Intra-eNB handover procedure can be omitted.

[0156]

As shown in Fig. 9 to Fig. 11, by introducing K_{eNB} updating in the radio base station using the parameter "RC", K_{eNB} can be updated while omitting an inquiry to the switching center MME.

[0157]

Meanwhile, in the procedures shown in Fig. 9 to Fig. 11, the parameter "RC" may be omitted from "RRC HO Command (handover command signal)".

[0158]

When the parameter "RC" is omitted from "RRC HO Command (handover command signal)", necessity of incrementing "RC" can be determined by determining whether the parameter "KI" has been incremented or not.

[0159]

If the "KI" has been incremented, "RC" may be reset to "0", whereas if the "KI" has not been incremented, "RC" may be incremented.

[0160]

Alternatively, if the parameter "RC" is omitted from "RRC HO Command (handover command signal)", the mobile station UE may, on a trial basis, maintain the present value of "RC", increment "RC" or reset "RC" to "0" and then check "Integrity" with respect to a message received for each of the cases to autonomously determine which one of the cases is correct.

[0161]

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

[0162]

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 (Electronically Erasable and Programmable ROM), a register, a hard disk, a removable disk, or a CD-ROM.

[0163]

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 switching center MME, the radio base station eNB and the mobile station UE. Also, the storage medium and the processor may be provided in the switching center MME, the radio base station eNB and the mobile station UE as a discrete component.

[0164]

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.

WHAT IS CLAIMED IS:

1. A mobile communication method in which a mobile station performs a handover from a handover source radio base station to a handover target radio base station via an inter-radio base station interface, the mobile communication method comprising the steps of:

(A) acquiring, at the handover target radio base station, from the handover source radio base station, a first target base station-mobile station generative key for generating a target base station-mobile station certain key used in a communication between the handover target radio base station and the mobile station; and

(B) acquiring, at the handover target radio base station, from a switching center, a next target base station-mobile station generative key for generating a next target base station-mobile station certain key used in a communication between a next handover target radio base station and the mobile station;

(C) updating, at the mobile station, upon receiving a handover command signal from the handover source radio base station, a source base station-mobile station generative key for generating a source base station-mobile station certain key used in a communication between the handover source radio base station and the mobile station, to the first target base station-mobile station generative key;

characterized in that

the step (C) comprises the steps of

(C1) generating, at the mobile station, the first target base station-mobile station generative key, based on a parameter included in the handover command signal and without using the source base station-mobile station generative key, when the parameter is incremented by the source radio base station; and

(C2) generating, at the mobile station, the first target base station-mobile station generative key based on the source base station-mobile station generative key, when the parameter included in the handover command signal is not incremented.

2. The mobile communication method according to claim 1, wherein in the step (C1), the mobile station generates, based on the parameter, an intermediate key, and generates the first target base station-mobile station generative key based on the intermediate key.

3. The mobile communication method according to claim 1 or 2, further comprising the step of:

(D) storing, at the mobile station, the received parameter.

4. The mobile communication method according to claim 1, wherein the parameter included in the handover command signal is a parameter which is incremented or not.

5. A mobile station which performs a handover from a handover source radio base station to a handover target radio base station, the mobile station comprising:

a key updating unit configured to update, upon receiving a handover command signal from the handover source radio base station, a source base station-mobile station generative key for generating a source base station-mobile station certain key used in a communication between the handover source radio base station and the mobile station, to a first target base station-mobile station generative key for generating a target base station-mobile station certain key used in a communication between the handover target radio base station and the mobile station;

characterized in that

the key updating unit is configured to generate, when the parameter included in the handover command signal is incremented, the first target base station-mobile station generative key, based on the parameter and without using the source base station-mobile station generative key; and

the key updating unit is configured to generate, when the parameter included in the handover command signal is not incremented, the first target base station-mobile station generative key, based on the source base station-mobile station generative key.

6. The mobile station according to claim 5, wherein

the key updating unit is configured to generate, when a parameter included in the handover command signal is incremented, an intermediate key, based on the parameter, and to generate the first target base station-mobile station generative key, based on the intermediate key.

7. The mobile station according to claim 5 or 6, wherein the key updating unit is configured to store the received parameter.

8. The mobile station according to claim 5, wherein the parameter included in the handover command signal is a parameter which is incremented or not.

9. A mobile communication method in which a mobile station (UE) performs a handover from a handover source radio base station to a handover target radio base station by an interface via a switching center, the mobile communication method comprising the steps of:

(A) acquiring, at the handover target radio base station, from the switching center, a first target base station-mobile station generative key for generating a target base station-mobile station certain key used in a communication between the handover target radio base station and the mobile station (UE); and

(B) generating, at the mobile station (UE), the first target base station-mobile station generative key based on an incremented parameter (KI=n+1) which is included in a handover command signal and without using a source base

station-mobile station generative key for generating a source base station-mobile station certain key used in a communication between the handover source radio base station and the mobile station, wherein the incremented parameter (KI=n+1) is obtained by incrementing a parameter (KI=n) which is used upon creating the source base station-mobile station generative key, when receiving the handover command signal from the handover source radio base station.

10. A mobile station which can perform a handover from a handover source radio base station to a handover target radio base station by an interface via a switching center, wherein
the mobile station is configured to generate a first target base station-mobile station generative key for generating a target base station-mobile station certain key used in a communication between the handover target radio base station and the mobile station (UE) based on an incremented parameter (KI=n+1) included in a handover command signal and without using a source base station-mobile station generative key for generating a source base station-mobile station certain key used in a communication between the handover source radio base station and the mobile station, wherein the incremented parameter (KI=n+l) is obtained by incrementing a parameter (KI=n) which is used upon creating the source base station-mobile station generative

ke, when receiving the handover command signal from the handover source radio base station.

FIG. 1

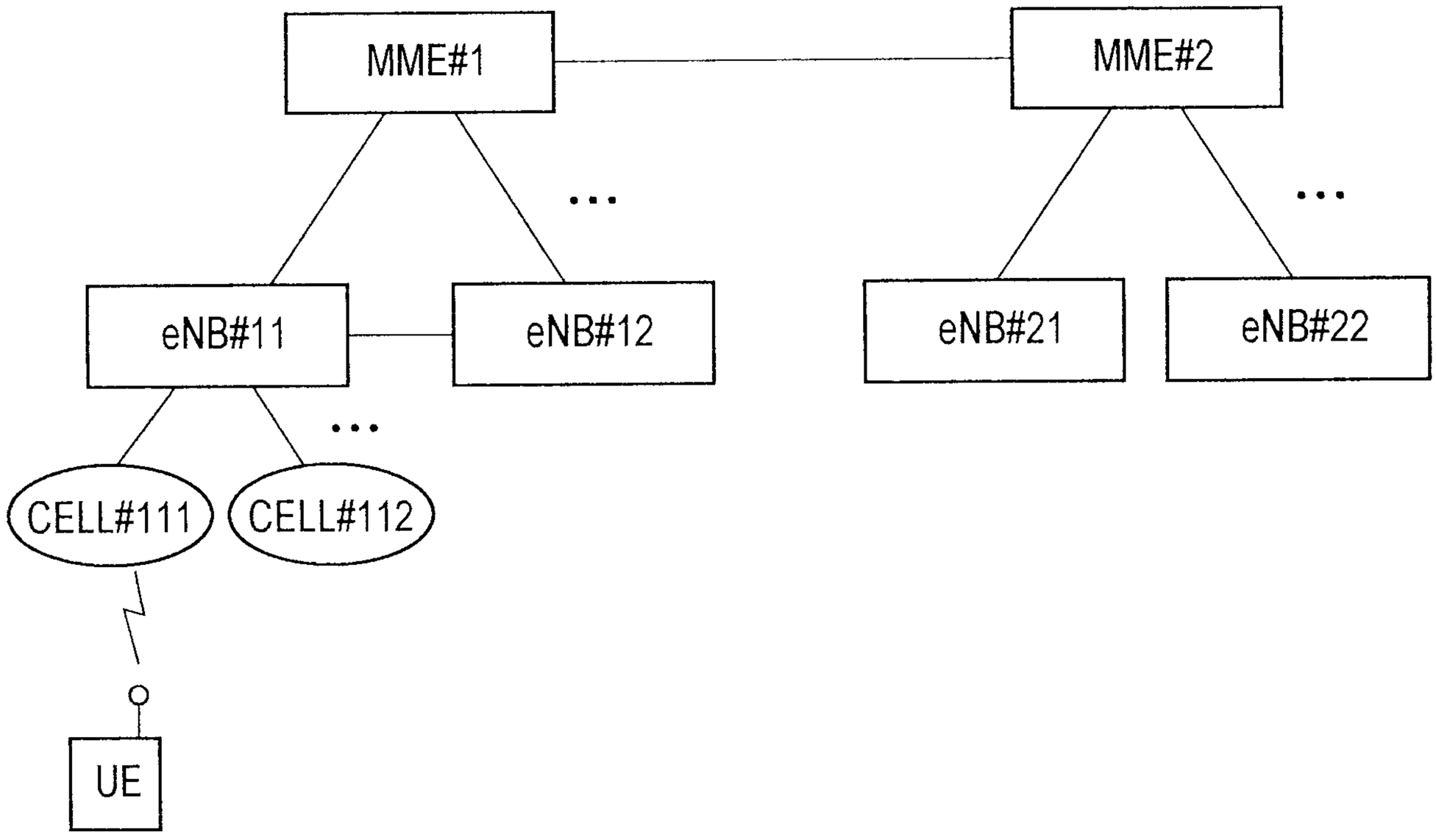
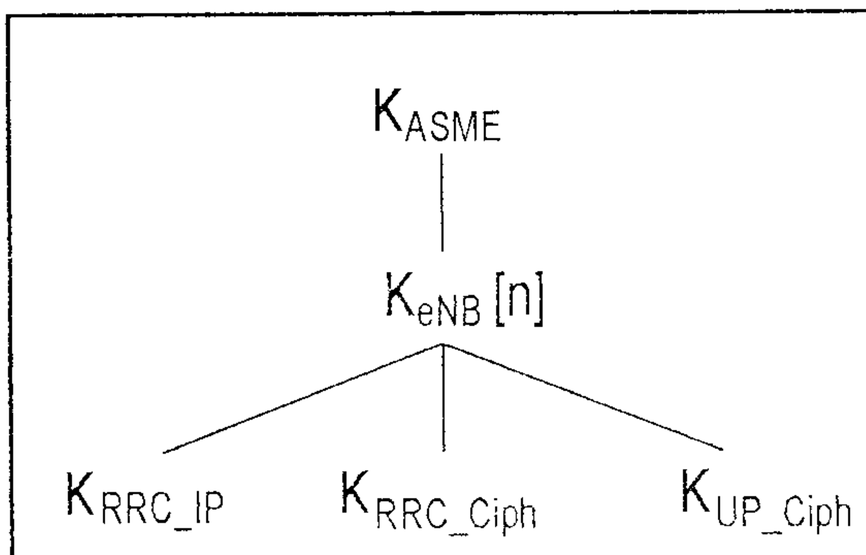


FIG. 2



$K_{eNB}[0]=KDF_0(K_{ASME}, \text{NAS SN})$

$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n]), (n \geqq 0)$

FIG. 3

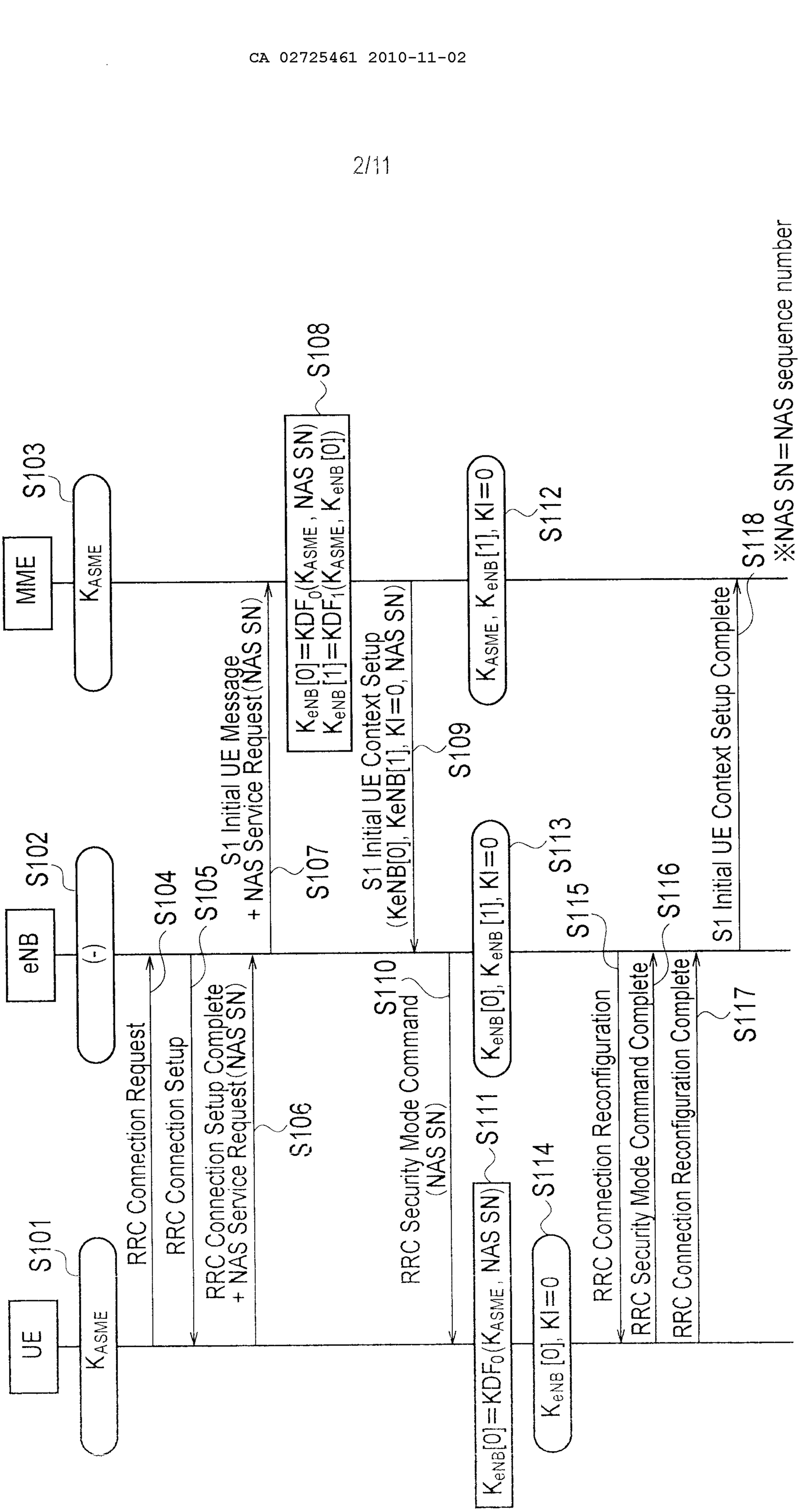

UE
eNB
MME
S101
S102
S103
S104
S105
S106
S107
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117
S118
※NAS SN=NAS sequence number
K_{ASME}
(-)
RRC Connection Request
RRC Connection Setup
RRC Connection Setup Complete
+ NAS Service Request(NAS SN)
S1 Initial UE Message
+ NAS Service Request(NAS SN)
$K_{eNB}[0]=KDF_0(K_{ASME}, NAS SN)$
$K_{eNB}[1]=KDF_1(K_{ASME}, K_{eNB}[0])$
S1 Initial UE Context Setup
(KeNB[0], KeNB[1], KI=0, NAS SN)
RRC Security Mode Command
(NAS SN)
K_{ASME}, $K_{eNB}[1]$, KI=0
$K_{eNB}[0]$, $K_{eNB}[1]$, KI=0
RRC Connection Reconfiguration
RRC Security Mode Command Complete
RRC Connection Reconfiguration Complete
S1 Initial UE Context Setup Complete
$K_{eNB}[0]=KDF_0(K_{ASME}, NAS SN)$
$K_{eNB}[0]$, KI=0

FIG. 4

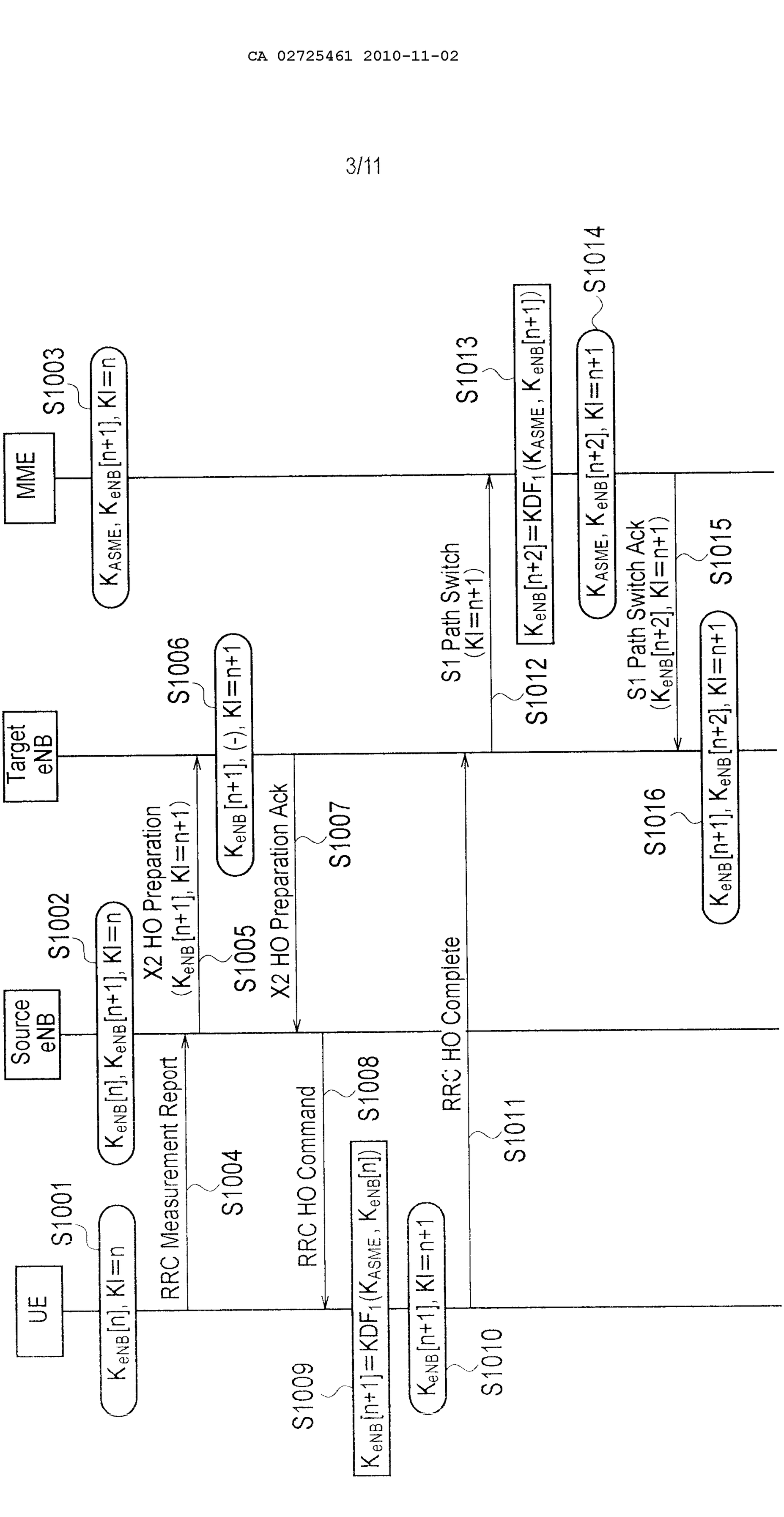

UE
Source eNB
Target eNB
MME
S1001
K_{eNB}[n], KI=n
S1002
K_{eNB}[n], K_{eNB}[n+1], KI=n
S1003
K_{ASME}, K_{eNB}[n+1], KI=n
RRC Measurement Report
S1004
X2 HO Preparation
(K_{eNB}[n+1], KI=n+1)
S1005
K_{eNB}[n+1], (-), KI=n+1
S1006
X2 HO Preparation Ack
S1007
RRC HO Command
S1008
RRC HO Complete
S1009
K_{eNB}[n+1]=KDF$_1$(K_{ASME}, K_{eNB}[n])
K_{eNB}[n+1], KI=n+1
S1010
S1011
S1012
S1 Path Switch
(KI=n+1)
S1013
K_{eNB}[n+2]=KDF$_1$(K_{ASME}, K_{eNB}[n+1])
S1014
K_{ASME}, K_{eNB}[n+2], KI=n+1
S1 Path Switch Ack
(K_{eNB}[n+2], KI=n+1)
S1015
K_{eNB}[n+2], KI=n+1
S1016
K_{eNB}[n+1], K_{eNB}[n+2]

FIG. 5

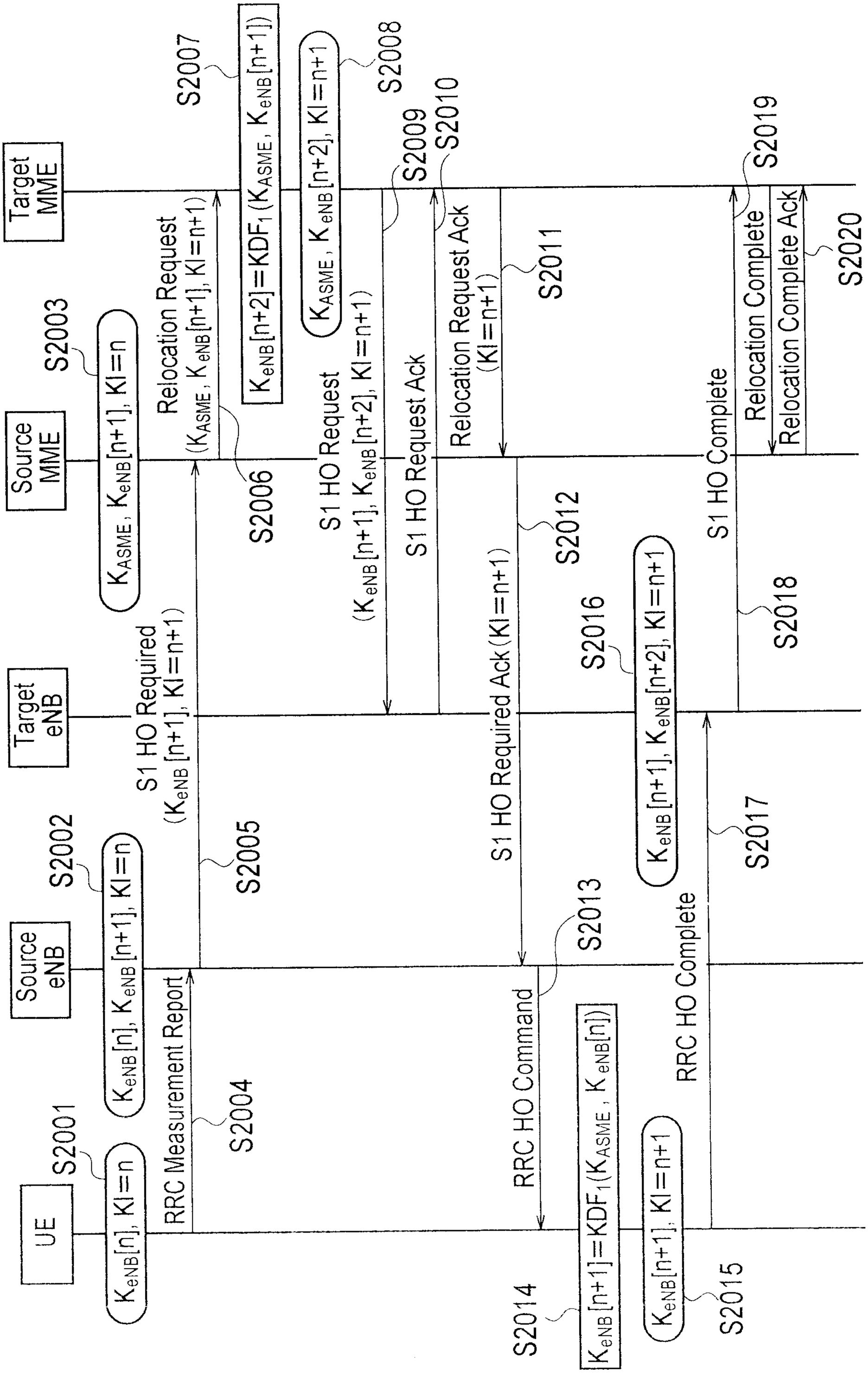

UE
Source eNB
Target eNB
Source MME
Target MME
S2001
S2002
S2003
S2004
S2005
S2006
S2007
S2008
S2009
S2010
S2011
S2012
S2013
S2014
S2015
S2016
S2017
S2018
S2019
S2020
RRC Measurement Report
S1 HO Required
S1 HO Required Ack
RRC HO Command
RRC HO Complete
S1 HO Request
S1 HO Request Ack
Relocation Request
Relocation Request Ack
S1 HO Complete
Relocation Complete
Relocation Complete Ack
KI=n
KI=n+1
KDF1(KASME, KeNB[n])
KDF1(KASME, KeNB[n+1])
KDF1(KASME, KeNB[n+2])

FIG. 6

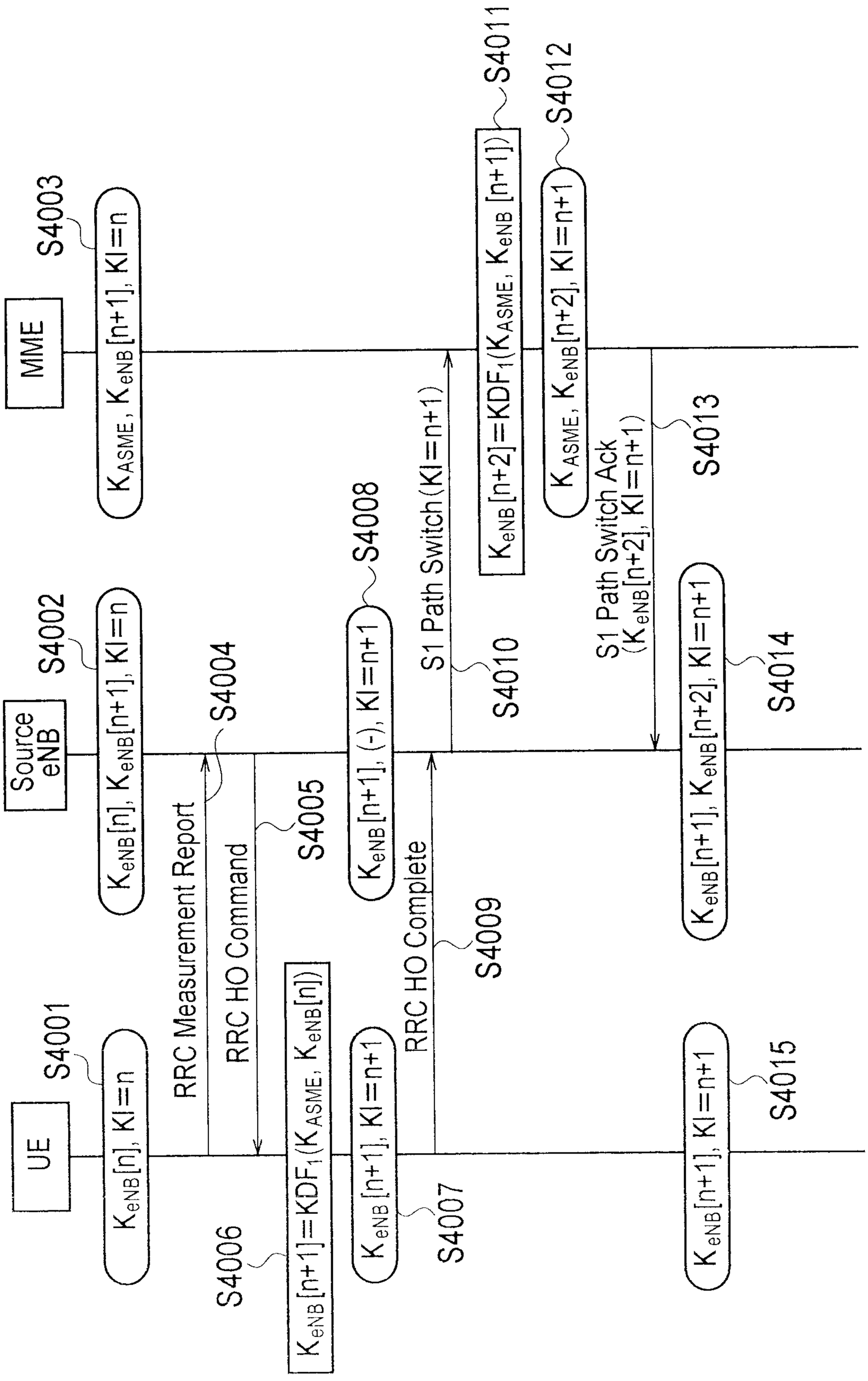

UE
Source eNB
MME
S4001
S4002
S4003
S4004
S4005
S4006
S4007
S4008
S4009
S4010
S4011
S4012
S4013
S4014
S4015
RRC Measurement Report
RRC HO Command
RRC HO Complete
S1 Path Switch (KI=n+1)
S1 Path Switch Ack (KI=n+1)
KeNB[n], KeNB[n+1], KI=n
KeNB[n+1], (-), KI=n+1
KeNB[n+1], KeNB[n+2], KI=n+1
KASME, KeNB[n+1], KI=n+1
KASME, KeNB[n+2], KI=n+1
KeNB[n+1]=KDF1(KASME, KeNB[n])
KeNB[n+2]=KDF1(KASME, KeNB[n+1])

FIG. 7

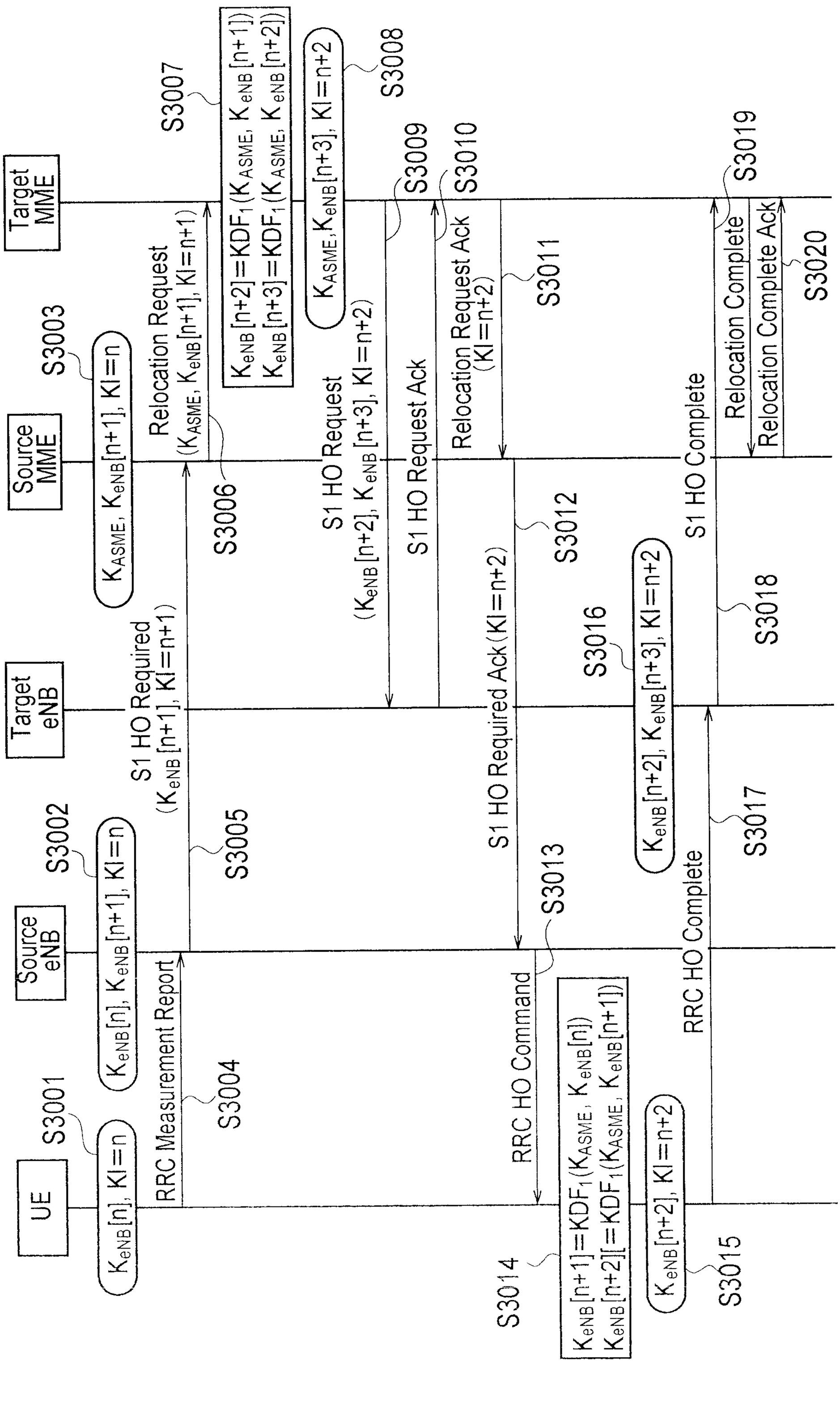

UE
Source eNB
Target eNB
Source MME
Target MME
S3001
K_eNB[n], KI=n
RRC Measurement Report
S3002
K_eNB[n], K_eNB[n+1], KI=n
S3003
Relocation Request (K_ASME, K_eNB[n+1], KI=n+1)
S3004
S3005
S3006
S1 HO Required (K_eNB[n+1], KI=n+1)
K_eNB[n+2]=KDF1(K_ASME, K_eNB[n+1])
K_eNB[n+3]=KDF1(K_ASME, K_eNB[n+2])
S3007
K_ASME, K_eNB[n+2], K_eNB[n+3], KI=n+2
S3008
S3009
S3010
S1 HO Request
S1 HO Request Ack
Relocation Request Ack (KI=n+2)
S3011
S3012
S1 HO Required Ack (KI=n+2)
S3013
RRC HO Command
S3014
K_eNB[n+1]=KDF1(K_ASME, K_eNB[n])
K_eNB[n+2]=KDF1(K_ASME, K_eNB[n+1])
K_eNB[n+2], KI=n+2
S3015
S3016
K_eNB[n+2], K_eNB[n+3], KI=n+2
S3017
RRC HO Complete
S3018
S1 HO Complete
Relocation Complete
S3019
Relocation Complete Ack
S3020

FIG. 8

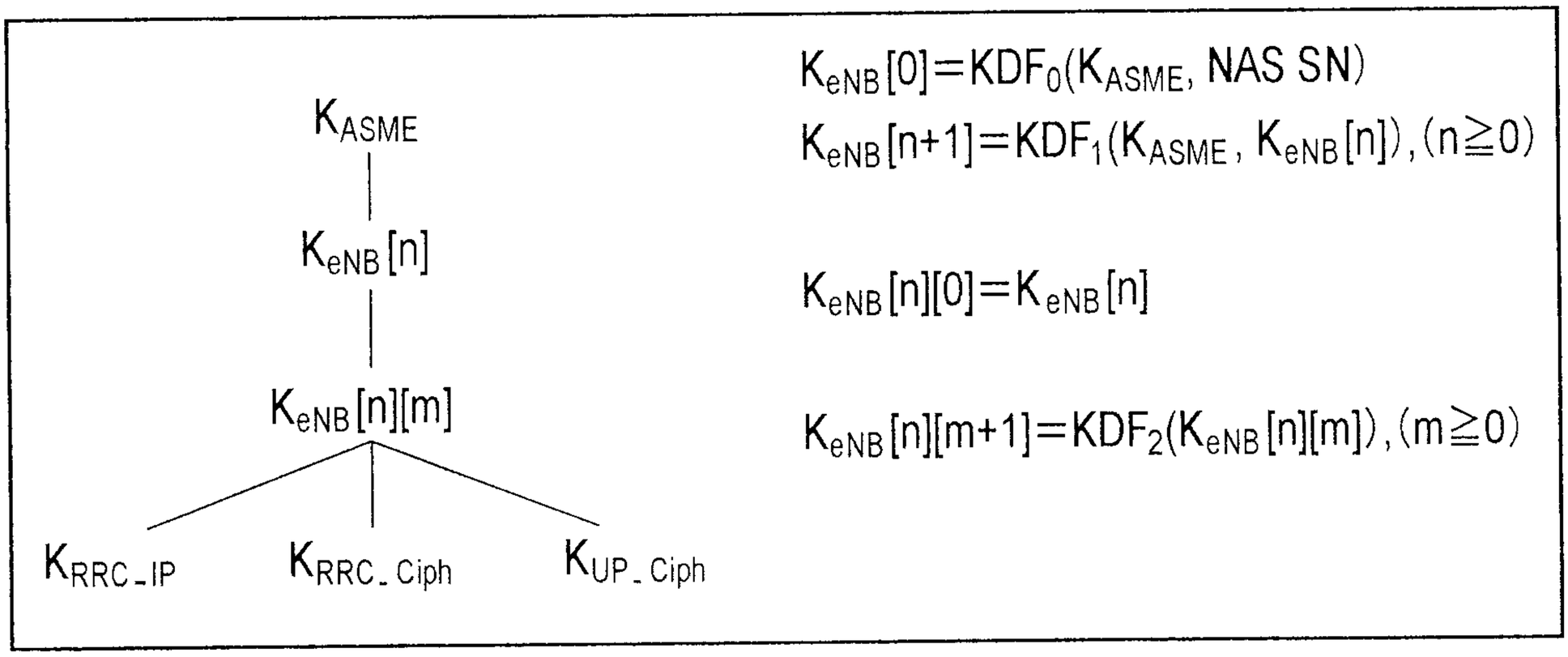

K_{ASME}
$K_{eNB}[n]$
$K_{eNB}[n][m]$
K_{RRC_IP}
K_{RRC_Ciph}
K_{UP_Ciph}
$K_{eNB}[0]=KDF_0(K_{ASME}, NAS\ SN)$
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n]),(n\geqq 0)$
$K_{eNB}[n][0]=K_{eNB}[n]$
$K_{eNB}[n][m+1]=KDF_2(K_{eNB}[n][m]),(m\geqq 0)$

FIG. 9

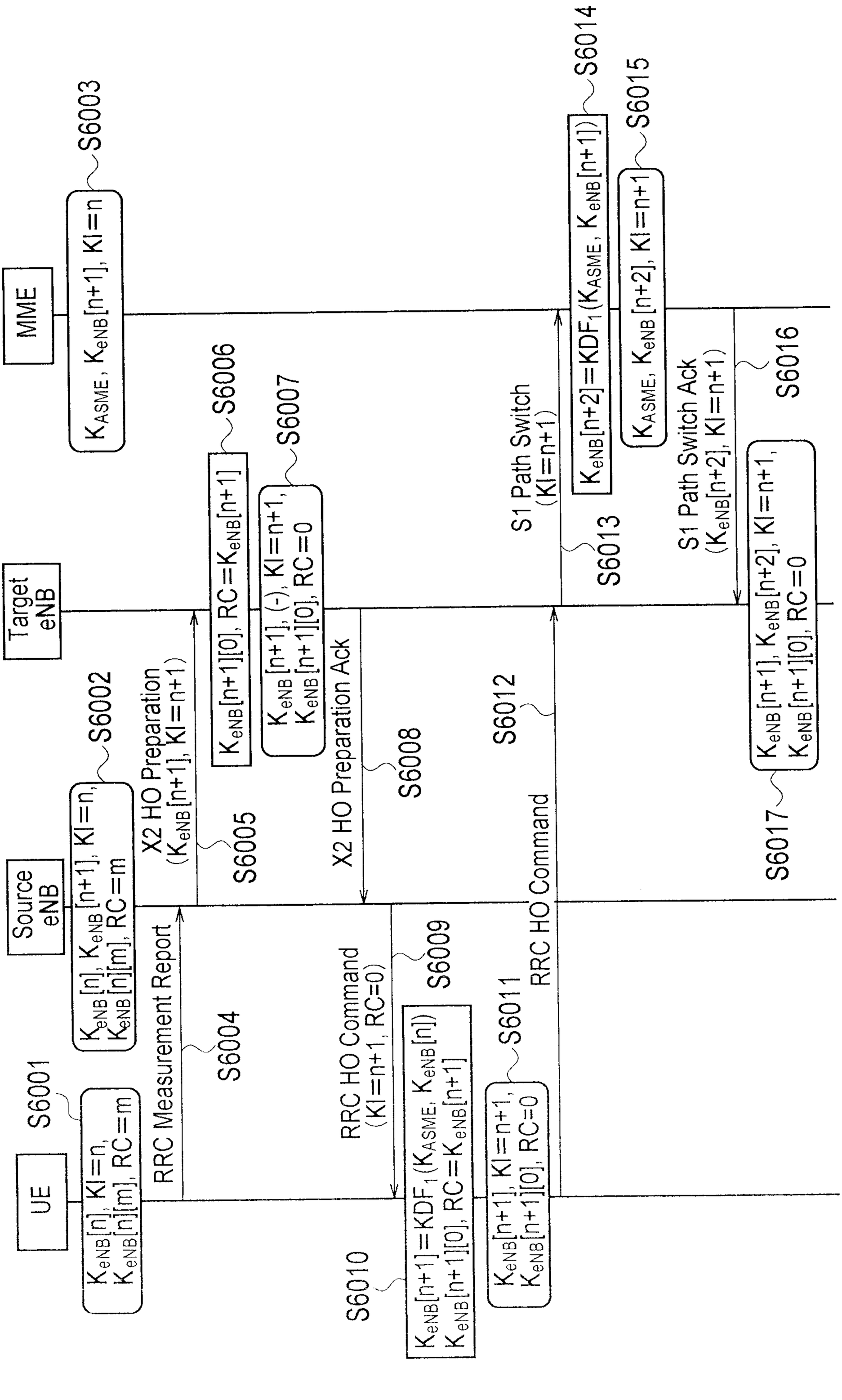

UE
Source eNB
Target eNB
MME
S6001
S6002
S6003
S6004
S6005
S6006
S6007
S6008
S6009
S6010
S6011
S6012
S6013
S6014
S6015
S6016
S6017
RRC Measurement Report
X2 HO Preparation
X2 HO Preparation Ack
RRC HO Command
S1 Path Switch
S1 Path Switch Ack
RRC HO Command
$K_{eNB}[n], K_{eNB}[n+1], KI=n, K_{eNB}[n][m], RC=m$
$K_{eNB}[n], K_{eNB}[n][m], RC=m$
$K_{eNB}[n+1], KI=n+1, RC=0$
$K_{eNB}[n+1][0], RC=K_{eNB}[n+1]$
$K_{eNB}[n+1], (-), KI=n+1, K_{eNB}[n+1][0], RC=0$
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n])$
$K_{eNB}[n+1][0], RC=K_{eNB}[n+1]$
$K_{ASME}, K_{eNB}[n+1], KI=n$
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n+1])$
$K_{ASME}, K_{eNB}[n+2], KI=n+1$
$K_{eNB}[n+2]=KDF_1(K_{ASME}, K_{eNB}[n+1])$
$K_{eNB}[n+1], K_{eNB}[n+2], KI=n+1, K_{eNB}[n+1][0], RC=0$
$K_{eNB}[n+1], K_{eNB}[n+2], KI=n+1, K_{eNB}[n+1][0], RC=0$
$K_{eNB}[n+1], KI=n+1, RC=0$
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n])$
$K_{eNB}[n+1][0], RC=K_{eNB}[n+1]$

FIG. 10

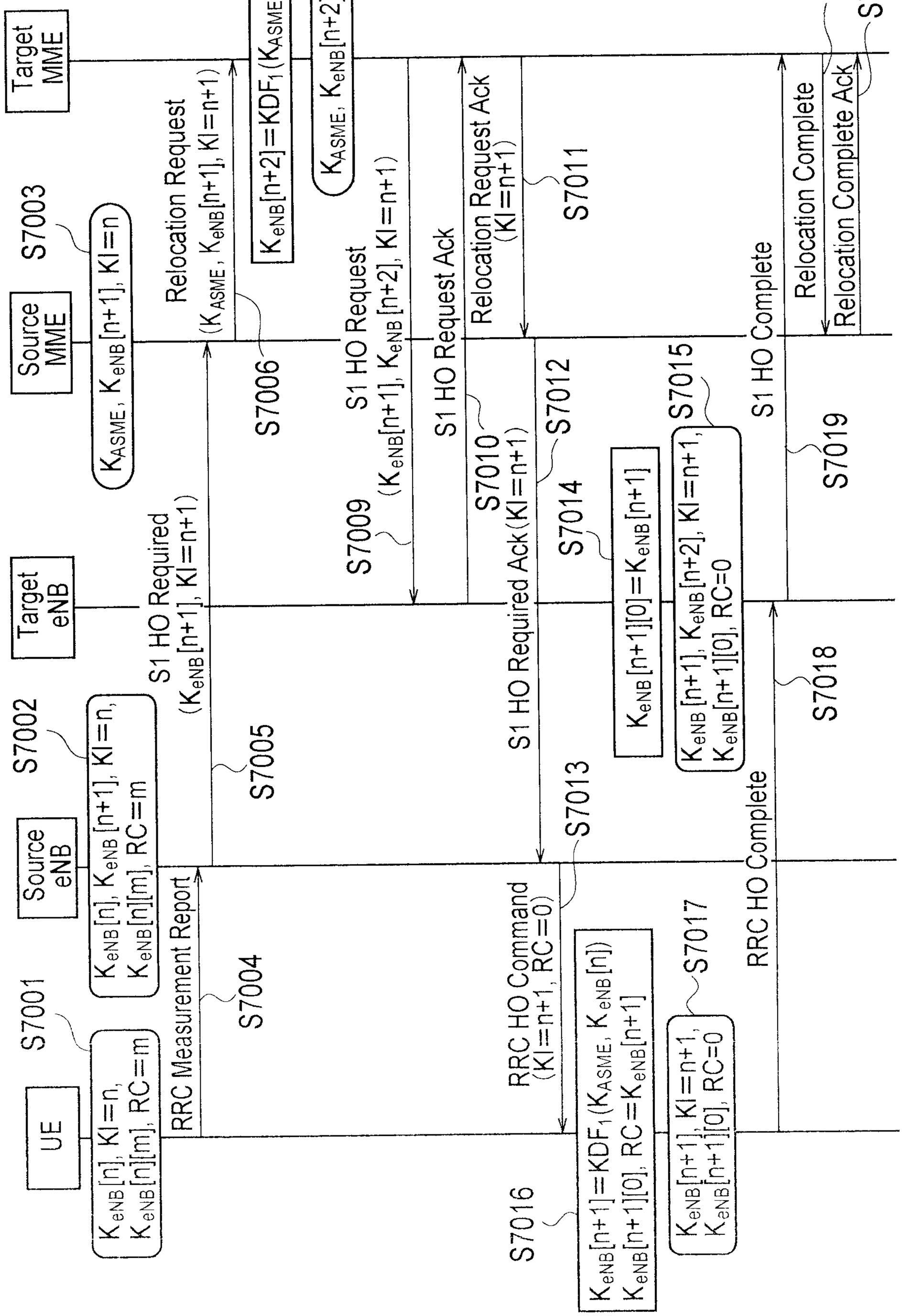

UE
Source eNB
Target eNB
Source MME
Target MME
S7001
S7002
S7003
S7004
S7005
S7006
S7007
S7008
S7009
S7010
S7011
S7012
S7013
S7014
S7015
S7016
S7017
S7018
S7019
S7020
S7021
RRC Measurement Report
S1 HO Required
S1 HO Request
S1 HO Request Ack
Relocation Request
Relocation Request Ack
S1 HO Required Ack
RRC HO Command
S1 HO Complete
RRC HO Complete
Relocation Complete
Relocation Complete Ack

FIG. 11

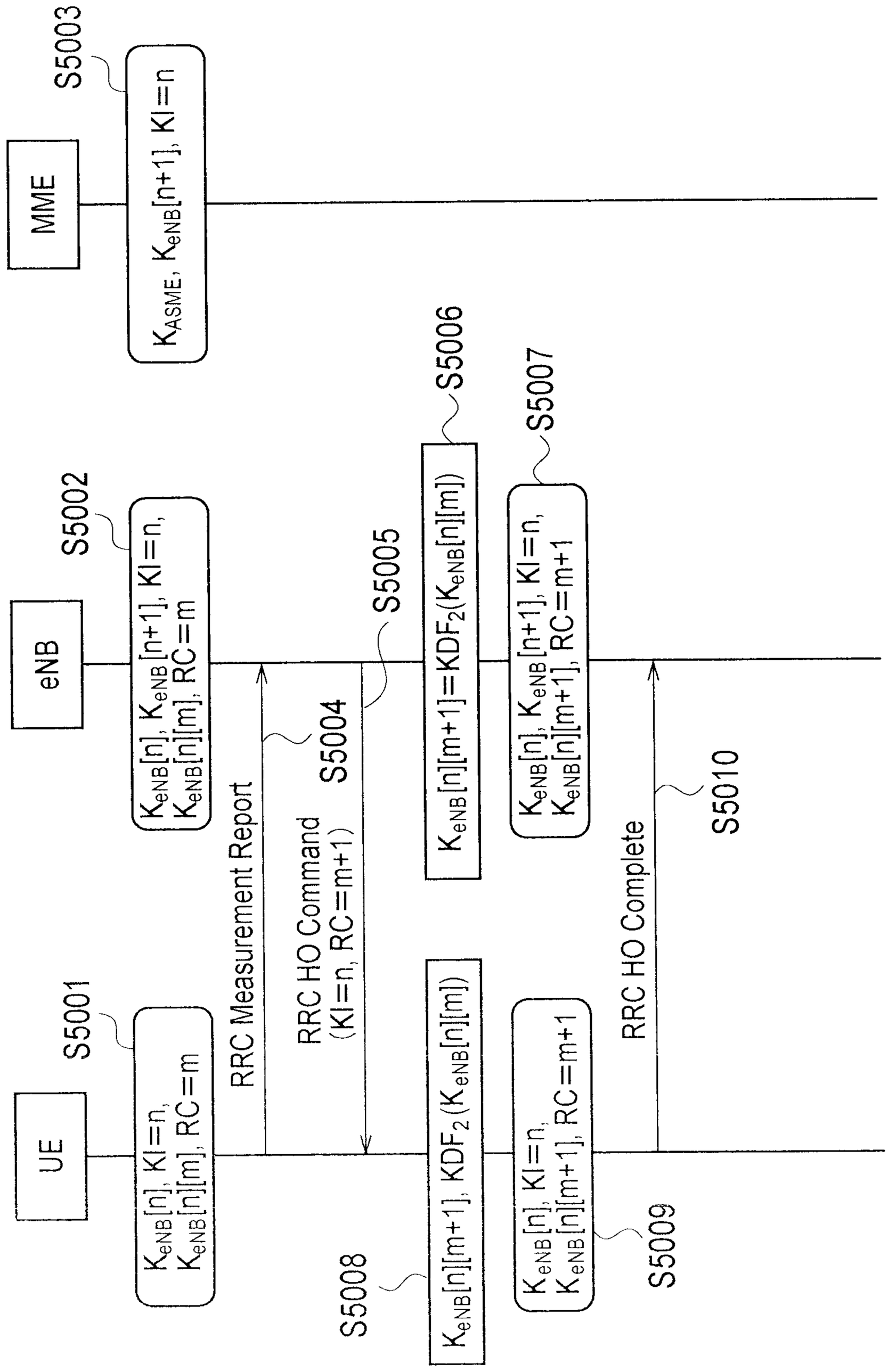

UE
eNB
MME
S5001
S5002
S5003
S5004
S5005
S5006
S5007
S5008
S5009
S5010
RRC Measurement Report
RRC HO Command (KI=n, RC=m+1)
RRC HO Complete

FIG. 12

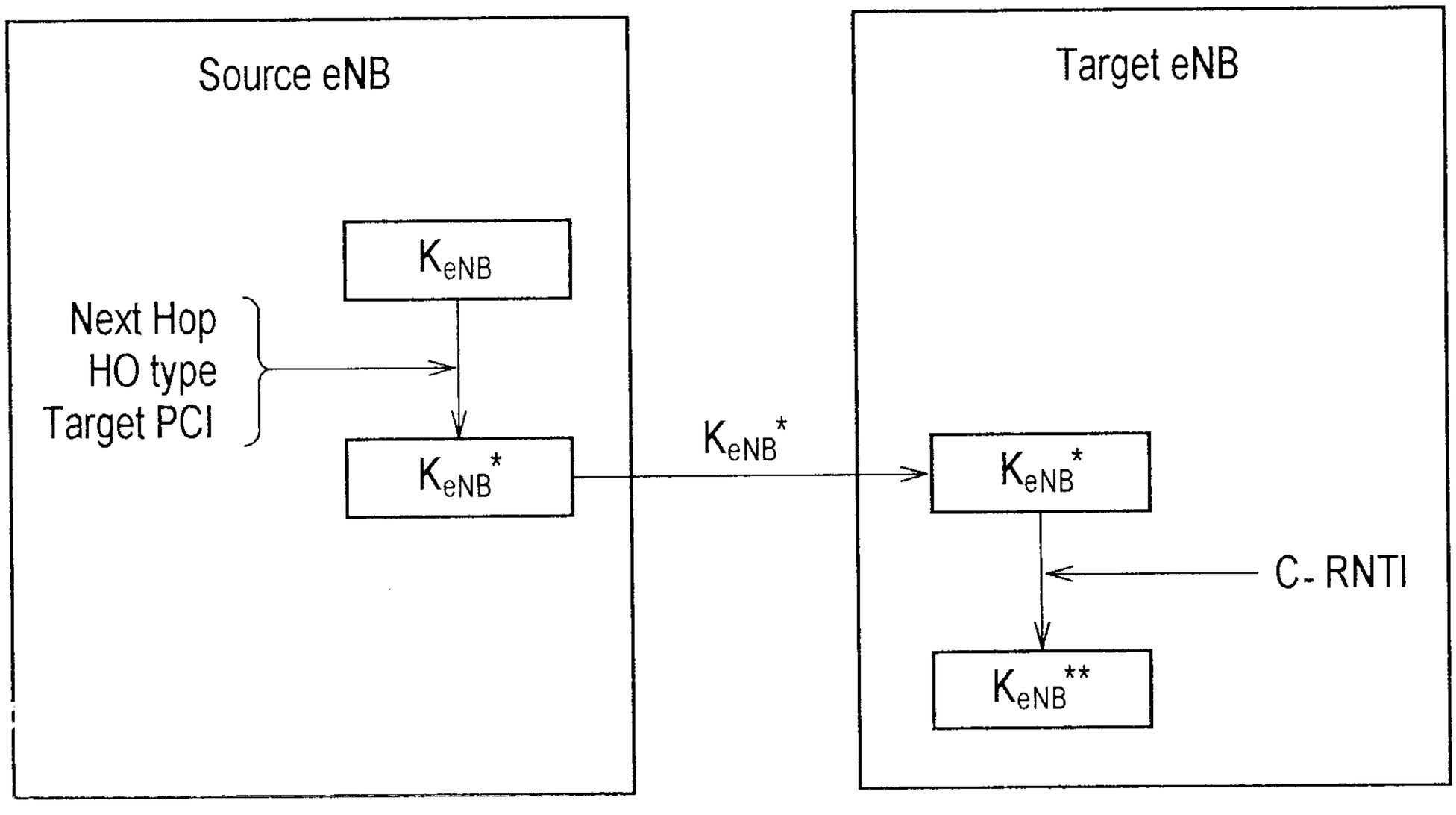
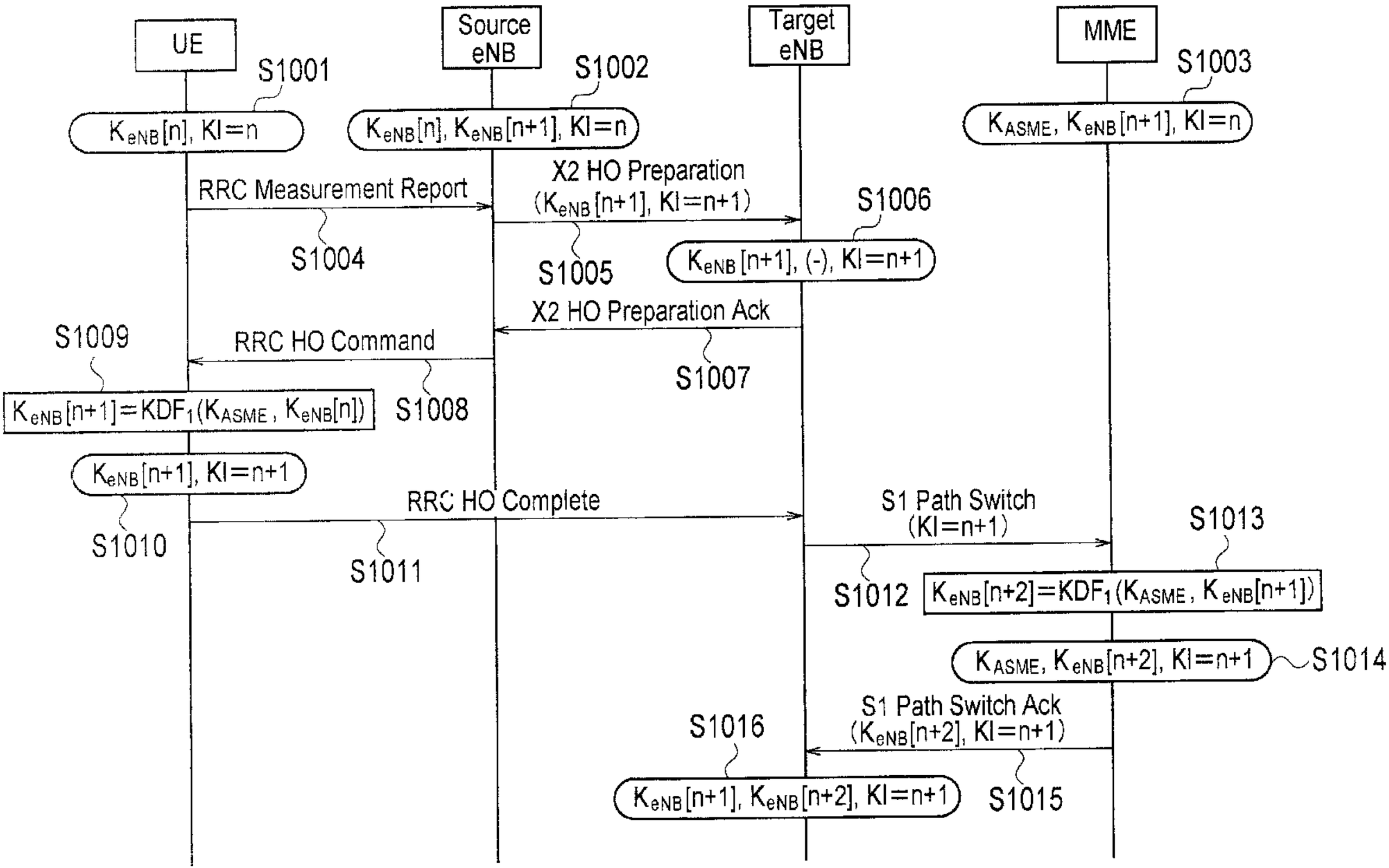

Source eNB
Target eNB
K_{eNB}
Next Hop
HO type
Target PCI
K_{eNB}^*
K_{eNB}^*
K_{eNB}^*
C- RNTI
K_{eNB}^{**}

FIG. 4


UE
Source eNB
Target eNB
MME
S1001
S1002
S1003
$K_{eNB}[n]$, KI=n
$K_{eNB}[n]$, $K_{eNB}[n+1]$, KI=n
K_{ASME}, $K_{eNB}[n+1]$, KI=n
RRC Measurement Report
S1004
X2 HO Preparation
($K_{eNB}[n+1]$, KI=n+1)
S1005
S1006
$K_{eNB}[n+1]$, (-), KI=n+1
X2 HO Preparation Ack
S1007
S1009
RRC HO Command
S1008
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n])$
$K_{eNB}[n+1]$, KI=n+1
S1010
RRC HO Complete
S1011
S1 Path Switch
(KI=n+1)
S1012
S1013
$K_{eNB}[n+2]=KDF_1(K_{ASME}, K_{eNB}[n+1])$
K_{ASME}, $K_{eNB}[n+2]$, KI=n+1
S1014
S1 Path Switch Ack
($K_{eNB}[n+2]$, KI=n+1)
S1015
S1016
$K_{eNB}[n+1]$, $K_{eNB}[n+2]$, KI=n+1