(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 024**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04W 36/06 (2009.01)
H04W 36/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.06.2009 E 09770257 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.12.2012 EP 2273808**

(54) Título: **Procedimiento de comunicaciones móviles**

(30) Prioridad:

27.06.2008 JP 2008169669

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2013

(73) Titular/es:

NTT DOCOMO, INC. (100.0%)
Sanno Park Tower 36th floor, 11-1, Nagata-cho 2-chome Chiyoda-ku
Tokyo 100-6150 , JP

(72) Inventor/es:

IWAMURA, MIKIO;
HAPSARI, WURI, ANDARMAWANTI;
YABUKI, SHOGO y
ZUGENMAIER, ALF

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento de comunicaciones móviles

Campo técnico

La presente invención se refiere a un procedimiento de comunicaciones móviles para la comunicación entre una estación móvil y una estación base de radio usando una cierta clave.

Antecedentes técnicos

Un sistema de comunicaciones móviles convencional del esquema LTE (Evolución a Largo Plazo) especificado por el 3GPP se configura para comunicar entre una estación móvil UE y una estación base de radio eNB usando una cierta clave.

Esta cierta clave incluye, por ejemplo una clave $K_{RRC\ Ciph}$ usada para el "Cifrado" en un protocolo RRC, que es un protocolo del plano C entre la estación móvil UE y la estación base de radio eNB (Estrato de Acceso, AS), una clave $K_{RRC\text{-}IP}$ usada para la "Protección de Integridad" en el protocolo RRC, y una clave $K_{UP\ Ciph}$ usada para el "Cifrado" en un protocolo del plano U entre la estación móvil UE y la estación base de radio eNB (Estrato de Acceso, AS) y similares. Estas ciertas claves se generan usando una primera clave K_{eNB}.

El uso de la misma clave como cualquiera de las ciertas claves y la primera clave K_{eNB} durante un largo tiempo no es preferible porque hace vulnerable la seguridad del sistema. Por esta razón, el 3GPP ideó un procedimiento para la actualización tal cierta clave o una primera clave K_{eNB} durante la transferencia.

En este punto, se describen las operaciones de la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del reestablecimiento para adquirir una primera clave KeNB** usada para la generación de una cierta clave en el procedimiento de restablecimiento para una estación móvil UE, con referencia a la Fig. 8.

Como se muestra en la Fig. 8, en primer lugar, una estación base de radio (eNB Fuente) que gestiona una célula fuente del restablecimiento genera una clave intermedia KeNB* en base a una primera clave almacenada KeNB, un parámetro de "Próximo Salto", un parámetro de "Tipo de Transferencia" que representa a un tipo de transferencia y un parámetro de "PCI Objetivo" que representa la información de identificación de una célula objetivo de la transferencia.

En segundo lugar, la estación base de radio (eNB Fuente) que gestiona la célula fuente del restablecimiento transmite la clave intermedia generada KeNB* a la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del restablecimiento.

En tercer lugar, la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del restablecimiento genera la primera clave KeNB** usada para generar una cierta clave en la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del restablecimiento, en base a la clave intermedia recibida KeNB* y "C-RNTI (ID Temporal de la Red de Radio de Llamada)" asignada por la célula objetivo del restablecimiento.

La publicación del 3GPP TR 33.821, V0.8.0 se refiere a un procedimiento de comunicaciones de radio de un eNB objetivo que adquiere la K_{eNB}* del Próximo Salto desde el MME en la transferencia entre eNB.

La publicación del 3GPP TS 33.401, V1.1.0 se refiere a un procedimiento similar.

Revelación de la Invención

Problema a resolver por la invención

Sin embargo, como se ha descrito anteriormente, el procedimiento de restablecimiento convencional en el sistema de comunicaciones móviles tiene el problema de que tanto la estación base de radio (eNB Fuente) que gestiona la célula fuente del restablecimiento como la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del restablecimiento tienen que usar una pluralidad de parámetros y funciones para generar una primera clave K_{eNB}** usada en la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del restablecimiento.

En particular, hay el problema de que tanto la estación base de radio (eNB Fuente) que gestiona la célula fuente del restablecimiento como la estación base de radio (eNB Objetivo) que gestiona una célula objetivo del restablecimiento tienen que usar las funciones de conversión de K_{eNB} (Función de Derivación de Claves, KDF) diferente en parámetros para cada una de las estaciones base de radio, y una estación móvil UE también se tiene que proveer con estas KDF, por lo que el procedimiento es complicado.

Además, es incómodo que K_{eNB} necesite actualizarse de acuerdo con la PCT (ID de la Célula Física) de la célula objetivo del restablecimiento.

En particular, en el caso donde el procedimiento es dependiente de PCI, cuando una estación móvil UE intenta el

restablecimiento con una célula diferente bajo el control de una estación base de radio con "contexto de UE" que existe en la estación base de radio, se puede rechazar el restablecimiento debido a la no coincidencia de ciertas claves entre la estación móvil UE y la estación base de radio.

Además, hay una restricción en el cambio flexible de la asignación de C-RNTI, ya que KeNB necesita actualizarse de acuerdo con C-RNTI.

Por lo tanto, la presente invención se ha hecho a la vista de los problemas descritos anteriormente, y un objeto de la presente invención es proporcionar un procedimiento de comunicaciones móviles en el cual la primera clave usada por la estación base de radio (eNB Objetivo) que gestiona la célula objetivo del restablecimiento se puede generar a través de un procedimiento simplificado.

Solución al problema

Este problema se resuelve por el procedimiento de comunicaciones con las características de la reivindicación 1, la estación base de radio con las características de la reivindicación 4, y la estación móvil con las características de la reivindicación 6.

Breve descripción de los dibujos

[Fig. 1], la Fig. 1 es una vista de la configuración global de un sistema de comunicaciones móviles de acuerdo con una primera realización de la presente invención.
[Fig. 2], la Fig. 2 es un diagrama que muestra un ejemplo de una estructura jerárquica y un procedimiento de cálculo de una clave usada en el sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención.
[Fig. 3], la Fig. 3 es un diagrama de secuencia que muestra un procedimiento de restablecimiento intra eNB en el sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención.
[Fig. 4], la Fig. 4 es un diagrama de secuencia que muestra un procedimiento de restablecimiento entre eNB en el sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención.
[Fig. 5], la Fig. 5 es un diagrama de secuencia que muestra un ejemplo de estructura jerárquica y un procedimiento de cálculo de una clave usada en un sistema de comunicaciones móviles de acuerdo con una segunda realización de la presente invención.
[Fig. 6], la Fig. 6 es un diagrama de secuencia que muestra un procedimiento de restablecimiento intra eNB en el sistema de comunicaciones móviles de acuerdo con la segunda realización de la presente invención.
[Fig. 7], la Fig. 7 es un diagrama de secuencia que muestra un procedimiento de restablecimiento entre eNB en el sistema de comunicaciones móviles de acuerdo con la segunda realización de la presente invención.
[Fig. 8], la Fig. 8 es un diagrama que muestra un ejemplo de procedimiento de cálculo de una clave usada en un sistema de comunicaciones móviles de acuerdo con una técnica convencional.

Mejores modos para realizar la invención

(Sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención)

Un sistema de comunicaciones móviles de acuerdo con la primera realización se describe con relación a las Fig. 1 a la Fig. 4.

El sistema de comunicaciones móviles de acuerdo con esta realización es un sistema de comunicaciones móviles al que se aplica el esquema LTE, e incluye una pluralidad de centros de conmutación MME Nº 1, MME Nº 2, … y una pluralidad de estaciones base de radio eNB Nº 11, eNB Nº 12, eNB Nº 21, eNB Nº 22, …

Por ejemplo, una estación móvil UE se configura para comunicar, en la célula Nº 111 bajo el control de la estación base de radio eNB Nº 11, usando la estación base de radio eNB Nº 11 usando una cierta clave descrita anteriormente.

Además, en un procedimiento de restablecimiento para la estación móvil UE, una estación base de radio que gestiona la célula objetivo del restablecimiento (por ejemplo, la estación base de radio eNB Nº 12) se configura para adquirir las primeras claves $K_{eNB\ [n\ +\ m]}$, $K_{eNB\ [n\ +\ 2]}$ y similares para generar una cierta clave usada en las comunicaciones con la estación móvil UE, sin usar una clave intermedia K_{eNB^*} generada por una estación base de radio que gestiona una célula fuente del restablecimiento (por ejemplo, la estación base de radio eNB Nº 11).

La Fig. 2 muestra un ejemplo de una estructura jerárquica y el procedimiento de cálculo de una clave usada en el sistema de comunicaciones móviles de acuerdo con esta realización (esto es, una clave usada para calcular la cierta clave).

Como se muestra en la Fig. 2, una clave $K_{RRC\ IP}$ usada para "Protección de Integridad" en el protocolo RRC, una clave $K_{RRC\ Ciph}$ usada para el "Cifrado" en el protocolo RRC y una clave $K_{UP\ Ciph}$ usada para el "Cifrado" en el plano U de AS se generan usando una primera clave $K_{eNB\ [n]}$.

La primera clave $K_{eNB\ [n]}$ se calcula usando una clave maestra K_{ASME} según la fórmula dada a continuación.

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

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

En este punto la clave maestra K_{ASME} solo la conocen la estación móvil UE y el centro de conmutación MME, pero no debe ser conocida para la estación base de radio eNB.

Además NAS SN es el número de secuencia (SN) de un protocolo NAS que es el protocolo del plano C entre la estación móvil UE y el centro de conmutación MME (Estrato No de Acceso, NAS).

Después de esto, las operaciones del sistema de comunicaciones móviles de acuerdo con esta realización se describen con referencia a la Fig. 3 y la Fig. 4.

En primer lugar, el procedimiento de restablecimiento intra eNB (procedimiento de restablecimiento dentro de la estación base de radio) en el sistema de comunicaciones móviles de acuerdo con esta realización se describe con referencia a la Fig. 3.

Como se muestra en la Fig. 3, antes de comenzar los procedimientos de restablecimiento intra eNB, la estación móvil UE mantiene $K_{eNB\ [n]}$ y "KI (=n)" (etapa S1001), la estación base de radio eNB mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n+1]}$ y "K1 (=n)" (etapa S1002), y el centro de conmutación MME mantiene K_{ASME}, $K_{eNB\ [n+1]}$ y "K1 (=n)" (etapa S1003).

En la etapa S1004, donde la conexión de RRC se ha establecido entre la estación móvil UE y la estación base de radio eNB y se ha establecido la conexión S1 entre la estación base de radio eNB y el centro de conmutación MME, la estación móvil UE detecta el fallo del enlace de radio (RLF) en la conexión de RRC descrita anteriormente. Por ejemplo la estación móvil UE detecta el RLF en los siguientes casos.

- Cuando la RSRP (Potencia Recibida de la Señal de Referencia) en la conexión de RRC es menor de un umbral predeterminado durante un periodo de tiempo predeterminado.
- Cuando el procedimiento de acceso aleatorio no es satisfactorio.
- Cuando falla el procedimiento de transferencia.

Después de esto, la estación móvil UE realiza un procesamiento de selección de célula en la etapa S1005, y transmite, en la etapa S1006, la "Petición de Restablecimiento de la Conexión de RRC (señal de petición de restablecimiento)" a una célula seleccionada (o la estación base de radio eNB que gestiona la célula seleccionada) a través de un canal de control común.

En la etapa S1007, la estación base de radio eNB transmite un "Restablecimiento de la Conexión de RRC (señal de confirmación de restablecimiento)" a la estación móvil UE. El "Restablecimiento de la Conexión de RRC" puede incluir "KI (=n + 1)".

En este punto, la estación base de radio eNB mantiene $K_{eNB\ [n+1]}$ y "KI (= n + 1) (etapa S1008).

En la etapa S1109, la estación móvil UE calcula $K_{eNB\ [n+1]}$ a partir de la fórmula dada a continuación, en la etapa S1010, usando tal $K_{eNB\ [n+1]}$, transmite el "Restablecimiento Completo de la Conexión de RRC (señal de restablecimiento completo)" a la estación base de radio eNB.

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

En este punto, la estación móvil UE mantiene $K_{eNB\ [n+1]}$ y "KI (=n + 1)" (etapa S1011).

En la etapa S1012, la estación base de radio eNB transmite, al centro de conmutación MME, una "Conmutación de la Trayectoria S1 (señal de conmutación de trayectoria)" incluyendo "KI (= n + 1)".

En la etapa S1013, el centro de conmutación MME calcula $K_{eNB\ [n+2]}$ según la fórmula dada a continuación y, en la etapa S1014, transmite, a la estación base de radio eNB una "Confirmación de Conmutación de Trayectoria S1 (señal de confirmación de conmutación de trayectoria)" incluyendo $K_{eNB\ [n+2]}$ y "KI (=n + 1)".

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

En este punto, el centro de conmutación MME mantiene K_{ASME}, $K_{eNB\ [n+2]}$ y "KI (=n + 1)" (en la etapa S1015).

En la etapa S1016, la estación base de radio eNB recibe la "Confirmación Conmutación Trayectoria S1" y mantiene $K_{eNB\ [n+1]}$, $K_{eNB\ [n+2]}$ y "KI (= n + 1)".

Esto es, en este caso, la estación base de radio eNB que gestiona la célula objetivo del restablecimiento adquiere la primera clave $K_{eNB\ [n+2]}$ para generar una cierta clave a usar en la comunicaciones entre la estación móvil UE y la siguiente célula objetivo del restablecimiento para la estación móvil UE.

En la etapa S1017, la estación base de radio eNB transmite, a la estación móvil UE, una "Re-configuración de la Conexión de RRC" y en la etapa S1018, la estación móvil UE transmite, a la estación base de radio eNB, una "Re-

configuración de la Conexión de RRC Completa".

De acuerdo con el procedimiento descrito anteriormente, K_{eNB} y la cierta clave se actualizan en el procedimiento de restablecimiento intra eNB.

Como se muestra en la Fig. 4, antes del comienzo del procedimiento de restablecimiento intra eNB, la estación móvil UE mantiene $K_{eNB\ [n]}$ y "KI (=n)" (etapa S2001), la estación base de radio eNB Nº 1 mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n+1]}$, y "KI (=n)" (etapa S2002), y el centro de conmutación MME mantiene K_{ASME}, $K_{eNB\ [n+1]}$ y "K1 (=n)" (etapa S2003).

En la etapa S2004, la estación base de radio eNB Nº 1 transmite, a una estación base de radio vecina eNB Nº 2, una "Preparación X2 HO (señal de preparación de la transferencia)" incluyendo $K_{eNB\ [n+1]}$ y "KI (=n + 1)".

En la etapa S2005, la estación base de radio eNB Nº 2 almacena la $K_{eNB\ [n+1]}$ y "KI (=n + 1)" recibidas y, en la etapa S2006, transmite a la estación base de radio eNB Nº 1, una "Confirmación de Preparación X2 HO (señal de confirmación de preparación de la transferencia)".

Esto es, en este caso, la estación base de radio eNB Nº 2 que gestiona la célula objetivo del restablecimiento adquiere la primera clave $K_{eNB\ [n+1]}$ para generar una cierta clave a usar en las comunicaciones con la estación móvil UE.

En la etapa S2007, donde la conexión de RRC se ha establecido entre la estación móvil UE y la estación base de radio eNB Nº 1 y la conexión S1 se ha establecido entre la estación base de radio eNB N1 y el centro de conmutación MME, la estación móvil UE detecta una RLF en la conexión de RRC descrita anteriormente.

Después de esto, la estación móvil UE realiza un procesamiento de selección de célula en la etapa S2008, y transmite, en la etapa S2009, una "Petición de Restablecimiento de la Conexión de RRC (señal de petición de restablecimiento)" a una célula seleccionada (o la estación base objetivo de restablecimiento) eNB Nº 2 a través de un canal de control común.

En la etapa S2010, la estación base objetivo del restablecimiento eNB Nº 2 transmite un "Restablecimiento de la Conexión de RRC (señal de confirmación de restablecimiento)" a la estación móvil UE. El "Restablecimiento de la Conexión de RRC" puede incluir "KI (=n + 1)".

En la etapa S2010, la estación móvil UE calcula $K_{eNB\ [n+1]}$ a partir de la formula dada a continuación y en la etapa S2013, usando tal $K_{eNB\ [n+1]}$, transmite un "Restablecimiento de la Conexión de RRC Completo (señal de reconexión completa)" a la estación base objetivo del restablecimiento eNB Nº 2.

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

En este punto, la estación móvil UE mantiene $K_{eNB\ [n+1]}$ y "KI (=n + 1)" (etapa S2012).

En la etapa S2014, la estación base de radio eNB Nº 2 transmite, al centro de conmutación MME, "Conmutación de Trayectoria S1" (señal de conmutación de trayectoria)" incluyendo "KI (=n + 1)".

En la etapa S2015, la estación base de radio eNB Nº 2 transmite, a la estación móvil UE, la "Re-configuración de la Conexión de RRC" y en la etapa S2016, la estación móvil UE transmite, a la estación base de radio eNB Nº 2 una "Re-configuración de la Conexión de RRC Completa".

En la etapa S2017, el centro de conmutación MME calcula $K_{eNB\ [n+2]}$ a partir de la fórmula dada a continuación y, en la etapa S2019, transmite, a la estación base objetivo del restablecimiento eNB Nº 2, una "Confirmación de Conmutación de la Trayectoria S1 (señal de confirmación de conmutación de la trayectoria)" incluyendo $K_{eNB\ [n+2]}$ y "KI (= n + 1)".

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

En este caso, el centro de conmutación MME mantiene K_{ASME}, $K_{eNB\ [n+2]}$ y "KI (=n + 1)" (etapa S2018).

En la etapa S2010, la estación base objetivo del restablecimiento eNB Nº 2 recibe la "Confirmación de Conmutación de la Trayectoria S1" y mantiene $K_{eNB\ [n+1]}$, $K_{eNB\ [n+2]}$ y "KI (=n + 1)"

Esto es, en este punto, la estación base de radio eNB Nº 2 que gestiona la célula objetivo del restablecimiento adquiere la primera clave $K_{eNB\ [n+2]}$ para generar una cierta clave a usar en las comunicaciones entre la estación móvil UE y una célula objetivo del restablecimiento siguiente para la estación móvil UE.

De acuerdo con el procedimiento descrito anteriormente K_{eNB} y la cierta clave se actualizan en el procedimiento de restablecimiento intra eNB.

(Operaciones y efectos del sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención)

En el sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención $K_{eNB\ [n+1]}$ y similares a usar en la estación base de radio eNB o eNB Nº 2 que gestiona la célula objetivo del restablecimiento se pueden generar a través de un procedimiento simplificado.

(Sistema de comunicaciones móviles de acuerdo con una segunda realización de la presente invención)

Refiriéndonos a las Fig. 5 a la Fig. 7 se describe un sistema de comunicaciones móviles de acuerdo con una segunda realización de la presente invención centrándonos en las diferencias con el sistema de comunicaciones móviles descrito anteriormente de acuerdo con la primera realización de la presente invención.

La Fig. 5 muestra un ejemplo de la estructura jerárquica y el procedimiento de cálculo de una clave usada en el sistema de comunicaciones móviles de acuerdo con esta realización (esto es, una clave usada para calcular la cierta clave).

Como se muestra en la Fig. 5, se generan una clave K_{RRC_IP} usada para la "Protección de Integridad" en el protocolo de RRC, una clave K_{RRC_Ciph} usada para el "Cifrado" en el protocolo RRC, y una clave K_{UP_Ciph} usada para el "Cifrado" en el plano U de AS usando $K_{eNB\ [n][m]}$.

$K_{eNB\ [n][m]}$ se calcula usando $K_{eNB\ [n]}$ a partir de las fórmulas dadas siguientes

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

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

Además, $K_{eNB\ [n]}$ se calcula a partir de las fórmulas dadas a continuación usando K_{ASME}.

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

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

Después de esto, se describen las operaciones del sistema de comunicaciones móviles de acuerdo con esta realización con referencia a la Fig. 6 y la Fig. 7.

En primer lugar se describe el procedimiento de restablecimiento intra eNB (procedimiento de restablecimiento dentro de la estación base de radio) en el sistema de comunicaciones móviles de acuerdo con esta realización con referencia a la Fig. 6.

Como se muestra en la Fig. 11, antes del comienzo del procedimiento de restablecimiento intra eNB, la estación móvil UE mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n][m]}$, "KI (= m)" (etapa S3001), la estación base de radio eNB mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n+1]}$, $K_{eNB\ [n][m]}$, "KI (=n)" y "RC (=m)" (etapa S3002), y el centro de conmutación MME mantiene K_{ASME}, $K_{eNB\ [n+1]}$ y "K1 (=n)" (etapa S3003).

En la etapa S3004, donde se ha establecido la conexión de RRC entre la estación móvil UE y la estación base de radio eNB y se ha establecido la conexión de S1 entre la estación base de radio eNB y el centro de conmutación MME, la estación móvil UE detecta el fallo del enlace de radio (RLF) en la conexión de RRC descrito anteriormente.

Después de esto, la estación móvil UE realiza un procedimiento de selección de célula en la etapa S3005, y transmite, en la etapa S3006 una "Petición de Restablecimiento de la Conexión de RRC (señal de petición de restablecimiento)" a una célula seleccionada (o la estación base de radio eNB que gestiona la célula seleccionada) a través un canal de control común.

En la etapa S3007, la estación base de radio eNB transmite a la estación móvil UE un "Restablecimiento de la Conexión de RRC (señal de confirmación de restablecimiento) incluyendo "KI (=n)" y "RC (= m + 1)".

En este caso, en la etapa S3008, la estación móvil UE calcula $K_{eNB\ [n][m]}$ a partir de la fórmula dada siguiente y, en la etapa S3009, mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n][m+1]}$, "KI (=n + 1)" y "RC (m + 1)".

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

De forma similar, en la etapa S3010, la estación base de radio eNB calcula $K_{eNB\ [n]}$ a partir de la fórmula dada a continuación, y en la etapa S3011, mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n+1]}$, $K_{eNB\ [n][m+1]}$, "KI (n + 1)" Y "RC (=m + 1)".

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

En la etapa S3012, la estación móvil UE transmite a la estación base de radio eNB un "Restablecimiento de la Conexión de RRC Completa (señal de restablecimiento competo)" usando la $K_{eNB\ [n+1]}$, descrita anteriormente.

En la etapa S3013, la estación base de radio eNB transmite, a la estación móvil UE, una "Re-configuración de la Conexión de RRC" y en la etapa S3014, la estación móvil UE transmite a la estación base de radio eNB, una "Re-configuración de la Conexión de RRC Completa".

De acuerdo con esta realización, se puede eliminar la "Conmutación de Trayectoria" en el procedimiento de restablecimiento intra eNB.

En segundo lugar, el procedimiento de restablecimiento intra eNB (procedimiento de e-establecimiento entre estaciones móviles diferentes) en el sistema de comunicaciones móviles de acuerdo con esta realización se describe con referencia a la Fig. 7.

Como se muestra en la Fig. 7, antes de comenzar el procedimiento de restablecimiento intra eNB, la estación móvil UE mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n][m]}$, "KI (=n)" y "RC (=m)" (etapa S4001), la estación base de radio eNB Nº 1 mantiene $K_{eNB\ [n]}$, $K_{eNB\ [n + 1]}$, $K_{eNB\ [n][m]}$, "KI (=n)" y "RC (=m)" (etapa S4002), y el centro de conmutación MME mantiene K_{ASME}, $K_{eNB\ [n + 1]}$ y "K1 (=n)" (etapa S4003).

En la etapa S4004, la estación base de radio eNB Nº 1 transmite a una estación base de radio vecina eNB Nº 2, una "X2 HO Preparación (señal de preparación de transferencia)" incluyendo $K_{eNB\ [n + 1]}$ y "KI (= n + 1)".

En las etapas S4004 y S4006, la estación base de radio eNB Nº 2 almacena $K_{eNB\ [n + 1]}$, $K_{eNB\ [n + 1][0]}$, "KI (=n + 1)" y "RC (=0)". En este caso, asumimos que $K_{eNB\ [n + 1][0]} = K_{eNB\ [n+1]}$.

En la etapa S4007, la estación base de radio eNB Nº 2 transmite a la estación base de radio eNB Nº 1 una "Confirmación de Preparación X2 HO (señal de confirmación de preparación de transferencia)".

Esto es, en este punto, la estación base de radio eNB Nº 2 que gestiona la célula objetivo del restablecimiento adquiere la primera clave $K_{eNB\ [n + 1][0]}$ para la generación de una cierta clave a usar en la comunicación con la estación móvil UE.

En la etapa S4008, donde se ha establecido la conexión de RRC entre la estación móvil UE y la estación base de radio eNB Nº 1 y se ha establecido la conexión S1 entre la estación base de radio eNB Nº 1 y el centro de conmutación MME, la estación móvil UE detecta la RLF en la conexión de RRC descrita anteriormente.

Después de esto, la estación móvil UE realiza un procesamiento de selección de célula en la etapa S4009, y transmite, en la etapa S4010, una "Petición de Restablecimiento de la Conexión de RRC (señal de petición de restablecimiento)" a la célula objetivo del restablecimiento (o la estación base de radio objetivo del restablecimiento) eNB Nº 2 a través de un canal de control común.

En la etapa S4011, la estación base de radio objetivo del restablecimiento eNB Nº 2 transmite, a la estación móvil UE, un "Restablecimiento de la Conexión de RRC" incluyendo "KI (=n + 1)" y "RC (=0)".

En la etapa S4012, la estación móvil UE calcula $K_{eNB\ [n + 1]}$ y $K_{eNB\ [n + 1][0]}$ a partir de las fórmulas dadas a continuación, y en la etapa S4013, mantiene $K_{eNB\ [n + 1]}$, $K_{eNB\ [n + 1][0]}$, "KI (=n + 1)" y "RC (=0)".

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

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

En la etapa S4014, la estación móvil UE transmite a la estación base de radio objetivo del restablecimiento eNB Nº 2 un "Restablecimiento de la Conexión de RRC Completo" usando la $K_{eNB\ [n + 1]}$ mencionada anteriormente.

En la etapa S4015, la estación base de radio objetivo del restablecimiento eNB Nº 2 transmite, al centro de conmutación MME, una "Conmutación de Trayectoria S1" incluyendo "KI (=n + 1)".

En la etapa S4016, la estación base de radio objetivo del restablecimiento eNB Nº 2 transmite, a la estación móvil UE, una "Re-configuración de Conexión de RRC" y en la etapa S4017, la estación móvil UE transmite a la estación base de radio objetivo del restablecimiento eNB Nº 2 una "Re-configuración de Conexión RRC Completa".

En la etapa S4018, el centro de conmutación MME calcula $K_{eNB\ [n + 2]}$ a partir de una fórmula dada a continuación y, en la etapa S4019, se mantienen K_{ASME}, $K_{eNB\ [n + 2]}$ y "KI (=n + 1)".

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

En la etapa S4020, el centro de conmutación MME transmite a la estación base de radio objetivo del restablecimiento eNB Nº 2, una "Confirmación de Conmutación de Trayectoria S1" incluyendo $K_{eNB\ [n + 2]}$ y "KI (=n + 1)".

En este caso, en la etapa S4021, la estación base de radio objetivo del restablecimiento eNB Nº 2 mantiene $K_{eNB\ [n + 1]}$, $K_{eNB\ [n + 2]}$, "KI (=n + 1)", $K_{eNB\ [n + 1][0]}$ y "RC (=0)".

Como se muestra en la Fig. 6 y la Fig. 7, introduciendo K_{eNB} en la actualización de la estación base de radio usando el parámetro "RC", se puede actualizar K_{eNB} mientras que se elimina una pregunta al centro de conmutación MME.

Entre tanto, en los procedimientos mostrados en la Fig. 6 y la Fig. 7, el parámetro "RC" se puede omitir del

"Restablecimiento RRC RRC".

Cuando se omite el parámetro "RC" del "Restablecimiento RRC RRC" se puede determinar la necesidad de incrementar "RC" determinando si el parámetro "KI" se ha incrementado o no se ha incrementado.

Si se ha incrementado "KI", "RC" se puede reiniciar a "O", mientras que si "KI" no se ha incrementado, se puede incrementar "RC".

Como alternativa, si se omite el parámetro "RC" del "Restablecimiento RRC RRC", la estación móvil UE puede, en base a ensayo, mantener el valor presente de "RC", incrementar "RC" o reiniciar "RC a "O", y a continuación comprobar la "integridad" con respecto a un mensaje recibido para cada uno de los casos para determinar de forma autónoma cual de los casos es el correcto.

(Modificación)

Obsérvese que la operación del centro de conmutación descrito anteriormente MME, la estación móvil UE y la estación base de radio eNB se puede implementar por medio de hardware, un módulo software ejecutado por un procesador, o una combinación de ambos.

El módulo software se puede proporcionar en cualquier tipo de almacenamiento tal como RAM (Memoria de Acceso Aleatorio), una memoria flash, una ROM (Memoria de Solo Lectura), una EPROM (ROM Programable que se puede Borrar) una EEPROM (ROM que se puede Borrar y Programar Electrónicamente), un registro, un disco duro, un disco extraíble, o un CD-ROM.

El medio de almacenamiento está conectado al procesador de modo que el procesador puede leer y escribir la información desde y al medio de almacenamiento. También, el medio de almacenamiento puede estar integrado en el procesador. También, el medio de almacenamiento y el procesador se pueden proporcionar en un ASIC. El ASIC se puede proporcionar en el centro de conmutación MME, la estación móvil UE y la estación base de radio eNB. También el medio de almacenamiento y el procesador se pueden proporcionar en el centro de conmutación MME, la estación móvil UE y la estación base de radio eNB como un componente discreto.

REIVINDICACIONES

1. Un procedimiento de comunicaciones móviles para la comunicación entre una estación móvil (UE) y una estación base de radio (eNB) a través de un enlace de radio usando una cierta clave (K_{RRC_CIPH}, K_{RRC_IP}, K_{UP_CIPH}), comprendiendo el procedimiento la etapa de:

(A) transmitir (S1006, S2009, S3006, S4010), desde la estación móvil (UE) a la estación base de radio (eNB), una señal de petición de restablecimiento al detectar fallo del enlace de radio (S1004, S2007, S3004, S4008) y
(B) realizar una re-configuración del enlace de radio entre la estación móvil (UE) y la estación base de radio (eNB) en respuesta a la transmisión de la señal de petición de restablecimiento; en donde

en la etapa (B), la estación base de radio transmite (S1007, S2010, S3007, S4011) a la estación móvil (UE) una señal de confirmación de restablecimiento, incluyendo un parámetro de índice para identificar una segunda clave ($K_{eNB\ [n]}$) para calcular una primera clave ($K_{eNB\ [n+1]}$) para generar una cierta clave que debe usarse en la estación base de radio (eNB) después de un procedimiento de restablecimiento, y la estación móvil (UE) calcula la primera clave ($K_{eNB\ [n+1]}$) que debe almacenarse en la estación móvil usando la segunda clave ($K_{eNB\ [n]}$) identificada por el parámetro de índice incluido en la señal de confirmación de restablecimiento recibida.

2. El procedimiento de comunicaciones móviles de acuerdo con la reivindicación 1, en el que
la primera clave la identifican un primer parámetro de índice y un segundo parámetro de índice; y
en la etapa (B), la estación base de radio (eNB) transmite, a la estación móvil (UE), la señal de confirmación de restablecimiento que incluye el primer parámetro de índice y no incluye el segundo parámetro de índice.

3. El procedimiento de comunicaciones móviles de acuerdo con la reivindicación 2 en el que
en la etapa (B), la estación móvil (UE) reinicia el segundo parámetro de índice cuando el primer parámetro de índice incluido en la señal de confirmación de restablecimiento recibida se incrementa, y se incrementa el segundo parámetro del índice cuando el primer parámetro de índice no se incrementa.

4. Una estación base de radio (eNB) que comunica con una estación móvil (UE) a través de un enlace de radio usando una cierta clave (K_{RRC_CIPH}, K_{RRC_IP}, K_{UP_CIPH}), comprendiendo la estación base de radio (eNB):

una unidad de recepción configurada para recibir una señal de petición de restablecimiento (S1006, S2009, S3006, S4010) de la estación móvil (UE), y
una unidad de re-configuración configurada para realizar una re-configuración del enlace de radio con la estación móvil (UE), de acuerdo con la señal de petición de restablecimiento, en el que
la unidad de re-configuración se configura para transmitir a la estación móvil (UE) una señal de confirmación de restablecimiento (S1007, S2010, S3007, S4011) que incluye un parámetro de índice para identificar una segunda clave ($K_{eNB\ [n]}$) para calcular una primera clave $K_{eNB\ [n+1]}$ para generar una cierta clave que debe usarse en la estación base de radio (eNB) después de un procedimiento de restablecimiento.

5. La estación base de radio (eNB) de acuerdo con la reivindicación 4,
en donde
la primera clave la identifican un primer parámetro de índice y un segundo parámetro de índice; y la unidad de re-configuración se configura para transmitir a la estación móvil (UE) la señal de confirmación de restablecimiento que incluye el primer parámetro de índice y no incluye el segundo parámetro de índice.

6. Una estación móvil (UE) que comunica con una estación base de radio (eNB) a través de un enlace de radio usando una cierta clave (K_{RRC_CIPH}, K_{RRC_IP}, K_{UP_CIPH}), comprendiendo la estación móvil (UE):

una unidad de transmisión configurada para transmitir a la estación base de radio (eNB) una señal de petición de restablecimiento (S1006, S2009, S3006, S4010) que detecta el fallo del enlace de radio; y
una unidad de re-configuración configurada para realizar una re-configuración del enlace de radio con la estación base (eNB);
en donde
la unidad de re-configuración está configurada para calcular una primera clave que debe almacenarse en la estación móvil (UE) cuando se recibe desde la estación base de radio (eNB) una señal de confirmación de restablecimiento, que incluye un parámetro de índice para identificar una segunda clave ($K_{eNB\ [n]}$) para calcular la primera clave ($K_{eNB\ [n+1]}$), siendo la primera clave una clave para generar una cierta clave que debe usarse en la estación base de radio (eNB) después de un procedimiento de restablecimiento.

7. La estación móvil (UE) de acuerdo con la reivindicación 6, en la que
la primera clave la identifica un primer parámetro de índice y un segundo parámetro de índice; y
la unidad de re-configuración se configura para calcular la primera clave que debe almacenarse en la estación móvil (UE) usando la segunda clave identificada por el primer parámetro de índice, cuando se recibe la señal de confirmación de restablecimiento que incluye el primer parámetro de índice y no incluye el segundo parámetro de índice.

8. La estación móvil (UE) de acuerdo con la reivindicación 7, en la que

la unidad de re-configuración se configura para reiniciar el segundo parámetro de índice cuando se incrementa el primer parámetro de índice incluido en la señal recibida de confirmación del restablecimiento, y para incrementar el segundo parámetro de índice cuando no se incrementa el primer parámetro de índice.

FIG. 1

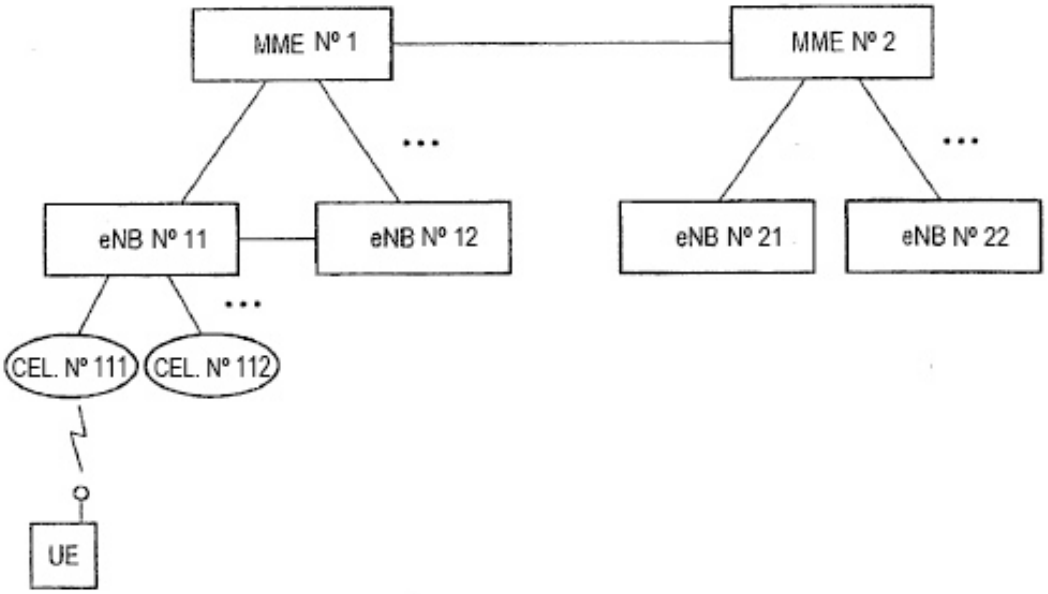

MME Nº 1
MME Nº 2
eNB Nº 11
eNB Nº 12
eNB Nº 21
eNB Nº 22
CEL. Nº 111
CEL. Nº 112
UE

FIG. 2

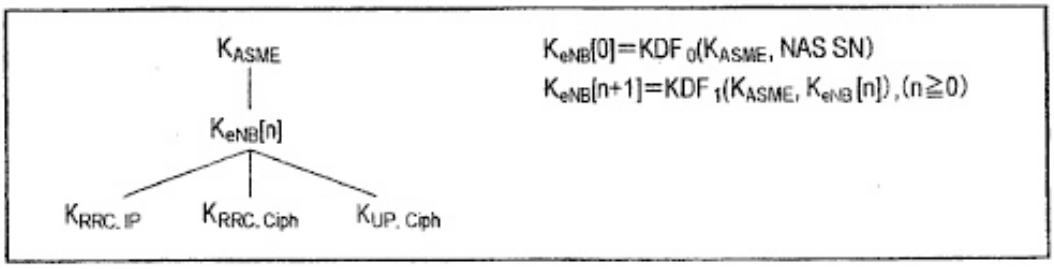

K_{ASME}
$K_{eNB}[n]$
$K_{RRC.IP}$
$K_{RRC.Ciph}$
$K_{UP.Ciph}$
$K_{eNB}[0]=KDF_0(K_{ASME}, NAS\ SN)$
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n]), (n \geqq 0)$

FIG. 3

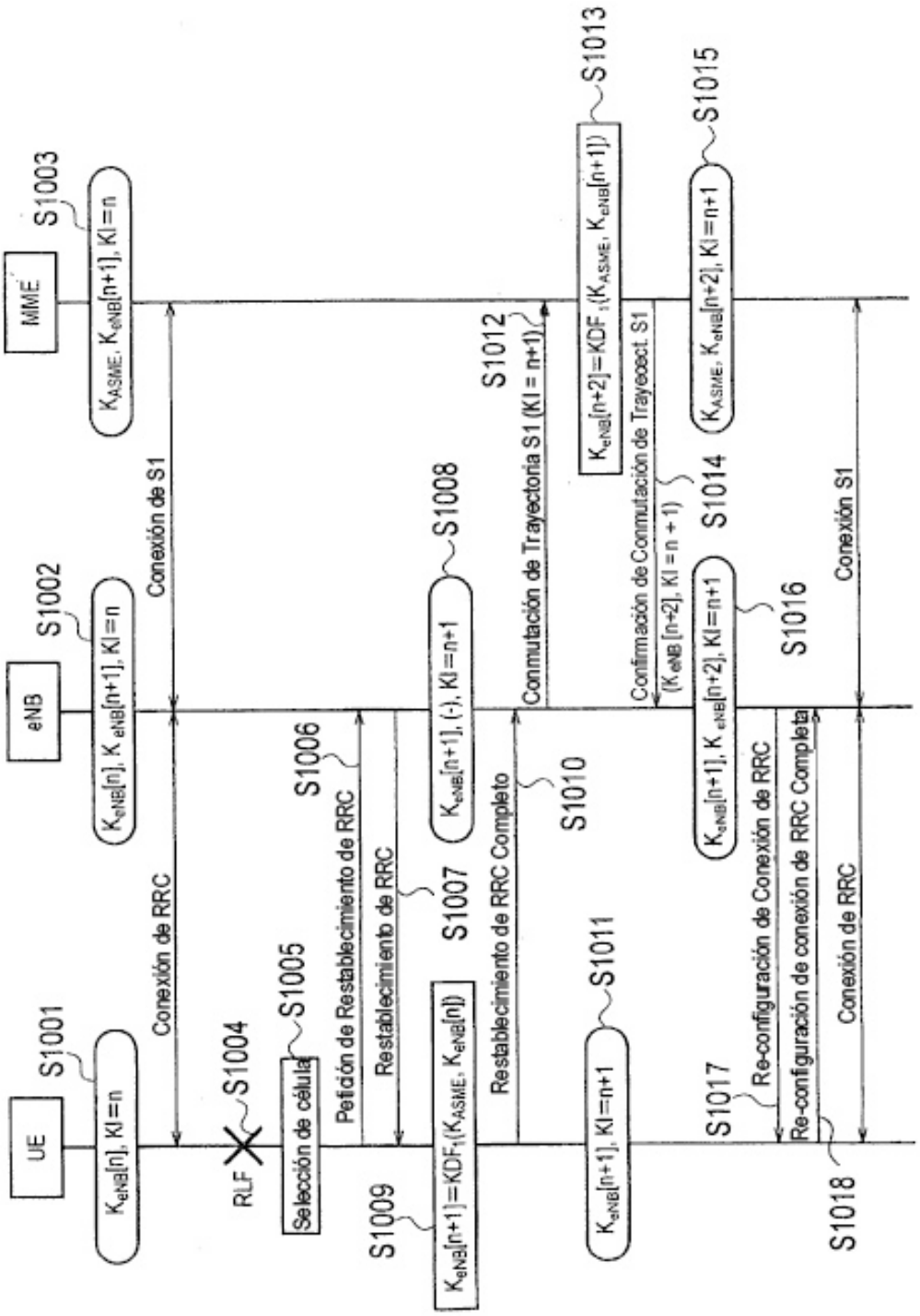

UE
eNB
MME
S1001
S1002
S1003
$K_{eNB}[n]$, KI=n
$K_{eNB}[n]$, $K_{eNB}[n+1]$, KI=n
K_{ASME}, $K_{eNB}[n+1]$, KI=n
Conexión de RRC
Conexión de S1
RLF
S1004
Selección de célula
S1005
Petición de Restablecimiento de RRC
S1006
Restablecimiento de RRC
S1007
$K_{eNB}[n+1]$, (-), KI=n+1
S1008
S1009
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n])$
Restablecimiento de RRC Completo
S1010
Conmutación de Trayectoria S1 (KI = n+1)
S1012
$K_{eNB}[n+2]=KDF_1(K_{ASME}, K_{eNB}[n+1])$
S1013
Confirmación de Conmutación de Trayectoria S1
$(K_{eNB}[n+2]$, KI = n +1)
S1014
K_{ASME}, $K_{eNB}[n+2]$, KI=n+1
S1015
$K_{eNB}[n+1]$, KI=n+1
S1011
$K_{eNB}[n+1]$, $K_{eNB}[n+2]$, KI=n+1
S1016
S1017
Re-configuración de Conexión de RRC
Re-configuración de conexión de RRC Completa
S1018
Conexión de RRC
Conexión S1

FIG. 4

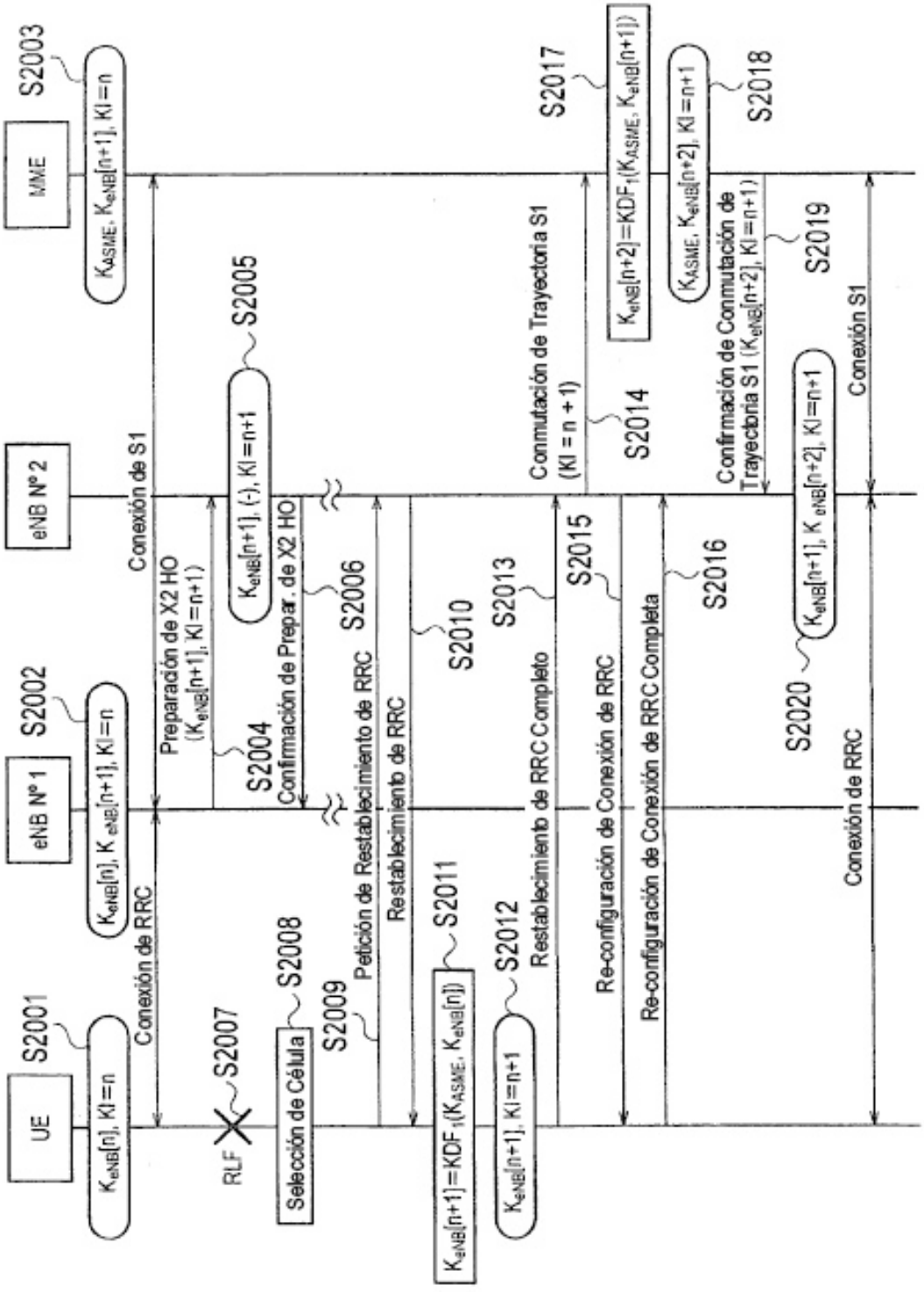

UE
eNB Nº 1
eNB Nº 2
MME
S2001
S2002
S2003
S2004
S2005
S2006
S2007
S2008
S2009
S2010
S2011
S2012
S2013
S2014
S2015
S2016
S2017
S2018
S2019
S2020
$K_{eNB}[n]$, KI=n
$K_{eNB}[n]$, $K_{eNB}[n+1]$, KI=n
K_{ASME}, $K_{eNB}[n+1]$, KI=n
Conexión de RRC
Conexión de S1
Preparación de X2 HO
($K_{eNB}[n+1]$, KI=n+1)
$K_{eNB}[n+1]$, (-), KI=n+1
Confirmación de Prepar. de X2 HO
RLF
Selección de Célula
Petición de Restablecimiento de RRC
Restablecimiento de RRC
$K_{eNB}[n+1]$=KDF_1(K_{ASME}, $K_{eNB}[n]$)
$K_{eNB}[n+1]$, KI=n+1
Restablecimiento de RRC Completo
Conmutación de Trayectoria S1
(KI = n +1)
Re-configuración de Conexión de RRC
Re-configuración de Conexión de RRC Completa
$K_{eNB}[n+2]$=KDF_1(K_{ASME}, $K_{eNB}[n+1]$)
K_{ASME}, $K_{eNB}[n+2]$, KI=n+1
Confirmación de Conmutación de Trayectoria S1 ($K_{eNB}[n+2]$, KI=n+1)
$K_{eNB}[n+1]$, $K_{eNB}[n+2]$, KI=n+1
Conexión S1
Conexión de RRC

FIG. 5

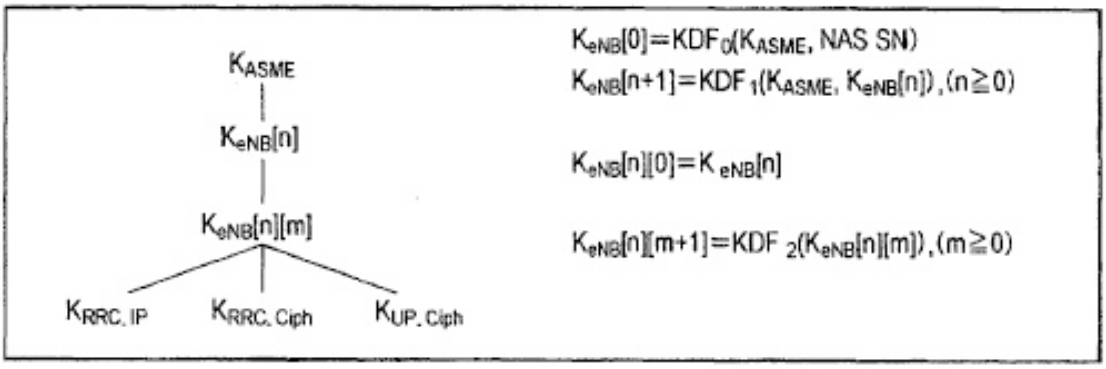

K_{ASME}
$K_{eNB}[n]$
$K_{eNB}[n][m]$
$K_{RRC.IP}$
$K_{RRC.Ciph}$
$K_{UP.Ciph}$
$K_{eNB}[0]=KDF_0(K_{ASME}, NAS\ SN)$
$K_{eNB}[n+1]=KDF_1(K_{ASME}, K_{eNB}[n]), (n \geqq 0)$
$K_{eNB}[n][0]=K_{eNB}[n]$
$K_{eNB}[n][m+1]=KDF_2(K_{eNB}[n][m]), (m \geqq 0)$

FIG. 6

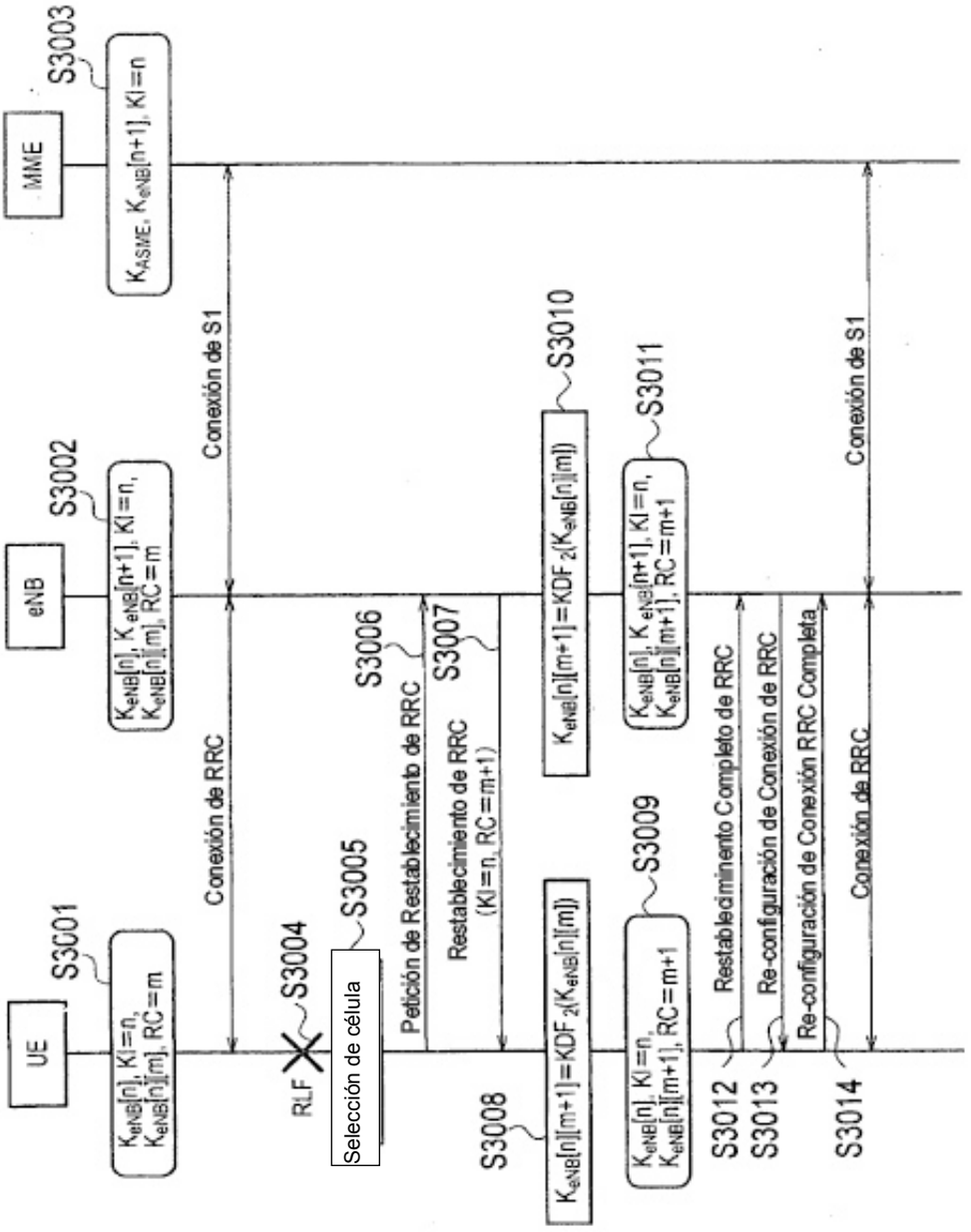

UE
eNB
MME
S3001
S3002
S3003
S3004
S3005
S3006
S3007
S3008
S3009
S3010
S3011
S3012
S3013
S3014
Conexión de RRC
Conexión de S1
RLF
Selección de célula
Petición de Restablecimiento de RRC
Restablecimiento de RRC
(KI=n, RC=m+1)
Restablecimiento Completo de RRC
Re-configuración de Conexión de RRC
Re-configuración de Conexión RRC Completa
Conexión de RRC
Conexión de S1

FIG. 7

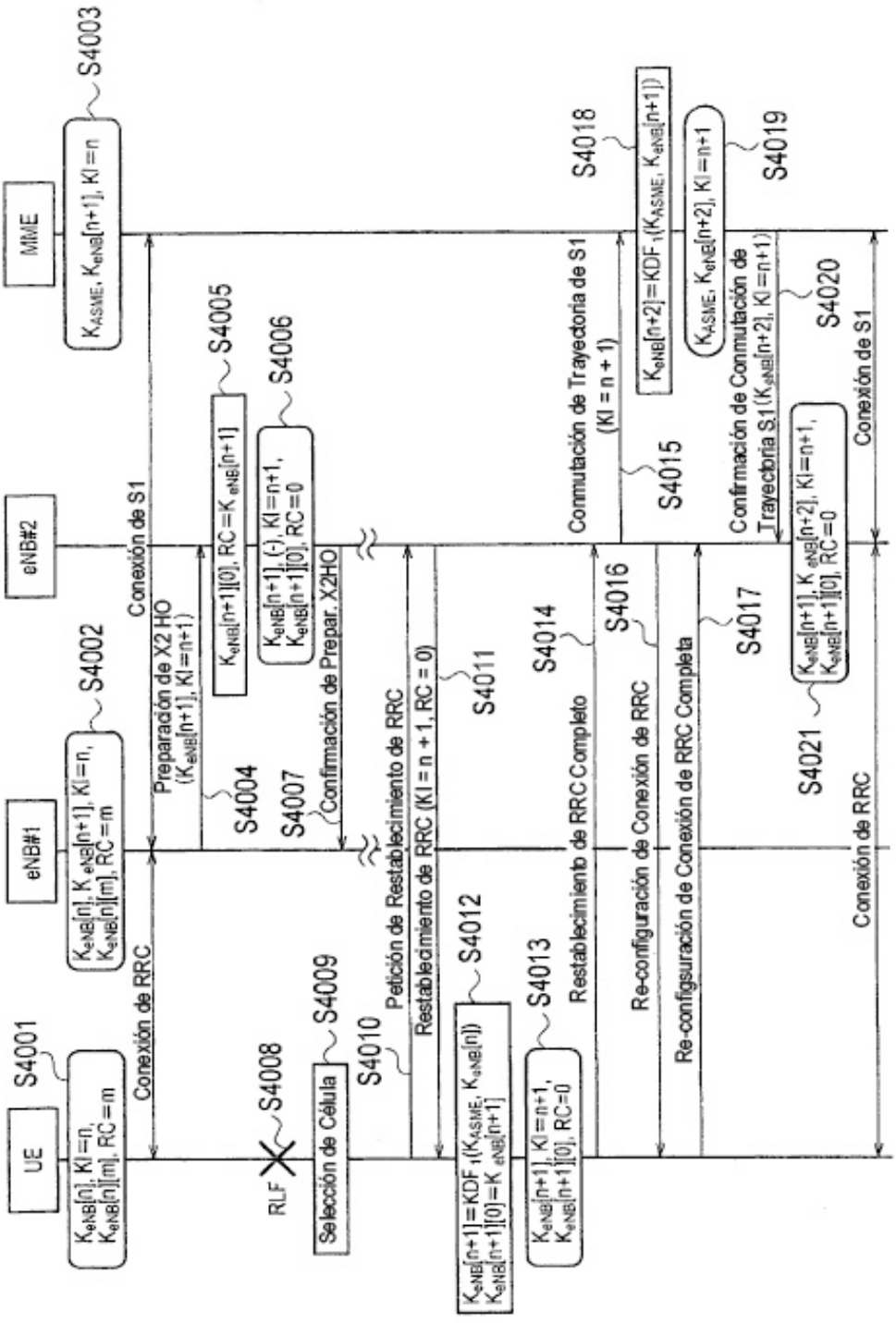
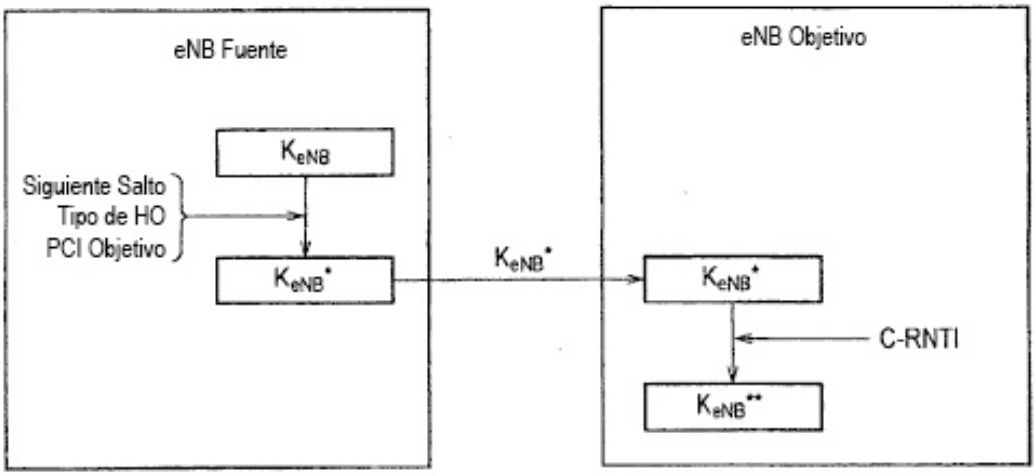

UE
eNB#1
eNB#2
MME
S4001
S4002
S4003
S4004
S4005
S4006
S4007
S4008
S4009
S4010
S4011
S4012
S4013
S4014
S4015
S4016
S4017
S4018
S4019
S4020
S4021
Conexión de RRC
Preparación de X2 HO
Conexión de S1
Confirmación de Prepar. X2HO
RLF
Selección de Célula
Petición de Restablecimiento de RRC
Restablecimiento de RRC (KI = n + 1, RC = 0)
Restablecimiento de RRC Completo
Re-configuración de Conexión de RRC
Re-configsuración de Conexión de RRC Completa
Conmutación de Trayectoria de S1 (KI = n + 1)
Confirmación de Conmutación de Trayectoria S1
Conexión de S1
Conexión de RRC

FIG. 8


eNB Fuente
eNB Objetivo
K_{eNB}
Siguiente Salto
Tipo de HO
PCI Objetivo
K_{eNB}^*
K_{eNB}^*
K_{eNB}^*
C-RNTI
K_{eNB}^{**}