(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 190**

(51) Int. CI.:
H04W 36/00 (2009.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09806756 .4**
(96) Fecha de presentación: **14.08.2009**
(97) Número de publicación de la solicitud: **2271143**
(97) Fecha de publicación de la solicitud: **05.01.2011**

(54) Título: **Procedimiento de comunicaciones móviles, estación base de radio, y estación móvil**

(30) Prioridad:
15.08.2008 JP 2008209386

(45) Fecha de publicación de la mención BOPI:
07.11.2012

(45) Fecha de la publicación del folleto de la patente:
07.11.2012

(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 y
ZUGENMAIER, ALF

(74) Agente/Representante:
CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de comunicaciones móviles, estación base de radio, y estación móvil

Campo técnico

La presente invención se refiere a un procedimiento de comunicaciones móviles, a una estación base de radio y a una estación móvil.

Técnica anterior

En el sistema LTE (Evolución a Largo Plazo), se toman medidas de seguridad para el "AS (Estrato de Acceso)" que es para la comunicación entre una estación móvil UE y una estación base de radio eNB.

Específicamente, en el sistema de LTE, el "Cifrado del plano C", la "Protección de la Integridad del plano C" y el "Cifrado del plano U" se emplean como tales medidas de seguridad.

A este respecto, se usa una clave $K_{RRC,\ ciph}$ cuando se realiza el Cifrado del plano C, se usa una clave $K_{RRC,\ IP}$ cuando se realiza la Protección de Integridad del plano C, y se usa una clave $K_{UP,\ ciph}$ cuando se realiza el cifrado del plano U. Todas estas claves se generan a partir de una clave de la estación base K_{eNB}.

La Fig. 5(a) muestra una estructura de capa típica de las claves usadas en el sistema de LTE. En este caso, una clave K_{ASME} es una clave conocida solamente para la MME de la estación superior y una estación móvil UE, y se usa para generar una clave de la estación base K_{eNB}.

Obsérvese que, la estructura de capas de las claves usadas en el sistema de LTE puede tener una forma como se muestra en la Fig. 5(b), ya que la generación de la clave de la estación base K_{eNB} requiere un parámetro llamado "NH (Salto Próximo)" que se genera a partir de la clave K_{ASME}.

Mientras tanto, del lado de la red, se configura una clave de la estación base K_{eNE} a gestionar por la estación móvil UE por cada una de las estaciones base de radio eNB, y a actualizar cuando la estación móvil correspondiente UE realiza una transferencia.

La clave de la estación base K_{eNB} también se gestiona por la estación móvil UE de modo que la estación móvil UE realiza la comunicación con la estación base de radio eNB. Usando la misma clave de la estación base K_{eNB}, la estación base de radio eNB y la estación móvil UE pueden realizar una comunicación con seguridad.

A continuación, se da una breve descripción de un procedimiento para la actualización de una clave de la estación base K_{eNB} con referencia a la Fig. 6.

En la Etapa (1), cuando se establece una conexión para una estación móvil UE, una MME de la estación superior genera una clave inicial temporal (K_{eNB}) sobre la base de una clave K_{ASME} y un "NAS SN (un número de secuencia en NAS = Estrato no de Acceso)".

En la Etapa (2), la MME de la estación superior notifica a la estación base de radio eNB Nº 1 de la clave inicial temporal (K_{eNB}) como una clase intermedia K_{eNB}*. En la Etapa (3), la estación base de radio eNB Nº 1 almacena la clave intermedia recibida K_{eNB}* sin cambiarla como una clave de la estación base K_{eNB}.

En la Etapa (11), la MME de la estación superior también genera un parámetro NH* sobre la base de la clave K_{ASME} y la clave inicial temporal K_{eNB}*, y notifica a la estación base de radio eNB Nº 1 del parámetro NH*.

En la Etapa (12), la estación base de radio eNB Nº 1 almacena el parámetro recibido NH* sin cambiarlo como un parámetro NH.

Consideremos un caso en el que la estación móvil UE realiza después de esto una transferencia desde una célula Nº 1 bajo el control de la estación base de radio eNB Nº 1 a la célula Nº 2 bajo el control de una estación base de radio eNB Nº 2. En este caso la estación base de radio eNB Nº 1 genera una clave intermedia K_{eNB}* en la Etapa (4) introduciendo la clave de la estación base actual K_{eNB} y la PCI (ID de la Célula Física) de la Célula Nº 2 en una primera sección, más concretamente, sobre la base de la primera función (función de deducción de claves = KDF (K_{eNB}, PCI), y notifica a la estación base de radio eNB Nº 2 de la clave intermedia K_{eNB}*.

Como alternativa, la estación base de radio eNB Nº 1 genera una clave intermedia K_{eNB}* en la etapa (13) introduciendo el parámetro actual de NH y la PCI de la célula Nº 2 en una primera función, más concretamente, sobre la base de la primera función (función de deducción de claves) = KDF (NH, PCI), y notifica a la estación base de radio eNB Nº 2 de la clave intermedia K_{eNB}*, cuando la estación móvil UE realiza una transferencia desde la célula Nº 1 bajo el control de la estación base de radio eNB Nº 1 a la célula Nº 2 bajo el control de la estación base de radio eNB Nº 2.

En tal procesamiento de cálculo para la clave intermedia K_{eNB}*, la clave se actualiza sobre la base de la PCI. La operación para la actualización de la clave sobre la base de la PCI como se ha descrito anteriormente se llama "atadura de PCI".

En esta caso, la estación base de radio eNB Nº 1 también notifica a la estación base de radio eNB Nº 2 de un "identificador de aumento del índice (indicador de aumento del índice)" que indica cual de las KDF (K_{eNB}, PCI) y KDF (NH, PCI) se usa como base para generar la clave intermedia K_{eNB}*.

La estación base de radio eNB Nº 2 que ha recibido la clave intermedia K_{eNB}* juzga si realizar o no una "atadura de C-RNTI" para la clave intermedia K_{eNB}*, sobre la base del "identificador de aumento del índice".

Específicamente, si la estación base de radio eNB Nº 2 reconoce del "identificador de aumento del índice" que la clave intermedia K_{eNB}* se genera sobre la base de la KDF (K_{eNB}, PCI), la estación base de radio eNB Nº 2 genera una clave de la estación base K_{eNB} en la Etapa (5) introduciendo la clave intermedia K_{eNB}* y el identificador de la estación móvil C-RNTI en una segunda función, más concretamente, sobre la base de KDF (K_{eNB}*, C-RNTI). En este caso, el identificador de la estación móvil C-RNTI se asigna temporalmente a la estación móvil UE en la célula Nº 2.

Por otra parte, si la estación base de radio eNB Nº 2 reconoce del "identificador de aumento del índice" que la clave intermedia K_{eNB}* se genera sobre la base de un parámetro actual NH, la estación base de radio eNB Nº 2 fija la clave intermedia recibida K_{eNB}* como una clave de la estación base K_{eNB} en la Etapa (14).

Obsérvese que, la estación base de radio eNB Nº 2 adquiere nuevamente un parámetro NH de la MME de la estación superior, cuando la MME de la estación superior realiza una "Conmutación de Trayectoria", en preparación para una siguiente transferencia para la estación móvil UE.

Además, la estación base de radio eNB Nº 1 notifica a la estación móvil UE de un parámetro de NCC (Cuenta de Encadenamiento de NH) a través de una señal de comando de transferencia (Comando de Transferencia). En este punto, el parámetro NCC indica un número para el parámetro actual de NH.

La estación móvil UE actualiza una clave de la estación base actual $K_{eNB[m]}$ con la siguiente fórmula para adquirir una clave de la estación base $K_{eNB[m+1]}$ si el parámetro recibido de NCC es el mismo que la NCC mantenida en la misma.

$$K_{eNB}^* = KDF\ (K_{eNB\ [m]},\ PCI)$$

$$K_{eNB\ [m+1]} = KDF\ (K_{eNB}^*,\ C - RNTI)$$

Por el contrario, si el parámetro recibido de NCC es mayor que la NCC mantenida en la estación móvil UE, la estación móvil UE repite el cálculo con las siguientes fórmulas y actualiza el parámetro NH hasta que la NCC mantenida en el mismo se hace igual al parámetro de NCC recibido. La estación móvil UE aumenta en uno la NCC mantenida en la misma en cada cálculo con la siguiente fórmula:

$$NH^* = KDF\ (K_{ASME},\ NH\ [m])$$

$$NH\ [m + 1] = NH^*$$

Con el procedimiento mencionado anteriormente, la clave de la estación base K_{eNB} se actualiza tanto en la estación móvil UE como en la estación base de radio eNB.

Mientras tanto, cuando falla una transferencia por alguna razón o cuando se produce un problema con el enlace de radio (Fallo del Enlace de Radio) durante la comunicación, la comunicación puede restaurarse por la ejecución del control de la reconexión.

A fin de que el sistema de LTE tenga éxito en el control de reconexión, la estación base de radio eNB, a la cual se va a realizar la reconexión, necesita mantener de antemano el contexto de la estación móvil UE (contexto del UE). De este modo el sistema de LTE puede realizar un "procedimiento de preparación de la transferencia (Preparación de HO)" sobre múltiples células vecinas.

La razón por la que la estación base de radio origen de la transferencia realiza una "atadura de PCI" en este caso es para asegurar en la medida de lo posible la unicidad de la clave intermedia K_{eNB}* en múltiples células en la ejecución de un "procedimiento de preparación de la transferencia (Preparación de HO)" sobre las células y por lo tanto mejorar la seguridad en el sistema de comunicaciones móviles.

El uso de la misma clave intermedia K_{eNB}* para múltiples células en un procedimiento de preparación de la transferencia accidentalmente permite a las estaciones base de radio eNB que tienen la clave intermedia K_{eNB}* deducir una clave de la estación base K_{eNB} a usar por la estación base de radio objetivo de la transferencia eNB para la comunicación con la estación móvil UE. Esto hace a la red vulnerable en términos de seguridad.

El documento 3GPP TS 33.401 V8.0.0 se refiere a aspectos de seguridad en las redes de comunicaciones móviles. Se describen las características de seguridad y los mecanismos de seguridad para el sistema evolucionado de

paquetes y el núcleo evolucionado de paquete, y los procedimientos de seguridad realizados dentro del sistema evolucionado de paquetes incluyendo el núcleo evolucionado de paquetes y la UTRAN evolucionada.

Sumario de la invención

Problema a resolver por la invención

En el caso de realización de un "procedimiento de preparación de la transferencia" sobre células de la misma frecuencia con el procedimiento antes mencionado, la unicidad de la clave intermedia K_{eNB}* puede asegurarse en las células ya que la PCI es geográficamente única.

Para ser más específico, consideremos el caso mostrado en la Fig. 7 donde se usa la misma frecuencia en una célula objetivo de la transferencia bajo el control de la estación base de radio objetivo de la transferencia (eNB Objetivo) y la preparación de la célula bajo el control de una estación base de radio objetivo para un procedimiento de preparación de la transferencia (eNB Preparada). En este caso, la PCI de la célula objetivo de la transferencia bajo el control de la estación base de radio objetivo de la transferencia es diferente de la PCI de la célula de preparación bajo el control de la estación base de radio objetivo para un procedimiento de preparación de la transferencia. Por esta razón, cuando una estación base de radio origen de la transferencia genera una clave intermedia $K_{eNB}*_1$ usando la PCI de la célula objetivo de la transferencia bajo el control de la estación base de radio objetivo de la transferencia y genera una clave intermedia $K_{eNB}*_2$ usando la PCI de la célula de preparación bajo el control de la estación base de radio objetivo para un procedimiento de preparación de la transferencia, la clave intermedia $K_{eNB}*_1$ resulta ser diferente de la clave intermedia $K_{eNB}*_2$.

En el caso de realizar un "procedimiento de preparación de la transferencia" sobre células de diferentes frecuencias, sin embargo surge un problema ya que la unicidad de la clave intermedia K_{eNB}* es menos probable de asegurar, ya que en algunos casos pueden existir células vecinas entre si que tienen diferentes frecuencias y usan la misma PCI.

La presente invención se realiza por lo tanto a la vista del problema mencionado anteriormente. Un objeto de la presente invención es proporcionar un procedimiento de comunicaciones móviles, una estación base de radio, y una estación móvil que permiten asegurar la unicidad de la clave intermedia K_{eNB}* en la ejecución de un "procedimiento de preparación de transferencia (Preparación de HO)" sobre múltiples células, independientemente de las frecuencias de las células.

Medios para resolver el problema

Un primer aspecto de la presente invención se resume como un procedimiento de comunicaciones móviles de realización de un procedimiento de transferencia para permitir que una estación móvil realice una transferencia desde una célula origen de la transferencia bajo el control de una estación base de radio origen de la transferencia a una célula objetivo de la transferencia bajo el control de una estación base de radio objetivo de la transferencia, incluyendo el procedimiento las etapas de: (A) la generación, en la estación base de radio origen de la transferencia, de una clave intermedia, introduciendo, dentro de una primera función, una clave de la estación base que es necesaria para la generación de una clave para las comunicaciones de la estación móvil en la célula origen de la transferencia, la información de identificación de la célula objetivo de la transferencia, y la información de identificación de una frecuencia para la célula objetivo de la transferencia; y transmitir, desde la estación base de radio origen de la transferencia a la estación base de radio objetivo de la transferencia, la clave intermedia, en el procedimiento de transferencia; y (B) la generación, en la estación base de radio objetivo de la transferencia, de una clave de la estación base, sobre la base de la clave intermedia en el procedimiento de transferencia, siendo necesaria la clave de la estación base para la generación de una clave para la comunicación de la estación móvil en la célula objetivo de la transferencia.

En el primer aspecto, en la etapa (B), la estación base de radio objetivo de la transferencia fija la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

Un segundo aspecto de la presente invención se resume como un procedimiento de comunicaciones móviles para la realización de un procedimiento de transferencia para permitir a una estación móvil realizar una transferencia desde una célula origen de la transferencia bajo el control de una estación base de radio origen de la transferencia a una célula objetivo de la transferencia bajo el control de una estación base de radio objetivo de la transferencia, incluyendo el procedimiento las etapas de: generación, en la estación base de radio origen de la transferencia, de una clave intermedia, introduciendo dentro de una primera función, un parámetro notificado por una estación superior, la información de identificación de la célula objetivo de la transferencia, y la información de identificación de una frecuencia para la célula objetivo de la transferencia; y la transmisión, desde la estación base de radio origen de la transferencia a la estación base de radio objetivo de la transferencia, de la clave intermedia, en el procedimiento de transferencia; y la generación, en la estación base de radio objetivo de la transferencia, de una clave de la estación base, sobre la base de una clave intermedia en el procedimiento de transferencia, siendo necesaria la clave de la estación base para la generación de una clave para la comunicación de la estación móvil en la célula objetivo de la transferencia.

Un tercer aspecto de la presente invención se resume como una estación base de radio capaz de dar servicio como una estación base de radio origen de la transferencia en un procedimiento de comunicaciones móviles en el cual se realiza un procedimiento de transferencia para permitir a una estación móvil realizar una transferencia desde una célula origen de la transferencia bajo el control de la estación base de radio origen de la transferencia a una célula objetivo de la transferencia bajo el control de una estación base de radio objetivo de la transferencia, en donde la estación base de radio se configura para generar una clave intermedia, introduciendo, dentro de una primera función, una clave de la estación base que es necesaria para la generación de una clave para la comunicación de la estación móvil en la célula origen de la transferencia, la información de identificación de la célula objetivo de la transferencia y la información de identificación de una frecuencia para la célula objetivo de la transferencia; y para transmitir, a la estación base de radio objetivo de la transferencia, la clave intermedia, en el procedimiento de transferencia.

Un cuarto aspecto de la presente invención se resume como una estación base de radio capaz de dar servicio como una estación base de radio origen de la transferencia en un procedimiento de comunicaciones móviles en el cual, se realiza un procedimiento de transferencia para permitir a una estación móvil realizar una transferencia desde una célula origen de la transferencia bajo el control de la estación base de radio origen de la transferencia a la célula objetivo de la transferencia bajo el control de una estación base de radio objetivo de la transferencia, en el que la estación base de radio se configura para generar una clave intermedia, introduciendo, dentro de una primera función, un parámetro notificado por una estación superior, la información de identificación de la célula objetivo de la transferencia, y la información de identificación de una frecuencia para la célula objetivo de la transferencia y para transmitir, a la estación base de radio objetivo de la transferencia, la clave intermedia, en el procedimiento de transferencia.

Un quinto aspecto de la presente invención se resume como una estación móvil configurada para realizar un procedimiento de transferencia para realizar una transferencia desde una célula origen de la transferencia bajo control de una estación base de radio origen de la transferencia a una célula objetivo de la transferencia bajo control de una estación base de radio objetivo de la transferencia, en donde la estación móvil está configurada para generar una clave intermedia, introduciendo, dentro de una primera función, una clave de la estación base que es necesaria para la generación de una clave para la comunicación de la estación móvil en la célula origen de la transferencia, la información de identificación de la célula objetivo de la transferencia, y la información de identificación de una frecuencia para la célula objetivo de la transferencia, en la célula objetivo de la transferencia, y la estación móvil se configura para generar una clave de la estación base, sobre la base de la clave intermedia en el procedimiento de transferencia, siendo necesaria la clave de la estación base para la generación de una clave para la comunicación de la estación móvil en la célula objetivo de la transferencia.

En el quinto aspecto, la estación móvil se configura para fijar la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

Un sexto aspecto de la presente invención se resume como un procedimiento de comunicaciones móviles de realización de un procedimiento de transferencia para permitir a una estación móvil realizar una transferencia desde una célula origen de la transferencia a una célula objetivo de la transferencia ambas bajo el control de una estación base de radio, comprendiendo el procedimiento las etapas de (A) generación, en la estación base de radio, de una clave intermedia, introduciendo, dentro de una primera función, un parámetro notificado por una estación superior, la información de identificación de la célula objetivo de la transferencia, y la información de identificación de una frecuencia para la célula objetivo de la transferencia, en el procedimiento de transferencia; y (B) generación, en la estación base de radio, de una clave de la estación base sobre la base de la clave intermedia en el procedimiento de transferencia, siendo necesaria la clave de la estación base para la generación de una clave para la comunicación de la estación móvil en la célula objetivo de la transferencia.

En el sexto aspecto, la estación base de radio establece la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

Efectos de la invención

Como se ha descrito anteriormente, la presente invención puede proporcionar un procedimiento de comunicaciones móviles, una estación base de radio, y una estación móvil que permite asegurar la unicidad de una clave intermedia K_{eNB}* en la ejecución de un "procedimiento de preparación de la transferencia (Preparación de HO)" sobre múltiples células, independientemente de las frecuencias de las células.

Breve descripción de los dibujos

[Fig. 1] la Fig.1 es un visión global de la configuración de un sistema de comunicaciones móviles de acuerdo con una primera realización de la presente invención.

[Fig. 2] la Fig.2 es un diagrama de bloques funcional de una estación móvil de acuerdo con la primera realización de la presente invención.

[Fig. 3] la Fig. 3 es un diagrama de bloques funcional de las estaciones base de radio (una estación base de radio de origen de la transferencia y una estación base de radio objetivo de la transferencia) de acuerdo con

la primera realización de la presente invención.
[Fig. 4] la Fig. 4 es un diagrama para la explicación de cómo se actualiza una clave K_{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 que ilustra los modelos de capas para las claves en un sistema de comunicaciones móviles definidos en el 3GPP.
[Fig. 6] la Fig. 6 es un diagrama que ilustra cómo se actualiza una clave K_{eNB} en el sistema de comunicaciones móviles definido en el 3GPP.
[Fig. 7] la Fig. 7 es un diagrama para la explicación de un problema en un sistema de comunicaciones móviles convencional.

Mejor modo de realización de la invención

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

Se describe un sistema de comunicaciones móviles de acuerdo con una primera realización de la presente invención con referencia a las Fig. 1 a 4.

Como se muestra en la Fig. 1, el sistema de comunicaciones móviles de acuerdo con esta realización es un sistema de comunicaciones móviles del sistema de LTE, e incluye un aparato de la puerta de acceso en servicio S-GW (Puerta de acceso en Servicio), una MME (Entidad de Gestión Móvil) de la estación superior, y múltiples estaciones base de radio eNB Nº 1 y Nº 2.

El aparato de la puerta de enlace en servicio S-GW es una entidad que realiza el encaminamiento en el plano U (encaminamiento de los paquetes de usuario) y la MME es una entidad de red al cargo del control en el plano C (tal como el control de autenticación, el control de registro de localización, y el control de transmisión/recepción).

Obsérvese que, como se muestra en la Fig. Nº 1, el sistema de comunicaciones móviles de acuerdo con esta realización describe un ejemplo de un caso donde se realiza un procedimiento de transferencia para permitir a una estación móvil UE realizar una transferencia desde una célula (célula origen de la transferencia) Nº 1 bajo el control de la estación base de radio eNB Nº 1 que es una estación base de radio origen de la transferencia (eNB de origen) a una célula (célula objetivo de la transferencia) Nº 2 bajo el control de la estación base de radio eNB Nº 2 que es una estación base de radio objetivo de la transferencia.

En este caso, la célula origen de la transferencia Nº 1 y la célula objetivo de la transferencia Nº 2 pueden tener la misma frecuencia o frecuencias diferentes.

Debería observarse que, cuando la célula origen de la transferencia Nº 1 y la célula objetivo de la transferencia Nº 2 tienen la misma frecuencia, la célula origen de la transferencia Nº 1 y la célula objetivo de la transferencia Nº 2 tienen PCI diferentes; cuando la célula origen de la transferencia Nº 1 y la célula objetivo de la transferencia Nº 2 tienen frecuencias diferentes, la célula origen de la transferencia Nº 1 y la célula objetivo de la transferencia Nº 2 pueden tener la misma PCI o diferentes PCI.

Esto se debe a la siguiente razón. Una PCI es un identificador sobre el cual depende la aleatorización de un canal de radio y similares. Por consiguiente, si las células que usan la misma frecuencia y la misma PCI son vecinas entre si, se produce interferencia y de este modo se causa un problema en la comunicación normal.

De este modo, a fin de que el sistema de comunicaciones móviles funcione normalmente como un sistema celular, una PCI necesita ser geográficamente única en células de la misma frecuencia. No es problemático, para las células que usan la misma PCI que sean geográficamente vecinos entre sí siempre que las células tengan frecuencias diferentes.

Como se muestra en la Fig. 2, una estación móvil UE de acuerdo con esta realización incluye una unidad de adquisición de parámetros y una unidad de actualización de claves 12.

La unidad de adquisición de parámetros 11 está configurada para adquirir parámetros necesarios para la actualización de claves desde la estación base de radio origen de la transferencia y la estación base de radio objetivo de la transferencia, en el procedimiento de transferencia para la estación móvil UE.

Por ejemplo, la unidad de adquisición de parámetros 11 está configurada para adquirir, como los parámetros antes mencionados, una "NCC" una "PCI" que es la información de identificación de la célula objetivo de la transferencia, un "ARFCN" que es la información de identificación de una frecuencia para la célula objetivo de la transferencia, un "C-RNTI" que es un identificador de la estación móvil temporalmente asignado a la estación móvil UE en la célula objetivo de la transferencia, y similares.

Obsérvese, en el sistema de LTE, el ARFCN (Número Absoluto del Código de la Frecuencia de Radio) se llama un "EARFCN (E-UTRA ARFCN)".

La unidad de actualización de claves 12 se configura para actualizar una clave de la estación base K_{eNB} que es necesaria para la generación de claves necesarias para la generación de una clave para la comunicación de la

estación móvil UE en la célula origen de la transferencia Nº 1 (tal como una clave $K_{RRC, ciph}$, una clave $K_{RRC, IP}$, y una clave $K_{UP, ciph}$), a una clave de la estación base K_{eNB} que es necesaria para la generación de las claves necesarias para la generación de una clave para la comunicación de la estación móvil UE en la célula objetivo de la transferencia Nº 2, en el procedimiento de transferencia para la estación móvil UE.

Específicamente, ante todo, la unidad de actualización de claves 12 se configura para generar una clave intermedia K_{eNB}* en un caso en el que el parámetro recibido de NCC es el mismo que la NCC mantenida en la estación móvil UE, en el procedimiento de transferencia para la estación móvil UE. La unidad de actualización de claves 12 se configura para generar la clave intermedia K_{eNB}*, introduciendo, dentro de una primera función KDF (*), una clave de la estación base $K_{eNE\ [m]\ [n]}$ que es necesaria para generar una clave para la comunicación de la estación móvil UE en la célula origen de la transferencia Nº 1, la PCI de la célula objetivo de la transferencia Nº 2, y el ARFCN de una frecuencia para la célula objetivo de la transferencia Nº 2.

En segundo lugar, la unidad de actualización de claves 12 se configura para generar una clave de la estación base $K_{eNB\ [m]\ [n + 1]}$, que es necesaria para la generación de claves para la comunicación de la estación móvil UE en la célula objetivo de la transferencia Nº 2, introduciendo el identificador de la estación móvil C-RNTI y la clave intermedia K_{eNB}* dentro de una segunda función KDF (*), el identificador de la estación móvil C-RNTI temporalmente asignado a la estación móvil UE en la célula objetivo de la transferencia Nº 2.

Por ejemplo, la unidad de actualización de claves 12 está configurada para actualizar la clave de la estación base K_{eNB} por la siguiente fórmula:

$$K_{eNB}* = KDF\ (K_{eNE\ [m]\ [n]},\ PCI,\ ARFCN)$$

$$K_{eNB\ [m]\ [n + 1]} = KDF\ (K_{eNB}*,\ C\text{-}RNTI).$$

Por otra parte, si el parámetro de NCC recibido es mayor que la NCC mantenida en la estación móvil UE, la estación móvil UE se configura para repetir el cálculo con la siguiente fórmula, y para actualizar un parámetro NH, hasta que la NCC mantenida en si misma se hace igual al parámetro recibido de NCC. La estación móvil UE se configura para incrementar por uno la NCC mantenida en si misma en cada cálculo con la siguiente fórmula:

$$NH* = KDF\ (K_{ASME},\ NH\ [m])$$

$$NH\ [m + 1] = NH*$$

La unidad de actualización de claves 12 está configurada para generar después de esto una clave intermedia K_{eNs}* introduciendo, dentro de la primera función KDF (*) el parámetro NH [m + 1] notificado por la MME de la estación superior, la información de identificación PCI de la célula objetivo de la transferencia Nº 2, y la información de identificación ARFCN de la frecuencia para la célula objetivo de la transferencia Nº 2.

La unidad de actualización de claves 12 está configurada para fijar a continuación la clave intermedia K_{eNB}* como una clave de la estación base $K_{eNB\ [m + 1]\ [0]}$ que es necesaria para la generación de claves para la comunicación de la estación móvil UE en la célula objetivo de la transferencia Nº 2.

Como se muestra en la Fig. 3, la estación base de radio eNB Nº 1 que sirve como la estación base de radio origen de la transferencia (eNB de origen) incluye una unidad del procesador de transferencias 21, una interfaz de MME (puede llamarse también una interfaz S1) 22, una interfaz de eNB (también puede llamarse una interfaz X2) 23, y una interfaz de UE 24.

La unidad de procesador de transferencia 21 está configurada para adquirir un parámetro NH* desde la MME de la estación superior a través de la interfaz de MME 22, en el procedimiento de transferencia para la estación móvil UE.

Además, la unidad de procesador de transferencia 21 está configurada para adquirir un parámetro inicial NH(0) desde la MME de la estación superior a través de la interfaz de MME 22, en el establecimiento de conexión para la estación móvil UE.

Además, la unidad de procesador de transferencia 21 está configurada para notificar, a la estación base de radio eNB Nº 2 en servicio como la estación base de radio objetivo de la transferencia (eNB Objetivo), una clave intermedia K_{eNB}*, una NCC, y un identificador de aumento del índice, a través de la interfaz de eNB 23.

Además, la unidad de procesador de transferencia 21 está configurada para notificar, a la estación móvil UE, la NCC, y la PCI y el ARFCN de la célula objetivo de la transferencia Nº 2 a través de la interfaz de UE 24.

Mientras tanto, la estación base de radio eNB Nº 2 que da servicio como la estación base de radio objetivo de la transferencia (eNB Objetivo) incluye una unidad del procesador de transferencia 31, una interfaz de eNB 32, una unidad del generador de claves 33 y una interfaz de UE 34.

La unidad del generador de claves 33 está configurada para generar una clave de la estación base K_{eNB} que es necesaria para la generación de claves para la comunicación de la estación móvil UE en la célula objetivo de la

transferencia Nº 2, sobre la base de la clave intermedia K_{eNB}*, la NCC, el identificador de aumento del índice y el C-RNTI. La clave intermedia K_{eNB}*, la NCC, y el identificador de aumento de índice se reciben a través de la interfaz de eNB 32, y se recibe el C-RNTI desde la unidad del procesador de transferencia 31 y se asignan a la estación móvil UE en la célula de transferencia Nº 2.

En adelante en este documento, con referencia a la Fig. 4, se da una descripción de cómo se actualiza una clave de la estación base K_{eNB}* cuando la estación móvil UE realiza una transferencia desde la célula Nº 1 bajo el control de la estación base de radio eNB Nº 1 a la célula Nº 2 bajo el control de la estación base de radio eNB Nº 2.

En la Etapa (1), durante el establecimiento de la conexión para la estación móvil UE, la MME de la estación superior genera un parámetro inicial NH(0) sobre la base de una clave K_{ASME} y un "NAS SN (un número de secuencia en NAS".

En la Etapa (2), la MME de la estación superior notifica a la estación base de radio eNB Nº 1 del parámetro inicial NH(0) como una clave intermedia K_{eNB}*. En la Etapa (3) la estación base de radio (eNB Nº 1 almacena la clave intermedia recibida K_{eNB}* sin cambiarla como una clave de la estación base $K_{ENB\ [0]\ [0]}$.

En la Etapa (11), la MME de la estación superior también genera un parámetro NH* sobre la base de la clave K_{ASME} y el parámetro inicial NH [0], y notifica a la estación base de radio eNB Nº 1 del parámetro NH*.

En la Etapa (12), la estación base de radio eNB Nº 1 almacena el parámetro recibido NH* sin cambiarlo como un parámetro NH [1].

Consideremos un caso en el que la estación móvil UE realiza después de esto una transferencia desde la célula Nº 1 bajo el control de la estación base de radio eNB Nº 1 a la célula Nº 2 bajo el control de la estación base de radio eNB Nº 2. En este caso la estación base de radio eNB Nº 1 genera una clave intermedia K_{eNB}* en la Etapa (4) introduciendo la clave de la estación actual $K_{eNB\ [0]\ [0]}$, la PCI de la célula Nº 2, y la información de identificación ARFCN de una frecuencia para la célula Nº 2 dentro de una primera función KDF(*), más concretamente, sobre la base de KDF ($K_{eNB\ [0]\ [0]}$, PCI, ARFCN), y notifica a la estación base de radio eNB Nº 2 de la clave intermedia K_{eNB}*.

En otras palabras, se realiza la operación para la actualización de la clave usando la información de identificación de frecuencia ARFCN, es decir una "atadura de ARFCN".

En un caso en el que la transferencia para la estación móvil UE descrita anteriormente es una transferencia entre células bajo el control de la misma estación base de radio eNB (Transferencia Intra eNB), por ejemplo, la estación base de radio eNB Nº 1 genera una clave intermedia K_{eNB}* sobre la base de KDF (($K_{eNB\ [0]\ [0]}$, PCI, ARFCN) como se ha descrito anteriormente. En este caso, la estación base de radio eNB Nº 1 y la estación base de radio objetivo de la transferencia eNB Nº 2 son la misma.

Como alternativa, la estación base de radio eNB Nº 1 puede generar una clave intermedia K_{eNB}* en la Etapa (13) introduciendo el parámetro actual NH [1], la PCI de la célula Nº 2, y la información de identificación ARFCN de la frecuencia para la célula Nº 2 dentro de la primera función KDF (*), más concretamente, sobre la base de KDF (NH [1], PCI, ARFCN), y notificar a la estación base de radio eNB Nº 2 de la clave intermedia K_{eNB}*, cuando la estación móvil UE realiza una transferencia desde la célula Nº 1 bajo el control de la estación base de radio eNB Nº 1 a la célula Nº 2 bajo el control de la estación base de radio eNB Nº 2 diferente de la estación base de radio eNB Nº 1.

En un caso en el que la transferencia para la estación móvil UE descrita anteriormente es una transferencia entre células bajo el control de diferentes estaciones base de radio eNB (Transferencia inter eNB), por ejemplo, la estación base de radio eNB Nº 1 genera una clave intermedia K_{eNB}* sobre la base de KDF (NH [1], PCI, ARFCN), como se ha descrito anteriormente.

Específicamente, si la estación base de radio eNB Nº 2 reconoce a partir del "identificador de aumento de índice", que se notifica por la estación base de radio eNB Nº 1, que la clave intermedia K_{eNB}* se genera en base a la KDF ($K_{eNB\ [0]\ [0]}$, PCI, ARFCN), la estación base de radio eNB Nº 2 genera una clave de la estación base $K_{eNB\ [0]\ [1]}$ en la Etapa (5) introduciendo la clave intermedia K_{eNB}* y el identificador de la estación móvil C-RNTI, que se asigna temporalmente a la estación móvil UE en la célula Nº 2, dentro de la segunda función KDF (*), más concretamente, sobre la base de KDF (K_{eNB}*, C-RNTI).

Por el contrario, si la estación base de radio eNB Nº 2 reconoce a partir del "identificador de aumento de índice" que se notifica por la estación base de radio eNB Nº 1, que la clave intermedia K_{eNB}* se genera sobre la base del parámetro actual NH [1], la estación base de radio eNB Nº 2 genera una clave de la estación base $K_{eNB\ [1]\ [0]}$ en la Etapa (14) introduciendo la clave intermedia K_{eNB}* y el identificador de la estación móvil C-RTNI, que se asigna temporalmente a la estación móvil UE en la célula Nº 2, dentro de la segunda función KDF (*), más concretamente, sobre la base de KDF (K_{eNB}*, C-RNTI).

Obsérvese que, la primera función y la segunda función pueden ser la misma función o funciones diferentes siempre que sean conocidas tanto para la estación base de radio eNB como la estación móvil UE.

Además, la "atadura de PCI" y la "atadura de ARFCN" en la Etapa (4) y la Etapa (13) pueden realizarse por la estación base de radio eNB Nº 2 que es la estación base de radio objetivo de la transferencia en lugar de realizarse por la estación base de radio eNB Nº 1que es la estación base de radio origen de la transferencia.

Además, la "atadura del C-RNTI" en la Etapa (5) y la Etapa (14) pueden omitirse.

(Efecto ventajoso del sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención)

El sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención se configura en que la estación base de radio origen de la transferencia genera una clave intermedia K_{eNB}* usando no solo la PCI de la célula objetivo de la transferencia (o la célula objetivo para un procedimiento de preparación de la transferencia) sino también la información de identificación ARFCN de una frecuencia para la célula objetivo de la transferencia (o la célula objetivo para el procedimiento de preparación de la transferencia). Esto permite al sistema de comunicaciones móviles de acuerdo con la primera realización de la presente invención asegurar la unicidad de la clave intermedia K_{eNB}* en la ejecución del "procedimiento de preparación de la transferencia" sobre múltiples células.

Obsérvese que la operación de la estación móvil UE descrita anteriormente y la estación base de radio eNB pueden implementarse por medio de hardware, un módulo software ejecutado por un procesador, o una combinación de ambos.

El módulo software puede proporcionarse en cualquier tipo de medio de almacenamiento tal como una RAM (Memoria de Acceso Aleatorio), una memoria flash, una ROM (Memoria de Solo Lectura), una EPROM (ROM Programable y Borrable), una EEPROM (ROM Borrable y Programable Eléctricamente), un registro, un disco duro, un disco desmontable, o un CD-ROM.

El medio de almacenamiento se conecta al procesador de modo que el procesador puede leer y escribir información desde y al medio de almacenamiento. También, el medio de almacenamiento puede estar integrado dentro del procesador. También, el medio de almacenamiento y el procesador puede proporcionarse en un ASIC. El ASIC puede proporcionarse en la estación móvil UE y la estación base de radio eNB. También el medio de almacenamiento y el procesador pueden proporcionarse en la estación móvil UE y la estación base de radio eNB como un componente discreto.

Anteriormente en este documento, se ha descrito la presente invención en detalle usando la realización anterior; sin embargo, es evidente para los especialistas en la técnica que la presente invención no se limita a la realización descrita en este documento. Las modificaciones y variaciones de la presente invención pueden realizarse sin aparatarse del alcance de la presente invención definida por la descripción del alcance de las reivindicaciones. De este modo, lo que se describe en este documento es para propósitos ilustrativos y no tiene ninguna intención que sea limitar la presente invención.

Explicación de los números de referencia

UE	ESTACIÓN MÓVIL
11	UNIDAD DE ADQUISICIÓN DE PARÁMETROS
12	UNIDAD DE ACTUALIZACIÓN DE CLAVES
eNB de Origen	ESTACIÓN BASE DE RADIO ORIGEN DE LA TRANSFERENCIA
21, 31	UNIDAD PROCESADORA DE LA TRANSFERENCIA
22	INTERFAZ DE MME
23, 32	INTERFAZ DE eNB
24, 34	INTERFAZ DE UE
eNB Objetivo	ESTACIÓN BASE DE RADIO OBJETIVO DE LA TRANSFERENCIA
33	UNIDAD GENERADORA DE CLAVES

REIVINDICACIONES

1. Un procedimiento de comunicaciones móviles de realización de un procedimiento de transferencia para permitir a una estación móvil (UE) realizar una transferencia desde una célula origen de la transferencia (CÉLULA Nº 1) bajo el control de una estación base de radio origen de la transferencia (eNB Nº 1) a una célula objetivo de la transferencia (CÉLULA Nº 2) bajo el control de una estación base de radio objetivo de la transferencia (eNB Nº 2), comprendiendo el procedimiento las etapas de:

(A) generar, en la estación base de radio origen de la transferencia (eNB Nº 1), una clave intermedia, introduciendo, dentro de una primera función, una clave de la estación base que es necesaria para la generación de una clave para las comunicaciones de la estación móvil (UE) en la célula origen de la transferencia (CÉLULA Nº 1), la información de identificación de la célula objetivo de la transferencia (CÉLULA Nº 2), y la información de identificación de una frecuencia para la célula objetivo de la transferencia (CÉLULA Nº 2); y transmitir, desde la estación base de radio origen de la transferencia (eNB Nº 1) a la estación base de radio objetivo de la transferencia (eNB Nº 2), la clave intermedia, en el procedimiento de transferencia; y
(B) generar, en la estación base de radio objetivo de la transferencia (eNB Nº 2), una clave de la estación base, sobre la base de la clave intermedia en el procedimiento de transferencia, siendo la clave de la estación base necesaria para la generación de una clave para la comunicación de la estación móvil (UE) en la célula objetivo de la transferencia (CÉLULA Nº 2).

2. El procedimiento de comunicaciones móviles de acuerdo con la reivindicación 1, en el que

en la etapa (B), la estación base de radio objetivo de la transferencia (eNB Nº 2) fija la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

3. El procedimiento de comunicaciones móviles de realización de un procedimiento de transferencia para permitir a una estación móvil (UE) realizar una transferencia desde una célula origen de la transferencia (CÉLULA Nº 1) bajo el control de una estación base de radio origen de la transferencia (eNB Nº 1) a una célula objetivo de la transferencia bajo el control de una estación base de radio objetivo de la transferencia (eNB Nº 2), comprendiendo el procedimiento las etapas de:

(A) generar, en la estación base de radio origen de la transferencia (eNB Nº 1), una clave intermedia, introduciendo, dentro de una primera función, un parámetro notificado por una estación superior, la información de identificación de la célula objetivo de la transferencia (CÉLULA Nº 2), y la información de identificación de una frecuencia para la célula objetivo de la transferencia (CÉLULA Nº 2); y transmitir, desde la estación base de radio origen de la transferencia a la estación base de radio objetivo de la transferencia (eNB Nº 2), la clave intermedia, en el procedimiento de transferencia; y
(B) generar, en la estación base de radio objetivo de la transferencia (eNB Nº 2), una clave de la estación base, sobre la base de la clave intermedia en el procedimiento de transferencia, siendo la clave de la estación base necesaria para la generación de una clave para la comunicación de la estación móvil (UE) en la célula objetivo de la transferencia (CÉLULA Nº 2).

4. El procedimiento de comunicaciones móviles de acuerdo con la reivindicación 3, en el que

en la etapa (B), la estación base de radio objetivo de la transferencia (eNB nº 2) fija la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

5. Una estación base de radio capaz de dar servicio como una estación base de radio origen de la transferencia (eNB Nº 1 en un procedimiento de comunicaciones móviles en el cual se realiza un procedimiento de transferencia para permitir a una estación móvil (UE) realizar una transferencia desde una célula origen de la transferencia (CÉLULA Nº 1) bajo el control de la estación base de radio origen de la transferencia a la célula objetivo de la transferencia (CÉLULA Nª 2) bajo el control de una estación base de radio objetivo de la transferencia (eNB Nº 2), en el que
la estación base de radio (eNB Nº 1) está configurada para generar una clave intermedia, introduciendo, dentro de una primera función, una clave de la estación base que es necesaria para generar una clave para la comunicación de la estación móvil en la célula origen de la transferencia (CÉLULA Nº 1), la información de identificación de la célula objetivo de la transferencia (CÉLULA N º 2), y la información de identificación de una frecuencia para la célula objetivo de la transferencia (CÉLULA Nº 2); y para transmitir, a la estación base de radio objetivo de la transferencia (eNB Nº 2), la clave intermedia, en el procedimiento de transferencia.

6. Una estación base de radio capaz de dar servicio a una estación base de radio origen de la transferencia (eNB Nº 1) en un procedimiento de comunicaciones móviles en el que se realiza un procedimiento de transferencia para permitir a una estación móvil (UE) realizar una transferencia desde una célula origen de la transferencia (CÉLULA Nº 1) bajo el control de la estación base de radio origen de la transferencia a una célula objetivo de la transferencia (CÉLULA Nº 2) bajo el control de la estación base de radio objetivo de la transferencia (eNB Nº 2), en el que
la estación base de radio (eNB Nº 1) está configurada para generar una clave intermedia, introduciendo, dentro de una primera función, un parámetro notificado por una estación superior, la información de identificación de la célula objetivo de la transferencia (CÉLULA Nº 2), y la información de identificación de una frecuencia para la célula objetivo de la transferencia (CÉLULA Nº 2), y para transmitir, a la estación base de radio objetivo de la transferencia (eNB Nº

2), la clave intermedia, en el procedimiento de transferencia.

7. Una estación móvil configurada para realizar un procedimiento de transferencia para la realización de una transferencia desde una célula origen de la transferencia (CÉLULA Nº 1) bajo el control de una estación base de radio origen de la transferencia (eNB Nº 1) a una célula objetivo de la transferencia (CÉLULA Nº 2) bajo el control de una estación base de radio objetivo de la transferencia (eNB Nº 2), en el que
la estación móvil (UE) está configurada para generar una clave intermedia, introduciendo, dentro de una primera función, una clave de la estación base, que es necesaria para la generación de una clave para la comunicación de la estación móvil (UE) en la célula origen de la transferencia, la información de identificación de la célula objetivo de la transferencia (CÉLULA Nº 2), y la información de identificación de una frecuencia para la célula objetivo de la transferencia (CÉLULA Nº 2), en la célula objetivo de la transferencia (CÉLULA Nº 2), y
la estación móvil (UE) está configurada para generar una clave de la estación base, sobre la base de la clave intermedia en el procedimiento de transferencia, siendo necesaria la clave de la estación base para la generación de una clave para la comunicación de la estación móvil (UE) en la célula objetivo de la transferencia (CÉLULA Nº 2).

8. La estación móvil de acuerdo con la reivindicación 7, en el que
la estación móvil (UE) está configurada para fijar la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

9. Un procedimiento de comunicaciones móviles de realización de un procedimiento de transferencia para permitir a una estación móvil (UE) realizar una transferencia desde una célula origen de la transferencia (CÉLULA Nº 1) a una célula objetivo de la transferencia (CÉLULA Nº 2) ambas bajo el control de una estación base de radio, comprendiendo el procedimiento las etapas de:

(A) generar, en la estación base de radio, una clave intermedia, introduciendo, dentro de una primera función, un parámetro notificado por una estación superior, la información de identificación de la célula objetivo de la transferencia (CÉLULA Nº 2), y la información de identificación de una frecuencia para la célula objetivo de la transferencia (CÉLULA Nº 2), en el procedimiento de transferencia; y
(B) generar, en la estación base de radio, una clave de la estación base, sobre la base de la clave intermedia en el procedimiento de transferencia, siendo la clave de la estación base necesaria para la generación de una clave para la comunicación de la estación móvil (UE) en la célula objetivo de la transferencia (CÉLULA Nº 2).

10. El procedimiento de comunicaciones móviles de acuerdo con la reivindicación 9, en el que
en la etapa (B), la estación base de radio fija la clave intermedia como la clave de la estación base en el procedimiento de transferencia.

FIG. 1

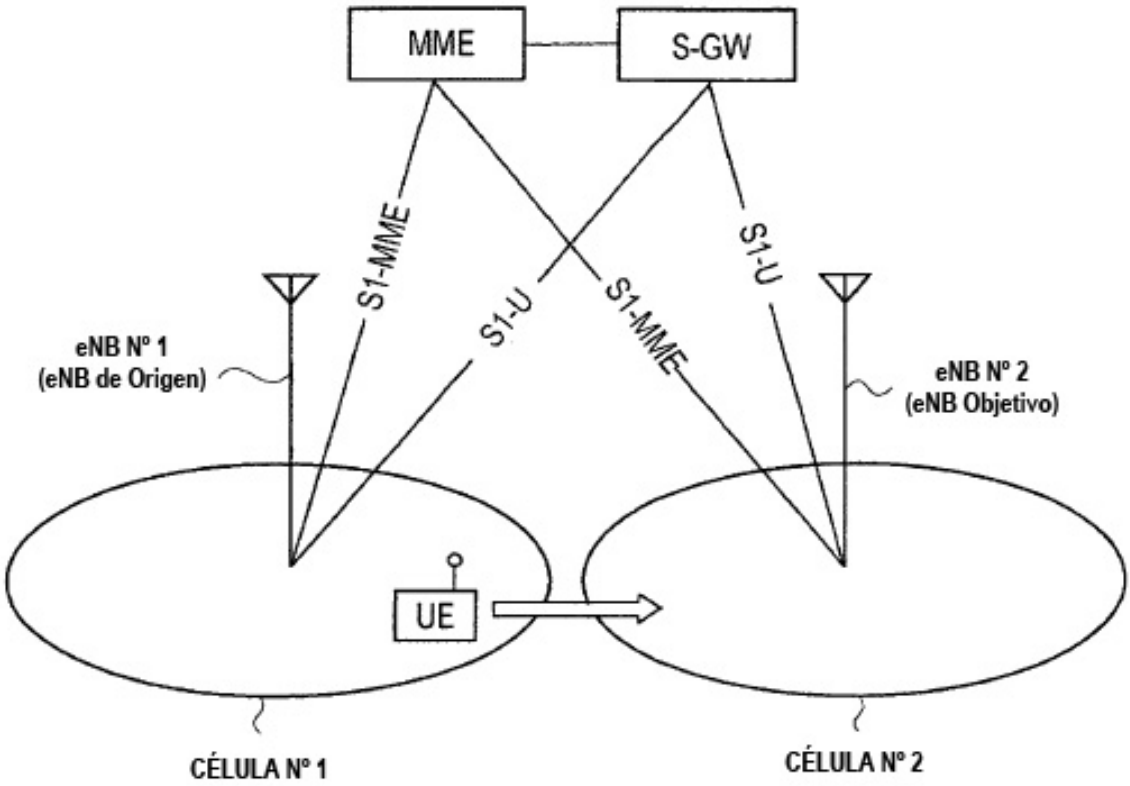

MME
S-GW
S1-MME
S1-U
S1-U
S1-MME
eNB Nº 1
(eNB de Origen)
eNB Nº 2
(eNB Objetivo)
UE
CÉLULA Nº 1
CÉLULA Nº 2

FIG. 2

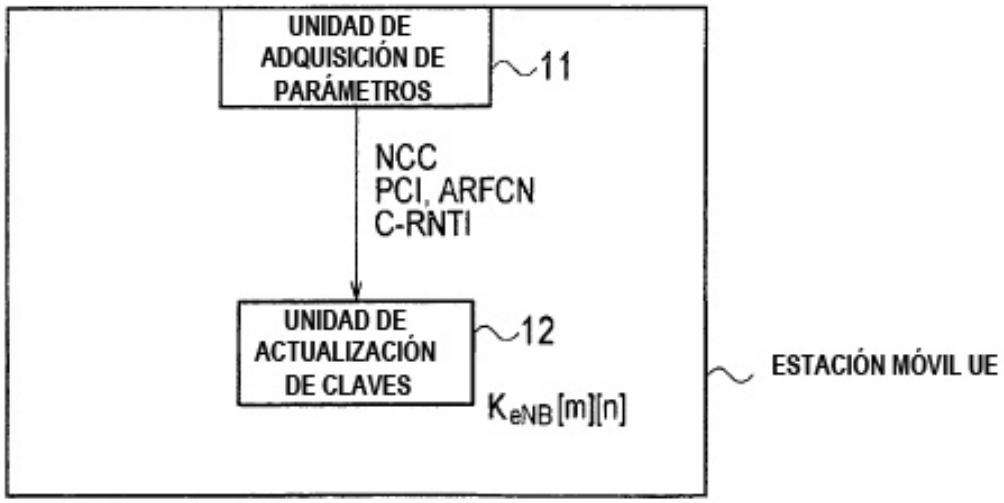

UNIDAD DE ADQUISICIÓN DE PARÁMETROS
11
NCC
PCI, ARFCN
C-RNTI
UNIDAD DE ACTUALIZACIÓN DE CLAVES
12
$K_{eNB}[m][n]$
ESTACIÓN MÓVIL UE

FIG. 3

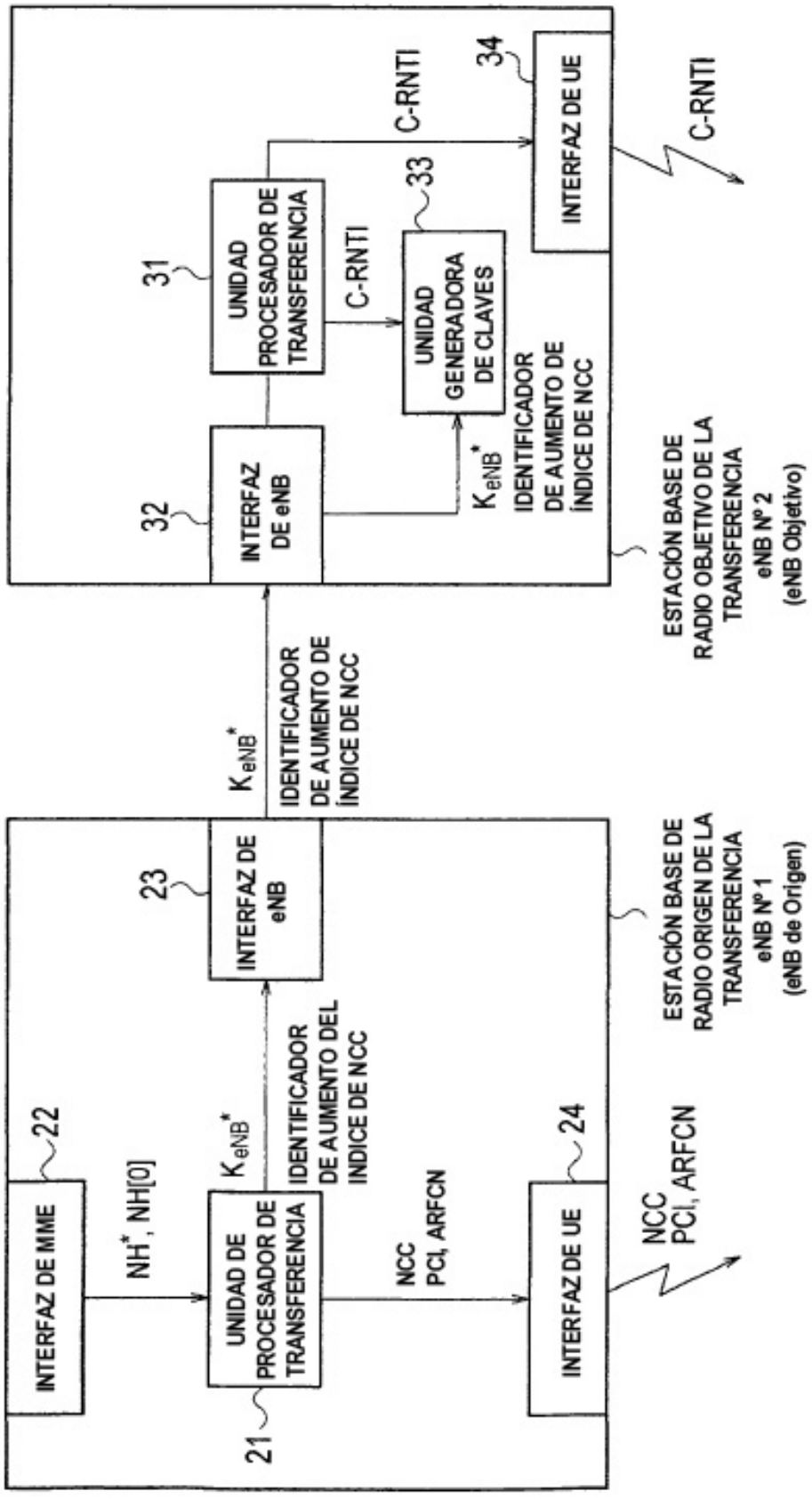

ESTACIÓN BASE DE RADIO ORIGEN DE LA TRANSFERENCIA eNB Nº 1 (eNB de Origen)
INTERFAZ DE MME
22
NH*, NH[0]
UNIDAD DE PROCESADOR DE TRANSFERENCIA
21
K_{eNB}*
IDENTIFICADOR DE AUMENTO DEL INDICE DE NCC
NCC
PCI, ARFCN
INTERFAZ DE eNB
23
INTERFAZ DE UE
24
NCC
PCI, ARFCN
K_{eNB}*
IDENTIFICADOR DE AUMENTO DE ÍNDICE DE NCC
ESTACIÓN BASE DE RADIO OBJETIVO DE LA TRANSFERENCIA eNB Nº 2 (eNB Objetivo)
INTERFAZ DE eNB
32
UNIDAD PROCESADOR DE TRANSFERENCIA
31
C-RNTI
UNIDAD GENERADORA DE CLAVES
33
C-RNTI
K_{eNB}*
IDENTIFICADOR DE AUMENTO DE ÍNDICE DE NCC
INTERFAZ DE UE
34
C-RNTI

FIG. 4

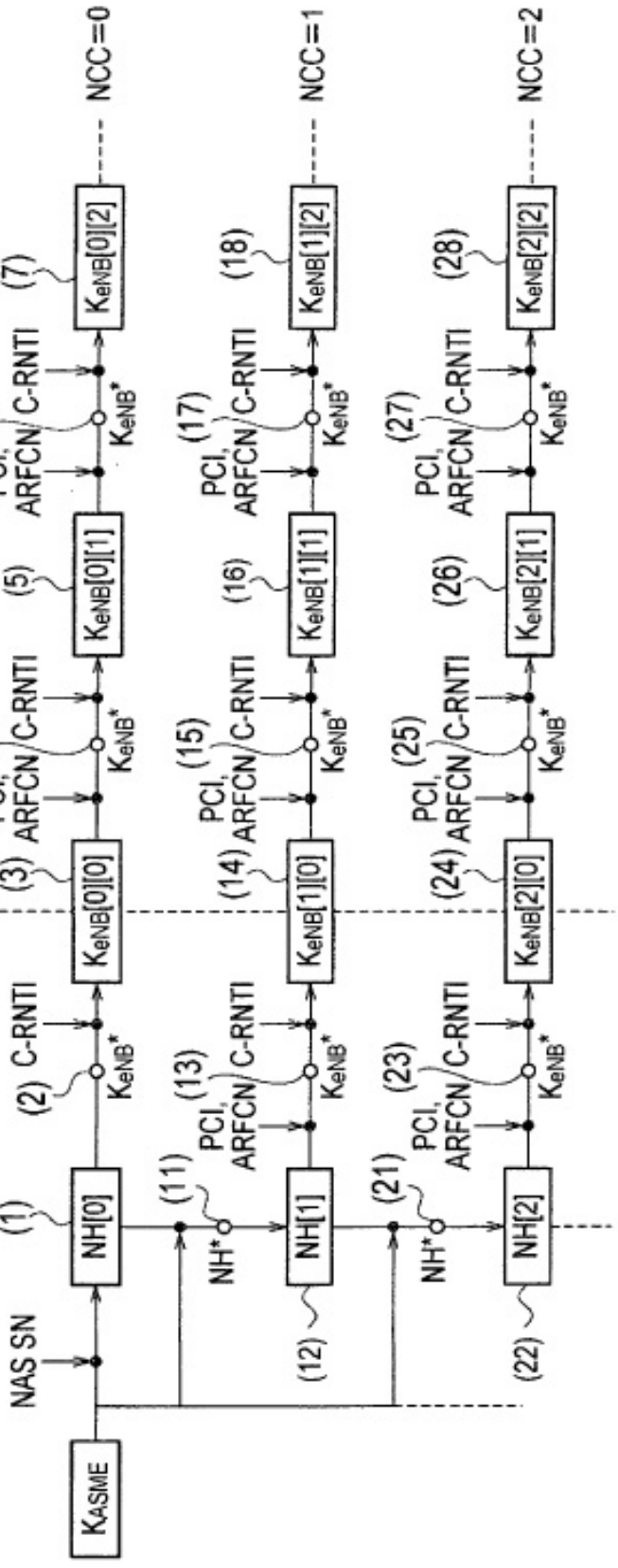

KASME
NAS SN
NH[0]
NH[1]
NH[2]
NH*
PCI, ARFCN
C-RNTI
KeNB*
KeNB[0][0]
KeNB[0][1]
KeNB[0][2]
KeNB[1][0]
KeNB[1][1]
KeNB[1][2]
KeNB[2][0]
KeNB[2][1]
KeNB[2][2]
NCC=0
NCC=1
NCC=2
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(11)
(12)
(13)
(14)
(15)
(16)
(17)
(18)
(21)
(22)
(23)
(24)
(25)
(26)
(27)
(28)

FIG. 5A

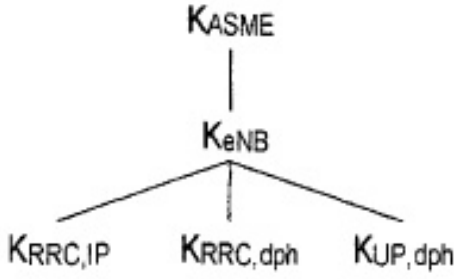

KASME
KeNB
KRRC,IP
KRRC,dph
KUP,dph

FIG. 5B

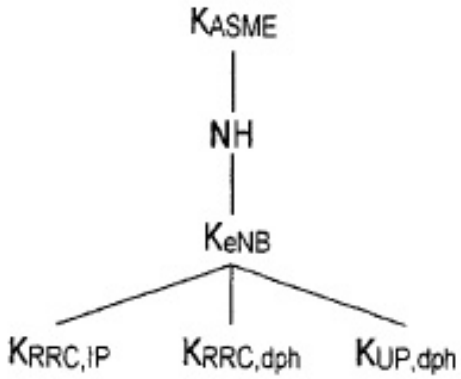

KASME
NH
KeNB
KRRC,IP
KRRC,dph
KUP,dph

FIG. 6

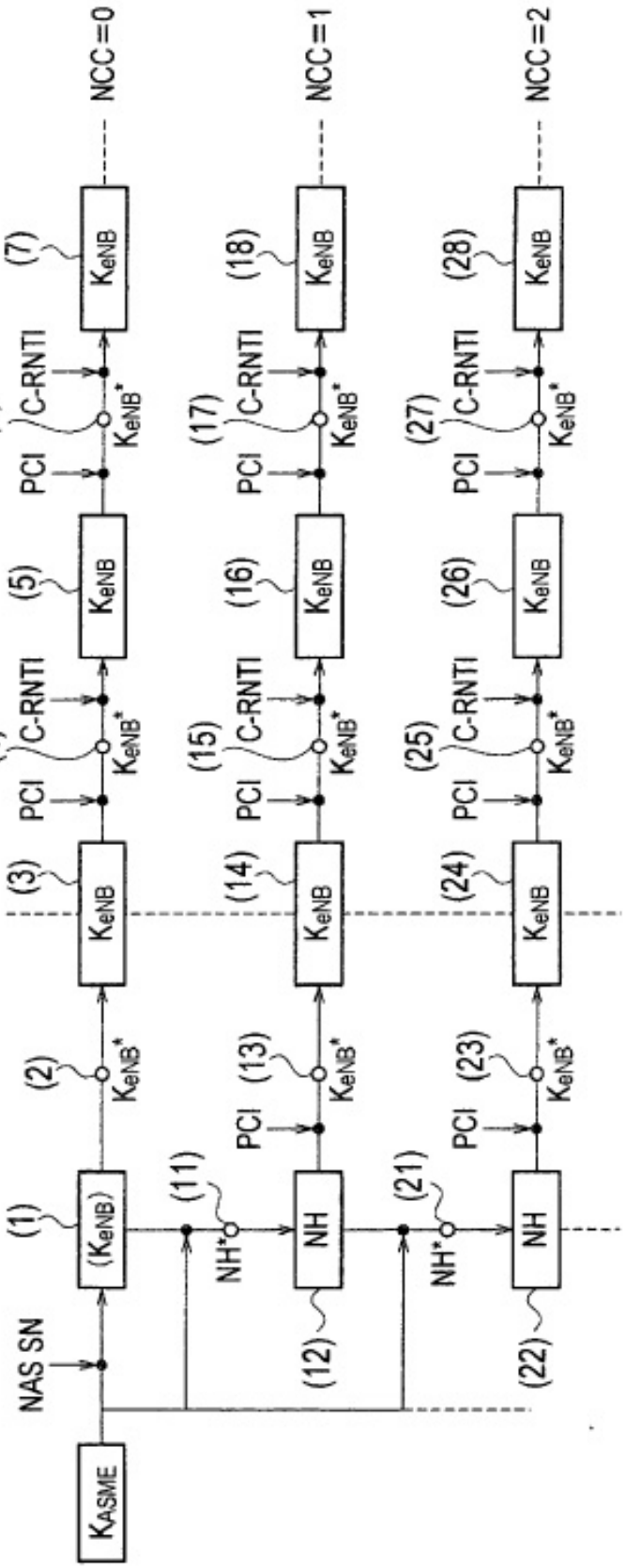
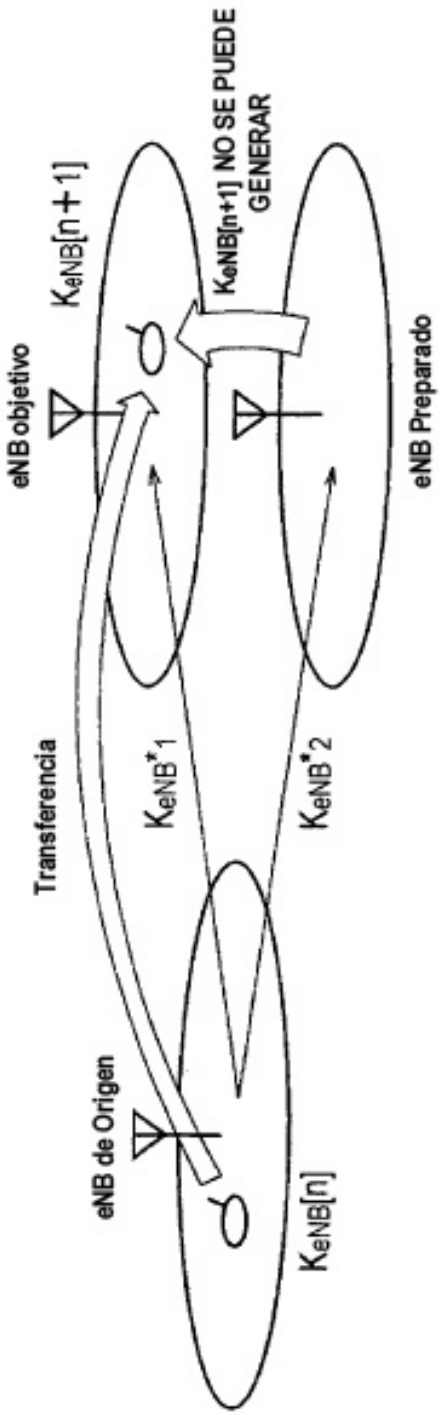

NCC=0
NCC=1
NCC=2
KASME
NAS SN
(1)
(KeNB)
(2)
KeNB*
(3)
KeNB
(4)
C-RNTI
PCI
KeNB*
(5)
KeNB
(6)
C-RNTI
PCI
KeNB*
(7)
KeNB
(11)
NH*
(12)
NH
(13)
PCI
KeNB*
(14)
KeNB
(15)
C-RNTI
PCI
KeNB*
(16)
KeNB
(17)
C-RNTI
PCI
KeNB*
(18)
KeNB
(21)
NH*
(22)
NH
(23)
PCI
KeNB*
(24)
KeNB
(25)
C-RNTI
PCI
KeNB*
(26)
KeNB
(27)
C-RNTI
PCI
KeNB*
(28)
KeNB

FIG. 7


eNB objetivo
KeNB[n+1]
KeNB[n+1] NO SE PUEDE GENERAR
eNB Preparado
Transferencia
KeNB*1
KeNB*2
eNB de Origen
KeNB[n]