(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 586 824**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 76/02 (2009.01)
H04W 88/06 (2009.01)
H04W 88/10 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.12.2012 E 12858204 (6)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2016 EP 2785088**

(54) Título: **Método y dispositivo asociado para generar una clave de estrato de acceso en un sistema de comunicaciones**

(30) Prioridad:

15.12.2011 CN 201110421275

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.10.2016

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD (100.0%)
Huawei Administration Building, Bantian Longgang District, Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

ZHANG, DONGMEI;
CHEN, JING y
CUI, YANG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo asociado para generar una clave de estrato de acceso en un sistema de comunicaciones

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de las radiocomunicaciones y más en particular, a un método y a un dispositivo asociado para generar una clave de estrato de acceso en un sistema de comunicaciones en el campo de las radiocomunicaciones.

ANTECEDENTES DE LA INVENCIÓN

En una arquitectura de LTE-Hi (Long Term Evolution-Hi, Evolución a largo plazo-Hi) propuesta, un equipo de usuario (User Equipment, UE) puede acceder a una red base por intermedio de un nodo NodeB evolucionado (evolved NodeB, eNB), o puede conectarse al nodo eNB por intermedio de un punto de acceso de LTE-Hi (LTE-Hi Access Point, LTE-Hi AP) y luego, acceder a la red base por intermedio del nodo eNB. El equipo de usuario UE puede conectarse también directamente a un dispositivo de pasarela en otra red por intermedio del LTE-Hi AP. En la arquitectura de LTE-Hi, el equipo de usuario UE tiene dos interfaces de aire de radio, es decir, una interfaz Uu entre el equipo de usuario UE y el nodo eNB y una interfaz Uu' entre el equipo UE y el punto de acceso LTE-Hi AP.

La arquitectura de LTE-Hi no solamente puede soportar el escenario operativo en el que el equipo UE realiza el acceso inicialmente desde el punto LTE-Hi AP y luego, algunos servicios se transfieren el nodo eNB, sino que también puede soportar el escenario operativo en el que el equipo UE realiza el acceso inicialmente desde el nodo eNB, y luego, algunos servicios se transfieren al punto de acceso LTE-Hi AP. Por lo tanto, un mecanismo de seguridad de interfaz de aire para la interfaz de aire Uu' necesita ser compatible con los dos escenarios operativos anteriores. El equipo UE puede recibir datos por intermedio de dos enlaces correspondientes a la interfaz de aire Uu' y la interfaz de aire Uu al mismo tiempo para comunicarse con el punto de acceso LTE-Hi AP y el nodo eNB al mismo tiempo. En dicho escenario operativo, dos bifurcaciones tienen sus propias interfaces de aire. La generación, el mantenimiento, la modificación y la supresión de un contexto de seguridad de estrato de acceso (Access Stratum, AS) en las dos interfaces de aire necesitan considerarse para garantizar la seguridad de los datos transmitidos por intermedio de cada interfaz de aire.

Sin embargo, en la técnica anterior, solamente se da a conocer una manera de generación de una clave AS en la interfaz de aire Uu, mientras que no incluye la forma de generación de la clave de AS en la interfaz de aire Uu'. En consecuencia, no puede garantizarse la seguridad de la transmisión de datos por intermedio de la interfaz de aire Uu'.

La solicitud de patente de los US US 2011/235802 da a conocer la generación de claves de autenticación para la comunicación de red de área local, que incluye: participación en la comunicación de un mensaje que contiene un tipo de selección del método de cifrado que indica el dispositivo de cifrado compatible con la red celular y la creación de claves de autenticación compatibles con la red celular en conformidad con dicho tipo de selección de dispositivo de cifrado.

La solicitud de patente EP 2 487 947 A1 da a conocer un método y dispositivo para obtener una clave de seguridad en un sistema de retransmisión. Un nodo en el sistema de retransmisión obtiene una clave inicial, en conformidad con la clave inicial, obteniendo el nodo una clave raíz de una clave de protección de interfaz de aire entre el nodo y otro nodo que es directamente adyacente al nodo y en conformidad con la clave raíz, el nodo obtiene la clave de protección de la interfaz de aire entre el nodo y otro nodo que está directamente adyacente a dicho nodo.

SUMARIO DE LA INVENCIÓN

La presente invención da a conocer un método y un dispositivo asociado para generar una clave de estrato de acceso en un sistema de comunicaciones, lo que resuelve un problema en la técnica anterior en donde no se puede garantizar la seguridad de la transmisión de datos por intermedio de dos interfaces de aire de un equipo de usuario UE al mismo tiempo y permite al equipo UE realizar una transmisión de datos segura por intermedio de las dos interfaces de aire, con lo que se mejora la seguridad del sistema.

La presente invención se define por las reivindicaciones adjuntas.

Sobre la base de las soluciones técnicas anteriores, el segundo dispositivo del lado de la red puede adquirir la clave KeNB* que se adquiere sobre la base de la clave KeNB en la primera interfaz de aire, y el equipo de usuario puede calcular la clave KeNB* en conformidad con la clave KeNB conocida por sí misma. De este modo, el segundo dispositivo del lado de la red y el equipo de usuario pueden tener la misma clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire. El segundo dispositivo del lado de la red y el equipo de usuario pueden generar la misma clave de estrato de acceso en conformidad con la misma clave KeNB*, lo que puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y garantizar la seguridad de los datos transmitidos

entre el segundo dispositivo del lado de la red y el equipo de usuario cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las formas de realización de la presente invención con mayor claridad, a continuación se introduce, de forma concisa, los dibujos adjuntos requeridos para describir las formas de realización. Evidentemente, los dibujos adjuntos en la descripción siguiente muestran simplemente algunas formas de realización de la presente invención y un experto en esta técnica puede derivar todavía otros dibujos a partir de estos dibujos adjuntos sin necesidad de esfuerzos creativos.

La Figura 1 es un diagrama de flujo de un método para generar una clave de estrato de acceso realizada por una estación base en conformidad con una forma de realización de la presente invención;

La Figura 2 es un diagrama de flujo de un método para generar una clave de estrato de acceso realizada por un dispositivo de acceso en conformidad con una forma de realización de la presente invención;

La Figura 3 es un diagrama de flujo de un método para generar una clave de estrato de acceso realizada por un equipo de usuario en conformidad con una forma de realización de la presente invención;

La Figura 4 es un diagrama esquemático de una arquitectura de LTE-Hi a modo de ejemplo;

La Figura 5 es una realización, a modo de ejemplo, de una pila de protocolos del plano de control en la arquitectura LTE-Hi ilustrada en la Figura 4;

La Figura 6 es una realización, a modo de ejemplo, de una pila de protocolo de enlace de datos en la arquitectura LTE-Hi que se ilustra en la Figura 4;

La Figura 7 es una segunda realización, a modo de ejemplo, de la generación de una clave de estrato de acceso entre un equipo de usuario UE y el punto de acceso LTE-Hi AP en una arquitectura de LTE-Hi;

La Figura 8 es un diagrama de flujo de otro método para generar una clave de estrato de acceso realizada por una estación base en conformidad con una forma de realización de la presente invención;

La Figura 9 es un diagrama de flujo de otro método para generar una clave de estrato de acceso realizada por un dispositivo de acceso en conformidad con una forma de realización de la presente invención;

La Figura 10 es un diagrama de flujo de otro método para generar una clave de estrato de acceso realizada por un equipo de usuario en conformidad con una forma de realización de la presente invención;

La Figura 11 es una tercera realización, a modo de ejemplo, de la generación de una clave de estrato de acceso entre un equipo de usuario UE y un punto de acceso LTE-Hi AP en una arquitectura LTE-Hi;

La Figura 12 es un diagrama de flujo de otro método para generar una clave de estrato de acceso realizada por una estación base en conformidad con una forma de realización de la presente invención;

La Figura 13 es un diagrama de flujo de otro método para generar una clave de estrato de acceso realizada por un dispositivo de acceso en conformidad con una forma de realización de la presente invención;

La Figura 14 es un diagrama de flujo otro método para generar una clave de estrato de acceso realizada por un equipo de usuario en conformidad con una forma de realización de la presente invención;

La Figura 15 es un diagrama de bloques estructural de un dispositivo del lado de la red en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención;

La Figura 15a es otro diagrama de bloques estructural de un dispositivo del lado de la red en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención;

La Figura 16 es otro diagrama de bloques estructural de un dispositivo del lado de la red en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención;

La Figura 16a es otro diagrama de bloques estructural de un dispositivo del lado de la red en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención;

La Figura 17 es un diagrama de bloques estructural de un equipo de usuario en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención; y

La Figura 18 es otro diagrama de bloques estructural de un equipo de usuario en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

A continuación se describe de forma clara y completa, las soluciones técnicas en las formas de realización de la presente invención haciendo referencia a los dibujos adjuntos en las formas de realización de la presente invención. Evidentemente, las formas de realización descritas son una parte y no la totalidad de las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por un experto en esta técnica sobre la base de las formas de realización de la presente invención sin necesidad de esfuerzos creativos caerán dentro del alcance de protección de la presente invención.

En primer lugar, un método 100 para generar una clave de estrato de acceso en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención se describe haciendo referencia a la Figura 1. En el sistema de comunicaciones, un equipo de usuario UE accede a una red base por intermedio de una estación base utilizando una primera interfaz de aire y se conecta a la estación base por intermedio de un dispositivo de acceso utilizando una segunda interfaz de aire para acceder a la red base. Por lo tanto, el sistema de comunicaciones que aplica el método 100 es un sistema que soporta una transmisión de descarga de datos, y el equipo de usuario UE puede conectarse a la estación base utilizando las dos interfaces de aire al mismo tiempo. Dicho sistema de comunicaciones puede incluir, sin limitación, a: una arquitectura de LTE-Hi, una arquitectura de LTE-WiFi, una arquitectura WCDMA-WiFi y similares.

Según se ilustra en la Figura 1, el método 100 incluye:

en la etapa S110, la adquisición de un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del dispositivo de acceso;

en la etapa S120, el cálculo de una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la clave KeNB* se calcula también por el equipo de usuario UE en conformidad con el parámetro de entrada y la clave de estrato de acceso KeNB; y

en la etapa S130, el envío de la clave KeNB* al dispositivo de acceso de modo que el dispositivo de acceso genere una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el equipo UE en conformidad con la clave KeNB*.

El método 100 se realiza por la estación base. En conformidad con la técnica anterior, la estación base y el equipo UE pueden memorizar la clave KeNB en la primera interfaz de aire. En esta forma de realización de la presente invención, el dispositivo de acceso conectado a la segunda interfaz de aire y el equipo UE necesitan tener la misma clave KeNB*, en donde la clave KeNB* se utiliza como una clave raíz para deducir la clave AS en la segunda interfaz de aire de modo que el dispositivo de acceso y el equipo UE puedan generar la misma clave AS en la segunda interfaz de aire. Conviene señalar que, en esta especificación técnica, la estación base puede denominarse también como un primer dispositivo del lado de la red y el dispositivo de acceso puede denominarse también un segundo dispositivo del lado de la red.

La estación base puede adquirir la clave KeNB* utilizando el parámetro de entrada y la clave KeNB. El equipo de usuario UE puede adquirir también la clave KeNB* utilizando el parámetro de entrada y la clave KeNB. Cuando la estación base envía la clave KeNB* al dispositivo de acceso conectado a la segunda interfaz de aire, el equipo UE y el dispositivo de acceso conectado a la segunda interfaz de aire tienen la misma clave KeNB* con el fin de generar, sobre la base de la misma clave raíz, la clave AS en la segunda interfaz de aire.

El parámetro de entrada requerido para generar la clave KeNB* puede incluir el parámetro variable en el tiempo y/o el parámetro relacionado con la célula de servicio del dispositivo de acceso. De este modo, diferentes formas de realización pueden tener diferentes maneras para calcular, de forma flexible, la clave KeNB*. El parámetro variable en el tiempo es un parámetro que varía con el tiempo, que puede ser un valor de un contador específico, puede ser un número aleatorio generado de forma aleatoria o puede ser otro parámetro que un experto en esta técnica puede crear y que utiliza el tiempo como un argumento funcional. El parámetro relacionado con la célula de servicio del dispositivo de acceso puede incluir, sin limitación, a un identificador de célula de la célula de servicio del dispositivo de acceso y/o una frecuencia central de la célula de servicio del dispositivo de acceso. El parámetro relacionado con la célula de servicio del dispositivo de acceso puede ser también otro parámetro físico que un experto en esta técnica puede considerar y tiene la célula de servicio del dispositivo de acceso.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un valor de conteo COUNT (count)

del PDCP (Packet Data Convergence Protocol, Protocolo de Convergencia de Datos por Paquetes) de un soporte del equipo de usuario UE en la primera interfaz de aire. El valor de PDCP COUNT es un valor de conteo que existe ya en la técnica anterior. El valor de conteo aumenta progresivamente con el envío y la recepción de un paquete de datos sobre un soporte correspondiente. De este modo, la estación base y el equipo de usuario UE pueden adquirir adecuadamente el parámetro variable en el tiempo especificando el valor de PDCP COUNT de un soporte en la estación base y el equipo UE en lugar de intercambiar un mensaje, lo que puede economizar los recursos de la red.

A modo de ejemplo, el valor de PDCP COUNT puede ser un valor de PDCP COUNT de un soporte correspondiente a un mensaje de configuración. En conformidad con una forma de realización de la presente invención, el mensaje de configuración puede ser un mensaje de configuración utilizado por la estación base para configurar la segunda interfaz de aire. Solamente unos pocos mensajes de configuración utilizados por la estación base para configurar la segunda interfaz de aire se envían a este respecto. Por lo tanto, difícilmente ocurre un caso en el que el valor de PDCP COUNT del soporte correspondiente al mensaje de configuración es objeto de nuevo conteo puesto que el valor de conteo alcanza el valor máximo, de modo que el valor de PDCP COUNT utilizado para calcular la clave KeNB* es diferente cada vez, por lo que sirve de ayuda para garantizar que la clave KeNB* calculada para el equipo UE sea diferente. En otras formas de realización, el mensaje de configuración puede ser también un mensaje de configuración utilizado para la estación base para configurar otra interfaz de aire o canal. Además, el valor de PDCP COUNT puede ser también un valor de PDCP COUNT de un soporte correspondiente a un servicio del equipo de usuario UE en la primera interfaz de aire, a modo de ejemplo, un servicio de descarga de ficheros y similar.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por la estación base. En este caso, la estación base adquiere el parámetro de entrada en conformidad con el número aleatorio generado por sí misma. Para permitir al equipo de usuario UE adquirir también el parámetro de entrada, la estación base necesita enviar el número aleatorio generado por sí misma al equipo UE. A modo de ejemplo, la estación base puede enviar el mensaje de configuración utilizado para configurar la segunda interfaz de aire para el equipo UE, en donde el mensaje de configuración contiene el número aleatorio generado por la estación base. De este modo, el hecho de que contener el número aleatorio en el mensaje de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a una secuencia de envío de mensajes existente. El equipo UE y la estación base pueden generar la misma clave KeNB* utilizando el mismo parámetro.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por el equipo UE. En este caso, el equipo UE adquiere el parámetro de entrada en conformidad con el número aleatorio generado por sí mismo. Para permitir a la estación base adquirir también el parámetro de entrada, el equipo UE necesita enviar el número aleatorio generado por sí mismo a la estación base. A modo de ejemplo, la estación base puede recibir, desde el equipo UE, un mensaje de terminación de configuración en respuesta al mensaje de configuración utilizado para configurar la segunda interfaz de aire, en donde el mensaje de terminación de la configuración contiene el número aleatorio generado por el equipo UE. De este modo, el hecho de contener el número aleatorio en el mensaje de terminación de la configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a la secuencia de envío de mensajes existente.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un primer número aleatorio generado por la estación base y un segundo número aleatorio generado por el equipo UE. Para permitir a la estación base y al equipo UE tener el mismo parámetro de entrada para generar la misma clave KeNB*, la estación base necesita enviar el primer número aleatorio al equipo UE, a modo de ejemplo, utilizando el mensaje de configuración usado para configurar la segunda interfaz de aire, y el equipo UE necesita enviar el segundo número aleatorio a la estación base, a modo de ejemplo, utilizando el mensaje de terminación de configuración en respuesta al mensaje de configuración. La generación de la clave KeNB* utilizando los números aleatorios separadamente generados por la estación base y el equipo UE tiene una más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por la estación base o el equipo de usuario UE.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro relacionado con la célula de servicio del dispositivo de acceso, el parámetro relacionado con la célula de servicio del dispositivo de acceso puede incluir al menos uno de los elementos siguientes: el identificador de célula de la célula de servicio del dispositivo de acceso y la frecuencia central de la célula de servicio del dispositivo de acceso. El uso de parámetros pertinentes de células diferentes ayuda a garantizar que la clave KeNB* deducida es diferente para distintas células.

Después de calcular la clave KeNB*, la estación base la envía al dispositivo de acceso. De este modo, el dispositivo de acceso y el equipo UE pueden deducir, además, la clave de estrato de acceso en la segunda interfaz de aire en conformidad con la misma clave raíz KeNB*, con lo que se introduce la clave de estrato de acceso en la segunda interfaz de aire para ayudar a realizar una transmisión segura. Por lo tanto, cuando la clave de estrato de acceso se

utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, puede mejorarse la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

La Figura 1 ilustra el método 100 para generar una clave de estrato de acceso en un lado de estación base. A continuación se describe un método 200 para generar una clave de estrato de acceso en un lado del dispositivo de acceso en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 2 y un método 300 para generar una clave de estrato de acceso en un lado del equipo UE en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 3. Tanto el método 200 como el método 300 corresponden al método 100. Por lo tanto, para descripciones específicas del método 200 y del método 300, puede hacerse referencia a las partes correspondientes del método 100 y sus detalles no se describen aquí de nuevo para evitar su repetición. Tanto el método 200 como el método 300 se aplican al sistema de comunicaciones siguiente: un equipo UE accede a una red base por intermedio de una estación base utilizando una primera interfaz de aire y se conecta a la estación base por intermedio de un dispositivo de acceso utilizando una segunda interfaz de aire para acceder a la red base.

Según se ilustra en la Figura 2, el método 200 incluye:

en la etapa S210, la recepción de una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire desde la estación base, en donde la clave KeNB* se calcula por la estación base en conformidad con un parámetro de entrada adquirido y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, la clave KeNB* se calcula también por el equipo UE en el conformidad con el parámetro de entrada y la clave KeNB, y el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del dispositivo de acceso; y

en la etapa S220, se genera una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el equipo UE en conformidad con la clave KeNB*.

El método 200 se realiza por el dispositivo de acceso conectado a la segunda interfaz de aire. El dispositivo de acceso puede tener la misma clave raíz de estrato de acceso en la segunda interfaz de aire puesto que el equipo UE adquiere la clave KeNB* desde la estación base, de modo que la clave de estrato de acceso en la segunda interfaz de aire puede deducirse en conformidad con la misma clave raíz, con lo que se introduce la misma clave que ayuda a realizar una transmisión segura para la segunda interfaz de aire. Por lo tanto, cuando se utiliza la clave de estrato de acceso para la transmisión de datos por intermedio de la segunda interfaz de aire, puede mejorarse la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y garantizarse la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

Según se ilustra en la Figura 3, el método 300 incluye:

en la etapa S310, la adquisición de un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del dispositivo de acceso;

en la etapa S320, se calcula una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la clave KeNB* se calcula también por la estación base en conformidad con el parámetro de entrada y la clave KeNB y se envía al dispositivo de acceso; y

en la etapa S330, se genera una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el dispositivo de acceso en conformidad con la clave KeNB*.

El método 300 se realiza por el equipo de usuario. El equipo de usuario puede adquirir la clave KeNB* utilizando el parámetro de entrada y la clave KeNB, y el dispositivo de acceso puede adquirir la misma clave KeNB* desde la estación base. De este modo, el equipo de usuario y el dispositivo de acceso pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire en conformidad con la misma clave KeNB*, con lo que se introduce la misma clave para la segunda interfaz de aire para ayudar a realizar una transmisión de datos segura.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un valor de PDCP COUNT de un soporte del equipo UE en la primera interfaz de aire. De este modo, la estación base y el equipo de usuario UE pueden adquirir adecuadamente el parámetro variable en el tiempo especificando el valor de PDCP COUNT de un soporte para calcular la clave KeNB* en lugar de intercambiar un mensaje, lo que puede economizar recursos de red. A modo de ejemplo, el valor de PDCP COUNT puede ser un valor de PDCP COUNT de un soporte correspondiente a un mensaje de configuración utilizado para la estación base para configurar la segunda interfaz de aire.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por la estación base. De este modo, el equipo UE necesita recibir el número aleatorio procedente de la estación base para generar la misma clave KeNB* que la estación base. A modo de ejemplo, el equipo UE puede recibir el mensaje de configuración utilizado para configurar la segunda interfaz de aire desde la estación base, en donde el mensaje de configuración contiene el número aleatorio generado por la estación base. De este modo, la inclusión del número aleatorio en el mensaje de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y para garantizar que la transmisión del número aleatorio no afecte a una secuencia de envío de mensajes existente.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por el equipo UE. En este caso, el equipo UE necesita enviar el número aleatorio generado por sí mismo a la estación base, de modo que la estación base utilice el mismo parámetro de entrada para generar la misma clave KeNB* que el equipo UE. A modo de ejemplo, el equipo UE puede enviar un mensaje de terminación de configuración en respuesta al mensaje de configuración utilizado para configurar la segunda interfaz de aire a la estación base, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo UE. De este modo, la inclusión del número aleatorio en el mensaje de terminación de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la combustión del número aleatorio no afecta a una secuencia de envío de mensajes existente.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un primer número aleatorio generado por la estación base y un segundo número aleatorio generado por el equipo UE. Para permitir a la estación base y al equipo UE tener el mismo parámetro de entrada para generar la misma clave KeNB*, la estación base necesita enviar el primer número aleatorio al equipo UE, a modo de ejemplo, utilizando el mensaje de configuración utilizado para configurar la segunda interfaz de aire, y el equipo UE necesita enviar el segundo número aleatorio a la estación base, a modo de ejemplo, utilizando el mensaje de terminación de configuración en respuesta al mensaje de configuración. La generación de la clave KeNB* utilizando los números aleatorios separadamente generados por la estación base y el equipo UE tiene más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por la estación base o el equipo UE.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro relacionado con la célula de servicio del dispositivo de acceso, el parámetro relacionado con la célula de servicio del dispositivo de acceso puede incluir al menos uno de los elementos siguientes: un identificador de célula de la célula de servicio del dispositivo de acceso y una frecuencia central de la célula de servicio del dispositivo de acceso. La utilización de parámetros pertinentes de diferentes células ayuda a garantizar que la clave KeNB* deducida es diferente para distintas células.

En conformidad con el método para generar una clave de estrato de acceso en esta forma de realización de la presente invención, el equipo de usuario y el dispositivo de acceso pueden utilizar la misma clave raíz KeNB* para generar la misma clave de estrato de acceso en la segunda interfaz de aire. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, puede mejorarse la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

A continuación se describe la puesta en práctica específica del método 100 al método 300 con referencia a casos prácticos específicos a modo de ejemplo. Un primer ejemplo y un segundo ejemplo se utilizan simplemente para ayudar a entender las soluciones técnicas proporcionadas por la presente invención y no plantear ninguna limitación sobre el alcance de protección de la presente invención. Antes de que se describa el primer ejemplo y el segundo ejemplo, se describe, haciendo referencia a la Figura 4 una realización, a modo de ejemplo, de un sistema de comunicación en el que se aplica un método para generar una clave de estrato de acceso. La Figura 4 ilustra una arquitectura de LTE-Hi. En esta arquitectura, una interfaz de aire Uu es la primera interfaz de aire, una interfaz de aire Uu' es la segunda interfaz de aire y un punto de acceso LTE-Hi AP es un dispositivo de acceso de la interfaz de aire Uu' se conecta a un nodo eNB para permitir a un equipo de usuario UE acceder a una red base. Esta arquitectura tiene también como objetivo ayudar a entender mejor las soluciones técnicas dadas a conocer por la presente invención y no plantea ninguna limitación sobre el alcance de protección de la presente invención.

En la arquitectura de LTE-Hi ilustrada en la Figura 4, el equipo de usuario UE puede acceder al nodo eNB utilizado la interfaz de aire Uu y luego, conectarse a una entidad MME (Mobility Management Entity, entidad de gestión de movilidad). Si el equipo UE está situado dentro de una zona de cobertura de una célula de servicio de un punto de acceso LTE-Hi AP 1, el equipo UE puede acceder también el punto de acceso LTE-Hi AP 1 utilizando la interfaz de aire Uu', el punto de acceso LTE-Hi AP 1 es objeto de convergencia a una pasarela LTE-Hi GW (gateway, pasarela) y la pasarela LTE-Hi GW se conecta al nodo eNB, con el fin de conectar el equipo UE a la entidad MME. La pasarela LTE-Hi GW en la Figura 4 puede converger señales del punto de acceso LTE-Hi AP 1 y un punto de acceso LTE-Hi

AP 2. Las conexiones de S1 con varios puntos de acceso LTE-Hi APs puede ser objeto de convergencia por la pasarela LTE-Hi GW, con lo que se reduce el número de conexiones S1 y la puesta en práctica del control y gestión de recursos de Hi.

Además de la conexión a una red base LTE utilizando el nodo eNB y el punto de acceso LTE-Hi AP (incluyendo el punto de acceso LTE-Hi AP 1 o el punto de acceso LTE-Hi AP 2 en la Figura 4), el equipo UE puede conectarse también a una red de servicio IP del operador y una red Internet por intermedio de la pasarela S/P GW utilizando el nodo eNB y el punto de acceso LTE-Hi AP o conectarse a Internet y una red Intranet por intermedio de una pasarela L-GW utilizando el punto de acceso LTE-Hi AP.

En la arquitectura de LTE-Hi ilustrada en la Figura 4, el equipo de usuario UE conectado al nodo eNB y al punto de acceso LTE-Hi AP 1, el punto de acceso LTE-Hi AP 1 y el nodo eNB pueden tener una pila de protocolos del plano de control que se ilustra en la Figura 5. El punto de acceso LTE-Hi AP 1 accede al nodo eNB utilizando una interfaz S1 mejorada, es decir, una interfaz S1'. Además, el equipo de usuario UE, el punto de acceso LTE-Hi AP 1 y el nodo eNB puede tener una pila de protocolos del plano de datos que se ilustra en la Figura 6. Los protocolos ilustrados en la pila de protocolos son los mismos que los de la técnica anterior y por ello no se describen aquí de nuevo. En conformidad con una pila de protocolos que se ilustra a modo de ejemplo, el equipo UE puede acceder a la red base por intermedio del nodo eNB utilizando la primera interfaz de aire Uu y conectarse al nodo eNB por intermedio del punto de acceso LTE-Hi AP 1 utilizando la segunda interfaz de aire Uu' para acceder a la red base.

En la arquitectura LTE-Hi ilustrada en la Figura 4, una clave de estrato de acceso puede generarse entre el equipo UE y el punto de acceso LTE-Hi AP 1 utilizando el método anterior, de modo que pueda realizarse una transmisión de datos segura entre el equipo de usuario UE y el punto de acceso LTE-Hi AP 1. Para brevedad de las descripciones, el punto de acceso LTE-Hi AP 1 al que se conecta el equipo UE se denomina un nodo LTE-Hi, de forma abreviada, en los ejemplos primero y segundo descritos a continuación. Además, un tercer ejemplo y un cuarto ejemplo siguientes se describen también sobre la base de la arquitectura de LTE-Hi en la Figura 4 y el punto de acceso LTE-Hi AP 1 al que se conecta el equipo UE se denomina también el nodo LTE-Hi en forma abreviada.

Primera realización a modo de ejemplo

Un equipo UE accede a una red utilizando un nodo eNB, para una necesidad de descarga, el nodo eNB establece una bifurcación de Hi para una interfaz de aire Uu'. La bifurcación de Hi se refiere a un radioenlace entre el equipo UE y el nodo LTE-Hi.

El nodo eNB configura la interfaz de aire Uu' para el equipo UE utilizando un método de reconfiguración de conexión. El equipo UE configura una RRC (Radio Resource Connection, conexión de recursos de radio) con el nodo LTE-Hi en conformidad con un mensaje de configuración y luego, se deduce, a nivel local, una clave KeNB* utilizada en una clave raíz de estrato de acceso en la interfaz de aire Uu'. El nodo eNB puede deducir la clave KeNB* en conformidad con la misma lógica y enviar la clave KeNB* deducida al nodo LTE-Hi.

Puesto que cambia el volumen de servicio, el nodo eNB puede liberar la bifurcación de Hi utilizada para la descarga. Cuando la bifurcación de Hi es posteriormente reañadida para la descarga, necesitan ser diferentes las múltiples claves raíces de estratos de acceso deducidas por el nodo eNB durante el establecimiento de la bifurcación de Hi. Por lo tanto, una entrada de deducción de clave de la bifurcación de Hi puede incluir un parámetro variable en el tiempo. El parámetro variable en el tiempo puede ser un valor de PDCP COUNT de un soporte, que se sincroniza por el nodo eNB y el equipo UE, a modo de ejemplo, el valor de PDCP COUNT de un soporte para enviar una señalización de RRC, o puede ser otro parámetro variable en el tiempo calculado sobre la base del valor de PDCP COUNT.

En el equipo UE y en el nodo eNB, la siguiente expresión puede utilizarse para calcular la clave KeNB*:

KeNB*=KDF (KeNB, PCI, DL EARFCN, PDCP COUNT)

en donde, KDF es una función de generación de claves; la clave KeNB es una clave raíz de estrato de acceso en una interfaz de aire Uu o una clave adquirida en conformidad con esta clave raíz, el valor de PDCP COUNT puede ser un valor de PDCP COUNT correspondiente al soporte contenido en el mensaje de configuración para configurar la bifurcación de Hi; el PCI (Physical Cell Identity, identidad de célula física) es un identificador de célula para una célula LTE-Hi cubierta por el nodo LTE-Hi; el valor DL EARFCN (DownLink E-UTRA Absolute Radio Frequency Channel Number, número de canal de radiofrecuencias absoluto de E-UTRA de enlace descendente) indica una frecuencia central de la célula LTE-Hi. Esta expresión es simplemente a modo de ejemplo y no plantea ninguna limitación sobre la forma de adquisición de la clave KeNB*.

Después de adquirir la clave KeNB*, el nodo LTE-Hi puede activar la protección de seguridad del estrato de acceso en la interfaz de aire Uu' por medio de un proceso de AS SMC (Access Stratum Security Mode Command, orden del modo de seguridad del estrato de acceso). El proceso de activación puede ser el mismo que un proceso de activación de la protección de seguridad de estrato de acceso en la interfaz de aire Uu en la técnica anterior con la

excepción de que un parámetro interviniente en el proceso es un parámetro en la interfaz de aire Uu' en lugar de un parámetro en la interfaz de aire Uu. Además, una manera de deducir la clave de estrato de acceso incluyendo una clave de protección de integridad de señalización de RRC, una clave de cifrado y una clave de cifrado de datos del plano de usuario en la interfaz de aire Uu' puede ser la misma que una manera de deducir una clave de estrato de acceso de LTE y por ello no se describe aquí de nuevo.

Segunda realización a modo de ejemplo

Una diferencia entre la segunda realización, a modo de ejemplo, ilustrada en la Figura 7 y la primera realización, a modo de ejemplo, radica principalmente en una manera de adquisición de la clave KeNB*. Una clave KeNB* se calcula en conformidad con un número aleatorio en la segunda realización a modo de ejemplo, pero se calcula en conformidad con el valor de PDCP COUNT en el primer ejemplo.

En el segundo ejemplo, el número aleatorio se introduce para distinguir diferentes claves deducidas por un nodo eNB en un tiempo diferente:

KeNB*=KDF (KeNB, PCI, DL EARFCN, nonce1, nonce2)

en donde KeNB* es una clave raíz de estrato de acceso en una interfaz de aire Uu'; KDF es una función de generación de claves; KeNB es una clave raíz de estrato de acceso en una interfaz de aire Uu; PCI es un identificador de velocidad de una célula LTE-Hi cubierta por un nodo LTE-Hi; DL EARFCN indica una frecuencia central de la célula LTE-Hi; nonce1 es un número aleatorio generado por el nodo eNB; nonce2 es un número aleatorio generado por un equipo UE. Conviene señalar que, aunque los parámetros nonce1 y nonce2 se utilizan en la manera de deducción de la clave KeNB* anterior, nonce1 o nonce2 pueden utilizarse de forma independiente en tanto que el número aleatorio se utiliza cuando se deduce la clave KeNB*. Cuando nonce1 y nonce2 se utilizan para deducir la clave KeNB*, puede proporcionarse una mejor seguridad. Además, esta expresión es simplemente a modo de ejemplo y no plantea ninguna limitación sobre cómo adquirir la clave KeNB*. A modo de ejemplo, cuando se deduce la clave KeNB*, solamente puede utilizarse el identificador PCI o DL EARFCN o ninguno de ellos.

En la etapa S705, el equipo UE realiza una transmisión de datos con el nodo eNB utilizando la interfaz de aire Uu. Los datos comunicados entre el equipo UE y una red base, una red de paquetes o similar se reenvían entre el nodo eNB y una pasarela MME/SGW (Serving Gateway, pasarela de servicio)/PGW (Packet Data Network Gateway, pasarela de red de datos por paquetes).

Según se ilustra en la Figura 7, tres canales de datos están configurados entre el equipo UE y la pasarela MME/SGW/PGW, esto es, el soporte de E-RAB (E-UTRAN Radio Access Bearer, soporte de acceso a radio de E-UTRAN)=0, E-RAB=1, y E-RAB=2. E-RAB=0 incluye el soporte de radio (Radio Bearer, RB)=0 entre el equipo UE y el nodo eNB y un soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW; E-RAB= 1 incluye RB=1 entre el equipo UE y el nodo eNB y el soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW; E-RAB=2 incluye RB=2 entre el equipo UE y el nodo eNB y el soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW.

En la etapa S710, el equipo UE realiza la medición del punto de acceso LTE-Hi AP.

En la etapa S715, el equipo UE envía un informe de medición al nodo eNB, en donde el informe de medición contiene una lista de CGI (Cell Global Identity, identidad global de célula) encontrada por el equipo UE para los puntos de acceso LTE-Hi APs.

En la etapa S720, el nodo eNB selecciona, en conformidad con el informe de medición, un punto de acceso LTE-Hi AP a partir de los puntos de acceso LTE-Hi APs informados por el equipo UE para servir al nodo eNB. En esta realización, se supone que el nodo eNB selecciona el punto de acceso LTE-Hi AP 1 en la arquitectura ilustrada en la Figura 4, que se denomina, en forma abreviada, el nodo LTE-Hi.

En la etapa S725, el nodo eNB envía un mensaje de reconfiguración de conexión de RRC (RRCConnectionReconfiguration) al equipo UE, en donde el mensaje incluye el CGI del punto de acceso LTE-Hi AP seleccionado por el nodo eNB. Si el número aleatorio nonce1 generado por el nodo eNB necesita utilizarse para deducir la clave KeNB*, el parámetro nonce1 está contenido también en el mensaje de reconfiguración de conexión de RRC.

En la etapa S730, el equipo UE calcula la clave KeNB* y deduce una clave de estrato de acceso en la interfaz de aire Uu' en conformidad con la clave KeNB*. Según se describe en la expresión en el segundo ejemplo, la clave KeNB* puede calcularse utilizando nonce1, utilizando nonce2 o utilizando ambos nonce1 y nonce2. Cuando nonce2 necesita utilizarse para el cálculo de la clave KeNB*, el equipo UE genera el número aleatorio nonce2 de forma aleatoria.

En la etapa S735, el equipo UE envía un mensaje de demanda de conexión de RRC (RRCConnectionRequest) al nodo LTE-Hi en conformidad con el nodo LTE-Hi seleccionado por el nodo eNB.

En la etapa S740, el nodo LTE-Hi envía un mensaje de configuración de conexión de RRC (RRCConnectionSetup) al equipo UE.

En la etapa S745, el equipo UE envía un mensaje de terminación de configuración de conexión de RRC (RRCConnectionSetupComplete) al nodo LTE-Hi.

En la etapa S750, el equipo UE accede a la célula LTE-Hi servida por el nodo LTE-Hi y envía un mensaje de terminación de reconfiguración de conexión de RRC (RRCConnectionReconfigurationComplete) al nodo eNB. Cuando necesita utilizarse nonce2 para deducir la clave KeNB*, además de un identificador C-RNTI (Cell-Radio Network Temporary Identifier, identificador temporal de red de radio-celular) asignado por el nodo LTE-Hi que necesita transmitirse por este mensaje en la técnica anterior, este mensaje necesita también contener nonce2.

En la etapa S755, el nodo eNB calcula la clave KeNB*. Cuando el número nonce2 aleatoriamente generado por el equipo UE necesita utilizarse para el cálculo de la clave KeNB*, el nodo eNB necesita calcular la clave KeNB* después de recibir el nonce2 en la etapa S750. Cuando solamente se requiere nonce1 en lugar de nonce2 para el cálculo de la clave KeNB*, el nodo eNB puede calcular también la clave KeNB* después de que se genere nonce1.

En la etapa S760, el nodo eNB envía un contexto del equipo UE al nodo LTE-Hi, en donde el contexto del equipo UE necesita incluir la clave KeNB* y una capacidad de seguridad del equipo UE. La clave KeNB* se utiliza por el nodo LTE-Hi para deducir la clave de estrato de acceso y la capacidad de seguridad del equipo UE se utiliza por el nodo LTE-Hi para realizar una negociación operativa de AS SMC con el equipo UE.

En la etapa S765, el nodo LTE-Hi inicia operativamente un proceso de AS SMC para negociar un algoritmo de seguridad de la interfaz Uu' con el equipo UE y activa la protección de seguridad de AS. El proceso de AS SMC realizado por el nodo LTE-Hi y el equipo UE puede ser el mismo que un proceso de AS SMC realizado en la interfaz de aire Uu en la técnica anterior y por ello no se describe aquí de nuevo. Después de lo que antecede, puede realizarse una protección de cifrado e integridad en todos los mensajes en la interfaz de aire Uu' en conformidad con Krreint y Krrcenc deducidos de la clave KeNB* y puede realizarse una protección de cifrado para datos del plano del usuario en conformidad con Kupenc. Un método para deducir una clave de protección de la integridad y una clave de cifrado de la señalización de RRC y una clave de cifrado para los datos del plano del usuario es el mismo que un método para deducir una clave de LTE AS.

En la etapa S770, el nodo eNB envía un mensaje de demanda de configuración de E-RAB al nodo LTE-Hi, en donde el mensaje contiene una lista de E-RAB a establecerse y C-RNTI del equipo de usuario UE. Se supone que ha de establecerse E-RAB=2

En la etapa S775, el nodo LTE-Hi envía el mensaje de reconfiguración de conexión de RRC al equipo UE, en donde el mensaje contiene E-RAB=2 y RB=3.

En la etapa S780, el equipo UE reenvía el mensaje de terminación de reconfiguración de conexión de RRC al nodo LTE-Hi.

En la etapa S785, el nodo LTE-Hi reenvía un mensaje de respuesta de configuración de E-RAB al nodo eNB, en donde el mensaje contiene una lista de configuración de E-RAB que incluye a RB=3.

En la etapa S790, el nodo eNB envía el mensaje de reconfiguración de conexión de RRC al equipo UE, demandado al UE la liberación de RB=2.

En la etapa S795, el equipo UE reenvía el mensaje de terminación de reconfiguración de conexión de RRC al nodo eNB.

De este modo, los tres canales de datos E-RAB=0, E-RAB=1 y E-RAB=2 se configuran entre el equipo UE y la pasarela MME/SGW/PGW en la configuración de la bifurcación de Hi por el nodo eNB. E-RAB=0 y E-RAB= 1 son los mismos valores que E-RAB=0 y E-RAB=1 iniciales. E-RAB=2 después de la reconfiguración incluye RB=3 entre el equipo UE y el nodo LTE-Hi, un soporte S1' entre el nodo LTE-Hi y el nodo eNB y el soporte de S1 entre el nodo eNB y la pasarela MME/SGW/PGW.

A continuación se describe otro método 800 para generar una clave de estrato de acceso en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 8. En el sistema de comunicaciones, un equipo de usuario UE accede a una red base por intermedio de una estación base utilizando una primera interfaz de aire y se conecta a la estación base por intermedio de un dispositivo de acceso utilizando una segunda interfaz de aire para acceder a la red base. Por lo tanto, el sistema de comunicaciones al que se aplica el método 800 es un sistema que soporta la transmisión de descarga de datos y el equipo de usuario UE puede conectarse a la estación base utilizando las dos interfaces al mismo tiempo. Dicho sistema de comunicaciones puede incluir, sin limitación, a: una arquitectura de LTE-Hi, una arquitectura de LTE-

WiFi, una arquitectura WCDMA-WiFi y similares.

Según se ilustra en la Figura 8, el método 800 incluye:

en la etapa S810, la adquisición de una clave raíz de estrato de acceso KeNB en la primera interfaz de aire; y

en la etapa S820, el envío de la clave KeNB al dispositivo de acceso de modo que el dispositivo de acceso calcule una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con un parámetro de entrada adquirido y la clave KeNB y genera una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*, en donde la clave KeNB* se calcula también por el equipo UE en conformidad con el parámetro de entrada y la clave KeNB, la clave de estrato de acceso en la segunda interfaz de aire se genera también por el equipo UE en conformidad con la clave KeNB*, y el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del dispositivo de acceso.

El método 800 se realiza por la estación base. En conformidad con la técnica anterior, la estación base y el equipo UE memorizan la clave KeNB en la primera interfaz de aire. En esta forma de realización de la presente invención, la estación base envía la clave KeNB memorizada al dispositivo de acceso. De este modo, el dispositivo de acceso puede generar la clave KeNB* en conformidad con el parámetro de entrada y la clave KeNB. El equipo UE tiene también el mismo parámetro de entrada y por lo tanto, el equipo UE puede generar también la clave KeNB* en conformidad con la clave KeNB memorizada en el equipo UE. De este modo, el dispositivo de acceso y el equipo UE pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire en conformidad con la misma clave raíz KeNB*.

En consecuencia, la clave de estrato de acceso puede introducirse en la segunda interfaz de aire para ayudar a realizar una transmisión segura. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, puede mejorarse la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

La Figura 8 describe el método 800 para generar una clave de estrato de acceso en un lado de la estación base. A continuación se describe un método 900 para generar una clave de estrato de acceso en un lado del dispositivo de acceso en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 9 y un método 1000 para generar una clave de estrato de acceso en un lado del equipo de usuario UE en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 10. Tanto el método 900 como el método 1000 corresponden al método 800. Por lo tanto, para descripciones específicas del método 900 y del método 1000, puede hacerse referencia a las partes correspondientes del método 800 y por ello no se describen aquí los detalles para evitar una repetición. Tanto el método 900 como el método 1000 se aplican al sistema de comunicaciones siguiente: un equipo de usuario UE accede a una red base por intermedio de una estación base utilizando una primera interfaz de aire y se conecta a la estación base por intermedio de un dispositivo de acceso utilizando una segunda interfaz de aire para acceder a la red base.

Según se ilustra en la Figura 9, el método 900 incluye:

en la etapa S910, la adquisición de un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo y/o u parámetro relacionado con una célula de servicio del dispositivo de acceso;

en la etapa S920, la recepción de una clave raíz de estrato de acceso KeNB en la primera interfaz de aire procedente de la estación base;

en la etapa S930, el cálculo de una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y la clave KeNB, en donde la clave KeNB* se calcula también por el equipo UE en conformidad con el parámetro de entrada y la clave KeNB; y

en la etapa S940, la generación de una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*, en donde el clave de estrato de acceso en la segunda interfaz de aire se genera también por el equipo UE en conformidad con la clave KeNB*.

El método 900 se realiza por el dispositivo de acceso. El dispositivo de acceso puede generar la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire utilizando el parámetro de entrada adquirido y la clave KeNB recibida procedente de la estación base. El equipo de usuario UE puede generar también la misma clave KeNB* utilizando el parámetro de entrada adquirido y la clave KeNB memorizada en el equipo UE. De este modo, tanto el dispositivo de acceso como el equipo UE pueden tener la misma clave raíz KeNB* y pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire utilizando la clave KeNB*, con lo que se mejora la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire.

Aunque la etapa S910 se realiza antes que la etapa S920 en el método 900, S910 puede realizarse también

después de S920 o puede realizarse de manera simultánea con S920 en tanto que se realicen antes de S930.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por el dispositivo de acceso. En este caso, el dispositivo de acceso adquiere el parámetro de entrada en conformidad con el número aleatorio generado por sí mismo. Para permitir al equipo UE adquirir también el parámetro de entrada, el dispositivo de acceso necesita enviar el número por sí mismo al equipo UE. A modo de ejemplo, el dispositivo de acceso puede enviar un mensaje de orden del modo de seguridad al equipo UE, en donde el mensaje de orden del modo de seguridad contiene el número aleatorio generado por el dispositivo de acceso. De este modo, la circunstancia de que el número aleatorio se contenga en el mensaje de orden del modo de seguridad puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a una secuencia de envío de mensajes existente. El equipo de usuario UE y el dispositivo de acceso pueden generar la misma clave KeNB* utilizando el mismo parámetro de entrada y la clave KeNB.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por el equipo UE. En este caso, el equipo UE adquiere el parámetro de entrada en conformidad con el número aleatorio generado por sí mismo. Para permitir al dispositivo de acceso adquirir también el parámetro de entrada, el equipo UE necesita enviar el número aleatorio generado por sí mismo al dispositivo de acceso. A modo de ejemplo, el dispositivo de acceso puede recibir un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está correctamente configurado en la segunda interfaz de aire desde el equipo UE, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo UE. De este modo, la inclusión del número aleatorio en el mensaje de terminación de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y asegurar que la transmisión del número aleatorio no afectará a la secuencia de envío de mensajes existente.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un primer número aleatorio generado por el dispositivo de acceso y un segundo número aleatorio generado por el equipo UE. Para permitir al dispositivo de acceso y al equipo UE tener el mismo parámetro de entrada para generar la misma clave KeNB*, el dispositivo de acceso necesita enviar el primer número aleatorio al equipo UE, a modo de ejemplo, utilizando el mensaje de orden del modo de seguridad, y el equipo UE necesita enviar el segundo número aleatorio a la estación base, a modo de ejemplo, utilizando el mensaje de terminación de configuración usado para indicar que el enlace de radio está correctamente configurado en la segunda interfaz de aire. La generación de la clave KeNB* utilizando los números aleatorios generados por el dispositivo de acceso y el equipo UE tienen una más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por el dispositivo de acceso o el equipo UE.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro relacionado con una célula de servicio del dispositivo de acceso, el parámetro relacionado con la servicio de servicio del dispositivo de acceso puede incluir al menos uno de los elementos siguientes: un identificador de célula de la célula de servicio del dispositivo de acceso y una frecuencia central de la célula de servicio del dispositivo de acceso. El uso de parámetros pertinentes de diferentes células ayuda a garantizar que la clave KeNB* deducida sea distinta para células diferentes.

En conformidad con el método para la generación de una clave de estrato de acceso en esta forma de realización de la presente invención, el equipo de usuario y el dispositivo de acceso pueden utilizar el mismo parámetro de entrada y la clave KeNB para generar la misma clave raíz KeNB*, de modo que la misma clave de estrato de acceso en la segunda interfaz de aire pueda deducirse sobre la base de la clave KeNB*. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y está garantizada la seguridad de la transmisión de datos entre el dispositivo de acceso y el equipo de usuario.

Según se ilustra en la Figura 10, el método 1000 incluye:

en la etapa S1010, la adquisición de un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del dispositivo de acceso;

en la etapa S1020, el cálculo de una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la clave KeNB* se calcula también por el dispositivo de acceso en conformidad con el parámetro de entrada y la clave KeNB recibida desde la estación base; y

en la etapa S1030, la energía de una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el

dispositivo de acceso en conformidad con la clave KeNB*.

El método 1000 se realiza por el equipo de usuario. El equipo de usuario puede generar la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire utilizando el parámetro de entrada adquirido y la clave de estrato de acceso KeNB conocida por sí mismo. El dispositivo de acceso puede generar también la misma clave KeNB* utilizando el parámetro de entrada adquirido y la clave KeNB recibida desde la estación base. De este modo, el equipo de usuario y el dispositivo de acceso pueden tener la misma clave raíz KeNB* y pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire utilizando la clave KeNB*, con lo que se mejora la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por el dispositivo de acceso. En este caso, el equipo UE necesita recibir el número aleatorio generado por el dispositivo de acceso procedente del dispositivo de acceso. A modo de ejemplo, el equipo UE puede recibir un mensaje de orden del modo de seguridad procedente del dispositivo de acceso, en donde el mensaje de orden del modo de seguridad contiene el número aleatorio generado por el dispositivo de acceso. De este modo, la inclusión del número aleatorio en el mensaje de orden del modo de seguridad puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a una secuencia de envío de mensajes existente. El equipo UE y el dispositivo de acceso pueden generar la misma clave KeNB* utilizando el mismo parámetro de entrada y la clave KeNB, con lo que se deduce la misma clave de estrato de acceso.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un número aleatorio generado por el equipo de UE. En este caso, el equipo UE necesita enviar el número aleatorio generado al dispositivo de acceso de modo que el dispositivo de acceso pueda generar la misma clave KeNB* que el equipo UE. A modo de ejemplo, el equipo UE puede enviar un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está correctamente configurado en la segunda interfaz de aire para el dispositivo de acceso, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo UE. De este modo, la inclusión del número aleatorio en el mensaje de terminación de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afectará a la secuencia de envío de mensajes existente.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro variable en el tiempo, el parámetro variable en el tiempo puede incluir un primer número aleatorio generado por el dispositivo de acceso y un segundo número aleatorio generado por el equipo UE. Para permitir al dispositivo de acceso y al equipo UE tener el mismo parámetro de entrada para generar la misma clave KeNB*, el dispositivo de acceso necesita enviar el primer número al equipo UE, a modo de ejemplo, utilizando el mensaje de orden del modo de seguridad, y el equipo UE necesita enviar el segundo número aleatorio al dispositivo de acceso, a modo de ejemplo, utilizando el mensaje de terminación de configuración usado para indicar que el enlace de radio está correctamente configurado en la segunda interfaz de aire. La generación de la clave KeNB* utilizando los números aleatorios generados por separado por el dispositivo de acceso y el equipo UE tienen más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por el dispositivo de acceso o el equipo UE.

En conformidad con una forma de realización de la presente invención, cuando el parámetro de entrada incluye el parámetro relacionado con la célula de servicio del dispositivo de acceso, el parámetro relacionado de la célula de servicio del dispositivo de acceso puede incluir al menos uno de los elementos siguientes: un identificador de célula de la célula de servicio del dispositivo de acceso y una frecuencia central de la célula de servicio del dispositivo de acceso. El uso de parámetros pertinentes de distintas células ayuda a garantizar que la clave KeNB* deducida es distinta para diferentes células.

En conformidad con el método para generar una clave de estrato de acceso en esta forma de realización de la presente invención, el equipo de usuario y el dispositivo de acceso pueden utilizar el mismo parámetro de entrada y la clave KeNB para generar la misma clave raíz KeNB*, de modo que la misma clave de estrato de acceso en la segunda interfaz de aire pueda deducirse sobre la base de la clave KeNB*. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

A continuación se describe una puesta en práctica específica del método 800 al método 1000 con referencia a una realización específica, a modo de ejemplo. Un tercer ejemplo se utiliza simplemente para ayudar a entender las soluciones técnicas dadas a conocer por la presente invención y no plantea ninguna limitación sobre el alcance de protección de la presente invención. El tercer ejemplo se pone en práctica también en la arquitectura de LTE-Hi ilustrada en la Figura 4 y el punto de acceso LTE-Hi AP 1 se denomina también un nodo LTE-Hi.

Tercera realización a modo de ejemplo

Una diferencia entre el tercer ejemplo ilustrado en la Figura 11 y el segundo ejemplo radica principalmente en una entidad de cálculo de la clave KeNB*. Una clave KeNB* se calcula por el nodo LTE-Hi y un equipo UE en el tercer ejemplo pero se calcula mediante un nodo eNB y el equipo UE en el segundo ejemplo.

En el tercer ejemplo, el nodo LTE-Hi y el equipo UE pueden deducir una clave raíz de estrato de acceso KeNB* en una interfaz de aire Uu' en conformidad con la expresión siguiente:

KeNB*=KDF (KeNB, PCI, DL EARFCN, nonce3, nonce4)

en donde KDF es una función de generación de claves; la clave KeNB es una clave raíz de estrato de acceso en una interfaz de aire Uu; PCI es un identificador de célula de una célula LTE-Hi cubierta por el nodo LTE-Hi; DL EARFCN indica una frecuencia central de la célula LTE-Hi; el nonce3 es un número aleatorio generado aleatoriamente por el nodo LTE-Hi; nonce4 es un número aleatorio generado de forma aleatoria por el equipo UE. Conviene señalar que, aunque nonce3 y nonce4 se utilizan en la manera de deducción de la clave KeNB* anterior, nonce3 o nonce4 pueden utilizarse independientemente en tanto que el número aleatorio se utilice cuando se proceda a la deducción de la clave KeNB*. Cuando nonce3 y nonce4 se utilizan para deducir la clave KeNB*, puede proporcionarse una mejor seguridad y los valores de las claves deducidas en un distinto momento son diferentes. Además, nonce3 y nonce4 tienen una función anti-retransmisión. Además, esta expresión es solamente a modo de ejemplo y no plantea ninguna limitación sobre la forma de adquirir la clave KeNB*. A modo de ejemplo, el nodo LTE-Hi puede utilizar solamente PCI o DL EARFCN o puede no utilizar ninguno de ellos cuando se deduce la clave KeNB*. Cuando solamente una célula Hi está nivel bajo el nodo LTE-Hi, no se puede utilizar PCI y DL EARFCN.

En la etapa S1105, el equipo UE realiza la transmisión de datos con el nodo eNB utilizando la interfaz de aire Uu, y los datos comunicados entre el equipo UE y una red base, una red de paquetes o similar que se reenvía entre el nodo eNB y la pasarela MME/SGW/PGW.

Según se ilustra en la Figura 11, tres canales de datos se configuran entre el equipo UE y la pasarela MME/SGW/PGW, es decir, E-RAB=0, E-RAB= 1 y E-RAB=2. E-RAB=0 incluye RB=0 entre el equipo UE y el nodo eNB y un soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW; E-RAB=1 incluye RB=1 entre el equipo UE y el nodo eNB y el soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW; E-RAB=2 incluye RB=2 entre el equipo UE y el nodo eNB y el soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW

En la etapa S1110, el equipo UE realiza el contexto del punto de acceso LTE-Hi AP.

En la etapa S1115, el equipo UE envía un informe de medición al nodo eNB, en donde el informe de medición incluye una lista de CGI encontrada por el equipo UE para los puntos de acceso LTE-Hi APs.

En la etapa S1120, el nodo eNB selecciona, en conformidad con el informe de medición, un punto de acceso LTE-Hi AP desde entre los puntos de acceso LTE-Hi APs informados por el equipo UE para servir al nodo eNB. En este ejemplo, se supone que el nodo eNB selecciona el punto de acceso LTE-Hi AP 1 en la arquitectura ilustrada en la Figura 4, que se denomina el nodo LTE-Hi de forma abreviada.

En la etapa S1125, el nodo eNB envía un reconfiguración de reconfiguración de RRC al equipo UE, en donde el mensaje contiene un CGI del LTE-Hi AP seleccionado por el nodo eNB.

En la etapa S1130, el equipo UE envía un mensaje de demanda de conexión de RRC al nodo LTE-Hi.

En la etapa S1135, el nodo LTE-Hi envía un mensaje de configuración de conexión de RRC al equipo UE.

En la etapa S1140, el nodo LTE-Hi envía un mensaje de terminación de configuración de conexión de RRC al equipo UE, en donde el mensaje contiene el número aleatorio nonce4 generado por el equipo UE.

En la etapa S1145, el equipo UE envía un mensaje de terminación de reconfiguración de conexión de RRC al nodo eNB, en donde el mensaje contiene un C-RNTI asignado por el nodo LTE-Hi.

En la etapa S1150, el nodo eNB envía un contexto de UE al nodo LTE-Hi, en donde el contexto del UE incluye la clave KeNB y una capacidad de seguridad del UE.

En la etapa S1155, el nodo LTE-Hi genera el número aleatorio nonce3, calcula la clave KeNB* en conformidad con el nonce4 recibido y el nonce3 aleatoriamente generado, y calcula una cálculo en conformidad con la clave KeNB*.

En la etapa S1160, el nodo LTE-Hi envía una orden del modo de seguridad al equipo UE, en donde la orden contiene el número aleatorio nonce3.

En la etapa S1165, el equipo UE calcula la clave KeNB* en conformidad con los números aleatorios nonce4 y nonce3 y calcula la clave raíz de estrato de acceso en conformidad con la clave KeNB*.

En la etapa S1170, el equipo UE reenvía un mensaje de terminación de modo de seguridad al nodo LTE-Hi. Después de esa operación, se realizan las protecciones de integridad y cifrado en todos los mensajes de RRC transmitidos entre el equipo UE y el nodo LTE-Hi, utilizando los parámetros Krreint y Krrcenc deducidos a partir de la clave KeNB* y se realiza la protección de cifrado para todos los datos del plano del usuario utilizando Kupenc deducido de la clave KeNB*.

En la etapa S1175, el nodo eNB envía un mensaje de demanda de configuración de E-RAB al nodo LTE-Hi, en donde el mensaje contiene una lista de E-RAB a establecerse y el C-RNTI del equipo UE. Se supone que ha de establecerse E-RAB=2.

En la etapa S1180, el nodo LTE-Hi envía el mensaje de reconfiguración de conexión de RRC al equipo UE, en donde el mensaje contiene E-RAB=2 y RB=3.

En la etapa S1185, el equipo UE reenvía el mensaje de terminación de reconfiguración de conexión de RRC al nodo LTE-Hi.

En la etapa S1190, el nodo LTE-Hi reenvía un mensaje de respuesta de configuración de E-RAB al nodo eNB, en donde el mensaje contiene una lista de configuración de E-RAB que incluye RB=3.

En la etapa S1195, el nodo eNB envía el mensaje de reconfiguración de conexión de RRC al equipo UE, demandando al UE que libere RB=2.

En la etapa S1198, el equipo UE reenvía el mensaje de terminación de reconfiguración de conexión de RRC al nodo eNB.

De este modo, los tres canales de datos E-RAB=0, E-RAB=1 y E-RAB=2 se configuran entre el equipo UE y la pasarela MME/SGW/PGW a la configuración de una bifurcación de Hi por el nodo eNB. E-RAB=0 y E-RAB=1 son los mismos que los E-RAB=0 y E-RAB=1 iniciales. E-RAB=2 después de la reconfiguración incluye RB=3 entre el equipo UE y el nodo LTE-Hi, un soporte S1' entre el nodo LTE-Hi y el nodo eNB y el soporte S1 entre el nodo eNB y la pasarela MME/SGW/PGW.

Aunque los números aleatorios nonce3 y nonce4 se envían utilizando el mensaje de orden del modo de seguridad y el mensaje de terminación de configuración de conexión de RRC, respectivamente en el tercer ejemplo, los números aleatorios nonce3 y nonce4 pueden enviarse también a un extremo del mismo nivel utilizando otros mensajes. Además, un método para deducir una clave de protección de integridad y una clave de cifrado de la señalización de RRC y una clave de cifrado de datos del plano del usuario es el mismo que un método para deducir una clave de LTE AS

A continuación se describe otro método 1200 para generar una clave de estrato de acceso en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 12. En el sistema de comunicaciones, un equipo UE accede a una red base por intermedio de una estación base utilizando una primera interfaz de aire y se conecta a la estación base por intermedio de un dispositivo de acceso utilizando una segunda interfaz de aire para acceder a la red base. Por lo tanto, el sistema de comunicaciones al que se aplica el método 1200 es un sistema que soporta la transmisión de descarga de datos y el equipo UE se puede conectar a la estación base usando las dos interfaces de aire al mismo tiempo. Dicho sistema de comunicaciones puede incluir, sin limitación, a: una arquitectura LTE-Hi, una arquitectura LTE-WiFi, una arquitectura WCDMA-WiFi y arquitecturas similares.

Según se ilustra en la Figura 12, el método 1200 incluye:

en la etapa S1210, la adquisición de una clave de estrato de acceso KeNB en la primera interfaz de aire; y

en la etapa S1220, el envío de la clave KeNB al dispositivo de acceso de modo que el dispositivo de acceso genere una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el equipo UE en conformidad con la clave KeNB.

El método 1200 se realiza por la estación base. En conformidad con la técnica anterior, la estación base y el equipo UE memorizan la clave KeNB en la primera interfaz de aire. En esta forma de realización de la presente invención, la clave KeNB se utiliza directamente como la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire. De este modo, después de recibir la clave KeNB desde la estación base, el dispositivo de acceso, junto con el equipo UE, pueden utilizar la clave KeNB como clave raíz de estrato de acceso en la segunda interfaz de aire y deducir la clave de estrato de acceso en la segunda interfaz de aire utilizando la clave KeNB, con lo que se introduce la clave

de estrato de acceso utilizada para una transmisión segura por intermedio de la segunda interfaz de aire.

Durante la deducción de la clave de estrato de acceso, el dispositivo de acceso y el equipo UE pueden utilizar un algoritmo de deducción preestablecido, el dispositivo de acceso selecciona un algoritmo de deducción y luego, lo envía al equipo UE, o el dispositivo de acceso y el equipo UE negocian operativamente el algoritmo de deducción. El dispositivo de acceso y el equipo UE pueden generar la misma clave de estrato de acceso cuando tienen el mismo algoritmo de deducción y la misma clave raíz, con lo que se ayuda a poner una transmisión de datos segura.

En conformidad con el método para generar una clave de estrato de acceso en esta forma de realización de la presente invención, el dispositivo de acceso y el equipo UE utilizan la clave KeNB como la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire y pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire conjuntamente. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario. Además, utilizando directamente las características de las claves KeNB y KeNB* se consigue una puesta en práctica simple y una baja complejidad.

La Figura 12 describe el método 1200 para generar una clave de estrato de acceso en un lado de la estación base. A continuación se describe un método 1300 para generar una clave de estrato de acceso en un lado del dispositivo de acceso en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 13 y un método 1400 para generar una clave de estrato de acceso en un lado del equipo UE en conformidad con una forma de realización de la presente invención haciendo referencia a la Figura 14. Tanto el método 1300 como el método 1400 corresponden al método 1200. Por lo tanto, para las descripciones específicas del método 1300 y del método 1400 puede hacerse referencia a las partes correspondientes del método 1200 y por ello sus detalles no se describen aquí de nuevo para evitar una repetición. Tanto el método 1300 como el método 1400 se aplican al sistema de comunicaciones siguiente: un equipo UE accede a una red base por intermedio de una estación base utilizando una primera interfaz de aire y se conecta a la estación base por intermedio de un dispositivo de acceso utilizando una segunda interfaz de aire para acceder a la red base.

Según se ilustra en la Figura 13, el método 1300 incluye:

en la etapa S1310, la recepción de una clave raíz de estrato de acceso KeNB en la primera interfaz de aire procedente de la estación base; y

en la etapa S1320, la generación de una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el equipo UE en conformidad con la clave KeNB.

El método 1300 se realiza por el dispositivo de acceso. Adquiriendo la clave KeNB desde la estación base, el dispositivo de acceso, junto con el equipo UE, pueden utilizar la clave KeNB como una clave raíz de estrato de acceso en la segunda interfaz de aire y deducir, en conformidad con la clave KeNB, la misma clave de estrato de acceso utilizada en la segunda interfaz de aire. De este modo se introduce una clave utilizada para una transmisión segura por intermedio de la segunda interfaz de aire y se resuelve un problema en la técnica anterior en donde no podría garantizarse la seguridad de la transmisión por intermedio de la segunda interfaz de aire.

En conformidad con el método para generar una clave de estrato de acceso en esta forma de realización de la presente invención, el dispositivo de acceso y el equipo UE utilizan la clave KeNB como la clave raíz de estrato de acceso en la segunda interfaz de aire y pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire de forma conjunta. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario. Además, utilizando directamente la clave KeNB como la clave KeNB* se puede realizar una puesta en práctica simple y con baja complejidad.

Según se ilustra en la Figura 14, el método 1400 incluye:

en la etapa S1410, la adquisición de una clave raíz de estrato de acceso KeNB en la primera interfaz de aire; y

en la etapa S1420, la generación de una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB, en donde la clave de estrato de acceso en la segunda interfaz de aire se genera también por el dispositivo de acceso en conformidad con la clave KeNB recibida desde la estación base.

El método 1400 se realiza por el equipo de usuario. El equipo de usuario y el dispositivo de acceso utilizan la clave KeNB como una clave raíz de estrato de acceso en la segunda interfaz de aire y pueden deducir la misma clave de estrato de acceso en la segunda interfaz de aire de forma conjunta. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la

seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario. Además, utilizando directamente la clave KeNB como la clave KeNB* se puede realizar una puesta en práctica simple y con baja complejidad.

A continuación se describe una puesta en práctica específica del método 1200 al método 1400 con referencia a una realización específica a modo de ejemplo. Un cuarto ejemplo se utiliza simplemente para ayudar a entender las soluciones técnicas dadas a conocer por la presente invención y no plantea ninguna limitación sobre el alcance de protección de la presente invención. El cuarto ejemplo se pone en práctica también en la arquitectura de LTE-Hi ilustrada en la Figura 4 y el punto de acceso LTE-Hi AP 1 también se denomina como un nodo LTE-Hi.

Cuarta realización a modo de ejemplo

En este ejemplo, una clave raíz de estrato de acceso KeNB* en una interfaz de aire Uu' es la misma que una clave raíz de estrato de acceso KeNB en una interfaz de aire Uu. De este modo, un nodo eNB envía un contexto de UE que incluye la clave KeNB al nodo LTE-Hi, de modo que el nodo LTE-Hi adquiera la clave KeNB y determine además, la clave KeNB*.

El nodo LTE-Hi y el equipo UE negocian operativamente un algoritmo en conformidad con la clave KeNB y generar una clave de estrato de acceso utilizada en la interfaz de aire Uu'. El algoritmo negociado por el nodo LTE-Hi y el equipo UE puede ser un algoritmo preestablecido en el nodo LTE-Hi y el equipo UE, un algoritmo utilizado en la interfaz de aire Uu, o un algoritmo que el nodo LTE-Hi selecciona y luego, envía al equipo UE. Utilizando directamente la clave KeNB como la KeNB*, el nodo LTE-Hi y el equipo UE pueden deducir una clave de cifrado y una clave de protección de integridad utilizadas en la interfaz de aire Uu', con lo que se realiza una transmisión de datos segura.

Lo que antecede describe los métodos para generar una clave de estrato de acceso en un sistema de comunicaciones en conformidad con las formas de realización de la presente invención. A continuación se describen diagramas de bloques estructuras de dispositivos correspondientes en conformidad con las formas de realización de la presente invención haciendo referencia a la Figura 15 a la Figura 18. Puesto que los dispositivos ilustrados en la Figura 15 a la Figura 18 están configurados para poner en práctica los métodos para generar una clave de estrato de acceso en conformidad con las formas de realización de la presente invención, para operaciones específicas y detalles de los dispositivos puede hacerse referencia a las descripciones contenidas en los métodos anteriores.

Las Figuras 15 y 15a son diagramas estructurales de un dispositivo del lado de la red en un sistema de comunicaciones en conformidad con formas de realización de la presente invención. En el sistema de comunicaciones un equipo de usuario UE accede a una red base por intermedio de un primer dispositivo del lado de la red utilizando una primera interfaz de aire y se conecta al primer dispositivo del lado de la red por intermedio de un segundo dispositivo del lado de la red utilizando una segunda interfaz de aire para acceder a la red base. El dispositivo del lado de la red puede ser el primer dispositivo del lado de la red, a modo de ejemplo, una estación base. El dispositivo del lado de la red puede ser también el segundo dispositivo del lado de la red, a modo de ejemplo, un dispositivo de acceso.

Cuando el dispositivo del lado de la red es el segundo dispositivo del lado de la red, el dispositivo del lado de la red incluye un módulo de adquisición 1510, un módulo de cálculo 1520 y un módulo de generación 1530. El módulo de adquisición 1510 puede ponerse en práctica utilizando una interfaz de entrada y/o un procesador. El módulo de cálculo 1520 y el módulo de generación 1530 pueden ponerse en práctica utilizando el procesador. El módulo de adquisición 1510 está configurado para adquirir un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del segundo dispositivo del lado de la red. El módulo de cálculo 1520 está configurado para calcular una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada adquirido por el módulo de adquisición 1510 y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, o utilizar la clave KeNB como la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire. El módulo de generación 1530 está configurado para generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB* calculada por el módulo de cálculo 1520.

Para las operaciones anteriores y otras operaciones y/o funciones del módulo de adquisición 1510, el módulo de cálculo 1520 y el módulo de generación 1530, puede hacerse referencia a las descripciones correspondientes en los métodos 200, 900 y 1300 y en los primero a cuarto ejemplos, y por ello los detalles no se describen aquí de nuevo para evitar una repetición.

Según se ilustra en la Figura 15a, cuando el dispositivo del lado de la red es el primer dispositivo del lado de la red, el dispositivo del lado de la red incluye el módulo de adquisición 1510, el módulo de cálculo 1520 y un módulo de envío 1530'. El módulo de adquisición 1510 puede ponerse en práctica utilizando la interfaz de entrada y/o el procesador. El módulo de cálculo 1520 puede ponerse en práctica utilizando el procesador. El módulo de envío 1530' puede ponerse en práctica utilizando una interfaz de salida.

Cuando el dispositivo del lado de la red es el primer dispositivo del lado de la red, el módulo de adquisición 1510 está configurado para adquirir el parámetro de entrada, en donde el parámetro de entrada incluye el parámetro variable en el tiempo y/o el parámetro relacionado con la célula de servicio del segundo dispositivo del lado de la red. El módulo de cálculo 1520 está configurado para calcular la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y la clave raíz de estrato de acceso KeNB en la primera interfaz de aire, o utilizar la clave KeNB como la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire. El módulo de envío 1530' está configurado para enviar el KeNB* calculada por el módulo de cálculo 1520 al segundo dispositivo del lado de la red, de modo que el segundo dispositivo del lado de la red genere la clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*.

Para las operaciones anteriores y otras operaciones y/o funciones del módulo de adquisición 1510, el módulo de cálculo 1520 y el módulo de envío 1530', puede hacerse referencia a las descripciones correspondientes en los métodos 100, 800 y 1200 y en los primero a cuarto ejemplos, y por ello los detalles no se describen aquí de nuevo para evitar una repetición.

En conformidad con el dispositivo del lado de la red en el sistema de comunicaciones en las formas de realización de la presente invención, el dispositivo de acceso y el equipo UE pueden deducir, además, la clave de estrato de acceso en la segunda interfaz de aire adquiriendo la misma clave raíz KeNB* con lo que se introduce la clave de estrato de acceso en la segunda interfaz de aire para ayudar a realizar una transmisión segura. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, puede mejorarse la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

La Figura 16 y la Figura 16a son diagramas de bloques estructurales de un dispositivo del lado de la red en un sistema de comunicaciones en conformidad con las formas de realización de la presente invención. En el sistema de comunicaciones, un equipo de usuario UE accede a una red base por intermedio de un primer dispositivo del lado de la red utilizando una primera interfaz de aire y se conecta al primer dispositivo del lado de la red por intermedio de un segundo dispositivo del lado de la red utilizando una segunda interfaz de aire para acceder a la red base. Un módulo de adquisición 1610, un módulo de cálculo 1620 y un módulo de generación 1630 o un módulo de envío 1630' del dispositivo del lado de la red son básicamente los mismos que un módulo de adquisición 1510, un módulo de cálculo 1520 y un módulo de generación 1530 o un módulo de envío 1530' de un dispositivo del lado de la red. Según se indicó con anterioridad, el dispositivo del lado de la red incluye el módulo de generación 1630 o el módulo de envío 1630'. Cuando el dispositivo del lado de la red es el segundo dispositivo del lado de la red, el dispositivo del lado de la red incluye el módulo de generación 1630. Cuando el dispositivo del lado de la red es el primer dispositivo del lado de la red, el dispositivo del lado de la red incluye el módulo de envío 1630'.

En conformidad con una forma de realización de la presente invención, si el dispositivo del lado de la red es el segundo dispositivo del lado de la red, el dispositivo del lado de la red incluye, además, un módulo de recepción 1640 que está configurado para recibir una clave KeNB procedente del primer dispositivo del lado de la red.

En conformidad con una forma de realización de la presente invención, un parámetro variable en el tiempo adquirido por el módulo de adquisición 1610 puede incluir un valor de PDCP COUNT de un soporte del equipo UE en la primera interfaz de aire. A modo de ejemplo, el valor de PDCP COUNT adquirido por el módulo de adquisición 1610 puede corresponder a un mensaje de configuración, en donde el mensaje de configuración es un mensaje de configuración utilizado para configurar la segunda interfaz de aire para el dispositivo del lado de la red. De este modo, cuando el dispositivo del lado de la red es una estación base, la estación base y el equipo UE pueden adquirir adecuadamente el parámetro variable en el tiempo especificando el valor de PDCP COUNT de un soporte en la estación base y el equipo UE en lugar de intercambian un mensaje, lo que puede economizar recursos de la red.

En conformidad con una forma de realización de la presente invención, el parámetro variable en el tiempo adquirido por el módulo de adquisición 1610 puede incluir un número aleatorio generado por el dispositivo del lado de la red y/o un número aleatorio generado por el equipo UE. En este caso, el módulo de adquisición 1610 está concretamente configurado para adquirir el número aleatorio generado por el dispositivo del lado de la red y/o el número aleatorio generado por el equipo UE. El dispositivo del lado de la red necesita incluir, además, un módulo de transmisión 1650 que está configurado para enviar el número aleatorio generado por el dispositivo del lado de la red al equipo UE o para recibir el número aleatorio generado por el equipo UE procedente de dicho equipo UE.

En conformidad con una forma de realización de la presente invención, el módulo de transmisión 1650 puede específicamente configurarse para enviar el mensaje de configuración utilizado para configurar la segunda interfaz de aire al equipo UE, en donde el mensaje de configuración contiene el número aleatorio generado por el dispositivo del lado de la red. De este modo, la inclusión del número aleatorio en el mensaje de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a una secuencia de envío de mensajes existente.

En conformidad con una forma de realización de la presente invención, el módulo de adquisición 1610 puede configurarse concretamente para recibir un mensaje de terminación de configuración utilizado para indicar que un

enlace de radio está correctamente configurado en la segunda interfaz de aire desde el equipo UE, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo UE. En otra forma de realización, el módulo de adquisición 1610 puede configurarse para recibir un mensaje de terminación de configuración en respuesta al mensaje de configuración utilizado para configurar la segunda interfaz de aire desde el equipo UE, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo UE. De este modo, la inclusión del número aleatorio en el mensaje de terminación del establecimiento o en el mensaje de terminación de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a la secuencia de envío de mensajes existente.

En un caso en que el parámetro variable en el tiempo incluye, a la vez, un primer número aleatorio generado por el dispositivo del lado de la red y un segundo número aleatorio generado por el equipo UE, cuando el dispositivo del lado de la red es la estación base, para permitir que la estación base y el equipo UE tengan el mismo parámetro de entrada para generar la misma clave KeNB*, la estación base necesita enviar el primer número aleatorio al equipo UE, a modo de ejemplo, utilizando el mensaje de configuración utilizado para configurar la segunda interfaz de aire, y el equipo UE necesita enviar el segundo número aleatorio a la estación base, a modo de ejemplo, utilizando el mensaje de terminación de configuración en respuesta al mensaje de configuración. La generación de la clave KeNB* utilizando los números aleatorios generados, por separado, por la estación base y el equipo UE tiene más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por la estación base o el equipo UE. Cuando el dispositivo del lado de la red es un dispositivo de acceso, para permitir al dispositivo de acceso y al equipo UE tener el mismo parámetro de entrada para generar la misma clave KeNB*, el dispositivo de acceso necesita enviar el primer número aleatorio al equipo UE, a modo de ejemplo, utilizando un mensaje de orden del modo de seguridad y el equipo UE necesita enviar el segundo número aleatorio al dispositivo de acceso, a modo de ejemplo, utilizando el mensaje de terminación de establecimiento para indicar que el enlace de radio está correctamente establecido en la segunda interfaz de aire. La generación de la clave KeNB* utilizando los números aleatorios generados, por separado, por el dispositivo de acceso y el equipo UE tiene más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por el dispositivo de acceso o el equipo UE.

En conformidad con una forma de realización de la presente invención, el parámetro relacionado con la célula de servicio del segundo dispositivo del lado de la red puede incluir al menos uno de los elementos siguientes: un identificador de célula de la célula de servicio del segundo dispositivo del lado de la red y una frecuencia central de la célula de servicio del segundo dispositivo del lado de la red. El uso de parámetros pertinentes de diferentes células ayuda a garantizar que la clave KeNB* deducida es distinta para diferentes células.

Para las operaciones anteriores y otras operaciones y/o funciones del módulo de recepción 1640 y el módulo de transmisión 1650, puede hacerse referencia a las descripciones correspondientes en los métodos 100, 200, 800, 900, 1200 y 1300 y en los primero a cuarto ejemplos, y por ello los detalles no se describen aquí de nuevo para evitar una repetición.

En conformidad con el dispositivo del lado de la red en el sistema de comunicaciones en las formas de realización de la presente invención, una clave utilizada para la transmisión segura puede introducirse para la segunda interfaz de aire utilizando la misma clave KeNB* para deducir una clave raíz de estrato de acceso en la segunda interfaz de aire. Por lo tanto, cuando se utiliza la clave de estrato de acceso para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

La Figura 17 es un diagrama de bloques estructural de un equipo de usuario en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención. En el sistema de comunicaciones, el equipo de usuario accede a una red base por intermedio de un primer dispositivo del lado de la red utilizando una primera interfaz de aire y se conecta al primer dispositivo del lado de la red por intermedio de un segundo dispositivo del lado de la red utilizando una segunda interfaz de aire para acceder a la red base.

El equipo de usuario incluye un módulo de adquisición 1710, un módulo de cálculo 1720 y un módulo de generación 1730. El módulo de adquisición 1710 puede ponerse en práctica utilizando un procesador y/o una interfaz de entrada. El módulo de cálculo 1720 y el módulo de generación 1730 pueden ponerse en práctica utilizando el procesador. El módulo de adquisición 1710 está configurado para adquirir un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo y/o un parámetro relacionado con una célula de servicio del segundo dispositivo del lado de la red. El módulo de cálculo 1720 está configurado para calcular una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada adquirido por el módulo de adquisición 1710 y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, o utilizar la clave KeNB como la clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire. El módulo de generación 1730 está configurado para generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB* calculada por el módulo de cálculo 1720.

Para las operaciones anteriores y otras operaciones y/o funciones del módulo de adquisición 1710, el módulo de cálculo 1720 y el módulo de generación 1730, puede hacerse referencia a las descripciones correspondientes en los métodos 300, 1000 y 1400 y en los primero a cuarto ejemplos, y por ello los detalles no se describen aquí de nuevo para evitar una repetición.

En conformidad con el equipo de usuario en el sistema de comunicaciones en esta forma de realización de la presente invención, el equipo de usuario y un dispositivo de acceso pueden adquirir la clave raíz KeNB* basada en la clave KeNB, con lo que se deduce la misma clave de estrato de acceso en la segunda interfaz de aire sobre la base de la clave KeNB*. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, puede mejorarse la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario.

La Figura 18 es un diagrama de bloques estructural de un equipo de usuario en un sistema de comunicaciones en conformidad con una forma de realización de la presente invención. En el sistema de comunicaciones, el equipo de usuario accede a una red base por intermedio de un primer dispositivo del lado de la red utilizando una primera interfaz de aire y se conecta al primer dispositivo del lado de la red por intermedio de un segundo dispositivo del lado de la red utilizando una segunda interfaz de aire para acceder a la red base. Un módulo de adquisición 1810, un módulo de cálculo 1820 y un módulo de generación 1830 del equipo de usuario son básicamente los mismos que el módulo de adquisición 1710, un módulo de cálculo 1720 y un módulo de generación 1730 de un equipo de usuario.

En conformidad con una forma de realización de la presente invención, un parámetro variable en el tiempo adquirido por el módulo de adquisición 1810 puede incluir un número aleatorio generado por un dispositivo del lado de la red y/o un número aleatorio generado por el equipo UE. En este caso, el módulo de adquisición 1810 está concretamente configurado para adquirir el número aleatorio generado por el dispositivo del lado de la red y/o el número aleatorio generado por el equipo UE. El equipo de usuario incluye, además, un módulo de transmisión 1840. El módulo de transmisión 1840 está configurado para enviar el número aleatorio que se genera por el equipo UE y se adquiere por el módulo de adquisición 1810 al dispositivo del lado de la red o para recibir el número aleatorio generado por el dispositivo del lado de la red. A modo de ejemplo, el módulo de adquisición 1810 puede estar específicamente configurado para recibir un mensaje de orden del modo de seguridad desde el dispositivo de acceso, en donde el mensaje de orden del modo de seguridad contiene el número aleatorio generado por el dispositivo de acceso. De este modo, la inclusión del número aleatorio en el mensaje de orden del modo de seguridad puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a una secuencia de envío de mensajes existente. A modo de otro ejemplo, el módulo de transmisión 1840 puede estar específicamente configurado para enviar un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está correctamente configurado en la segunda interfaz de aire al dispositivo de acceso, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo UE. De este modo, la inclusión del número aleatorio en el mensaje de terminación de configuración puede impedir un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y garantizar que la transmisión del número aleatorio no afecte a la secuencia de envío de mensajes existente. A modo de ejemplo, el módulo de transmisión 1840 puede estar específicamente configurado para recibir un mensaje de configuración que se envía por el dispositivo del lado de la red al equipo UE y utilizado para configurar la segunda interfaz de aire, en donde el mensaje de configuración contiene el número aleatorio generado por el dispositivo del lado de la red. Lo que antecede puede impedir también un aumento en la carga de la red debido al uso de un nuevo mensaje para transmitir el número aleatorio y que no afecte a la secuencia de envío de mensajes existente.

En un caso en que el parámetro variable en el tiempo incluye, a la vez un primer número aleatorio generado por el dispositivo del lado de la red y un segundo número aleatorio generado por el equipo de usuario, cuando el dispositivo del lado de la red es el dispositivo de acceso, para permitir al dispositivo de acceso y al equipo de usuario tener el mismo parámetro de entrada para generar la misma clave KeNB*, el dispositivo de acceso necesita enviar el primer número aleatorio al equipo UE, a modo de ejemplo, utilizando el mensaje de orden del modo de seguridad y el equipo de usuario necesita enviar el segundo número aleatorio al dispositivo de acceso, a modo de ejemplo, utilizando el mensaje de terminación de configuración utilizado para indicar que el enlace de radio está correctamente configurado en la segunda interfaz de aire. La generación de la clave KeNB* utilizando los números aleatorios generados, por separado, por el dispositivo de acceso y el equipo de usuario tiene más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por el dispositivo de acceso o el equipo de usuario. Cuando el dispositivo del lado de la red es una estación base, para permitir que la estación base el equipo de usuario tengan el mismo parámetro de entrada para generar la misma clave KeNB*, la estación base necesita enviar el primer número aleatorio al equipo de usuario, a modo de ejemplo, utilizando el mensaje de configuración usado para configurar la segunda interfaz de aire, y el equipo de usuario necesita enviar el segundo número aleatorio a la estación base, a modo de ejemplo, utilizando un mensaje de terminación de configuración en respuesta al mensaje de configuración. La generación de la clave KeNB* utilizando los números aleatorios generados por separado, por la estación base y el equipo de usuario tiene más alta seguridad que la generación de la clave KeNB* utilizando solamente el número aleatorio generado por la estación base o el equipo de usuario.

En conformidad con una forma de realización de la presente invención, un parámetro relacionado con una célula de servicio del segundo dispositivo del lado de la red puede incluir al menos uno de los elementos siguientes: un identificador de célula de la célula de servicio del segundo dispositivo del lado de la red y una frecuencia central de la célula de servicio del segundo dispositivo del lado de la red. El uso de parámetros pertinentes de diferentes células ayuda a garantizar que la clave KeNB* deducida es distinta para células diferentes.

Para las operaciones anteriores y otras operaciones y/o funciones del módulo de adquisición 1810 y el módulo de transmisión 1840, puede hacerse referencia a las descripciones correspondientes en los métodos 300, 1000 y 1400 y en los primero a cuarto ejemplos, y por ello los detalles no se describen aquí de nuevo para evitar una repetición.

En conformidad con el equipo de usuario en el sistema de comunicaciones en las formas de realización de la presente invención, el equipo de usuario y el dispositivo de acceso pueden utilizar la misma clave raíz de estrato de acceso KeNB* para deducir la misma clave de estrato de acceso en la segunda interfaz de aire. Por lo tanto, cuando la clave de estrato de acceso se utiliza para la transmisión de datos por intermedio de la segunda interfaz de aire, se puede mejorar la seguridad de la transmisión de datos por intermedio de la segunda interfaz de aire y se garantiza la seguridad de los datos transmitidos entre el dispositivo de acceso y el equipo de usuario. Además, utilizando solamente una clave KeNB como la clave KeNB* se consigue una puesta en práctica simple y de baja complejidad.

Un experto en esta técnica puede entender que las etapas y unidades del método descrito en las formas de realización dadas a conocer en esta descripción pueden ponerse en práctica mediante equipos físicos electrónicos, programas informáticos o una de sus combinaciones. Para describir con claridad la intercambiabilidad de hardware y software, lo que antecede fue generalmente descrito en etapas y composiciones de cada forma de realización en conformidad con las funciones respectivas. Si las funciones se realizan por hardware o software dependerá de las aplicaciones particulares y de las condiciones de limitaciones del diseño de las soluciones técnicas. Un experto en esta técnica puede utilizar distintos métodos para poner en práctica las funciones descritas para cada aplicación particular, pero no debe considerarse que la puesta en práctica se desvía del alcance de protección de la presente invención.

Las etapas descritas del método en las formas de realización dadas a conocer en esta descripción pueden ponerse en práctica mediante hardware, un programa de aplicación ejecutado por un procesador o una de sus combinaciones. El programa informático puede memorizarse en una memoria de acceso aleatorio (RAM), una memoria de solamente lectura (ROM), una memoria ROM eléctricamente programable, una memoria ROM eléctricamente programable y borrable, un registro, un disco duro, un disco extraíble, una memoria CD-ROM o un soporte de memorización de cualquier otra forma conocida en el campo técnico.

Aunque algunas formas de realización de la presente invención han sido descritas con anterioridad, un experto en esta técnica debe entender que todas las modificaciones realizadas sin desviarse del alcance de la presente invención caerán dentro del alcance de protección de la presente invención.

REIVINDICACIONES

1. Un método para generar una clave de estrato de acceso en un sistema de comunicaciones, en donde un primer dispositivo del lado de la red se conecta a un equipo de usuario, UE, por intermedio de una primera interfaz de aire y que accede a una red base, CN, y el primer dispositivo del lado de la red se conecta a un segundo dispositivo del lado de la red, en donde el segundo dispositivo del lado de la red es un dispositivo que se conecta al equipo de usuario UE por intermedio de una segunda interfaz de aire y el método comprende:

adquirir (S110), por el primer dispositivo del lado de la red, un parámetro de entrada, en donde el parámetro de entrada comprende un parámetro variable en el tiempo;

calcular (S120), por el primer dispositivo del lado de la red, una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la segunda interfaz de aire está situada entre el segundo dispositivo del lado de la red y el equipo de usuario UE; y

enviar (S130), por el primer dispositivo del lado de la red, la clave KeNB* al segundo dispositivo del lado de la red.

2. El método según la reivindicación 1, en donde el parámetro variable en el tiempo comprende un valor de contador.

3. El método según la reivindicación 1, en donde el parámetro variable en el tiempo comprende un valor de conteo de Protocolo de Convergencia de Datos por Paquetes, PDCP COUNT, de un soporte del equipo UE en la primera interfaz de aire.

4. El método según la reivindicación 3, en donde el valor de PDCP COUNT corresponde a un mensaje de configuración y el mensaje de configuración es un mensaje de configuración utilizado por el primer dispositivo del lado de la red para configurar la segunda interfaz de aire.

5. El método según la reivindicación 1,

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el primer dispositivo del lado de la red y un número aleatorio generado por el equipo de usuario UE;

la adquisición, por el primer dispositivo del lado de la red, de un parámetro de entrada comprende:

adquirir, por el primer dispositivo del lado de la red, el número aleatorio generado por el primer dispositivo del lado de la red y la recepción desde el equipo UE del número aleatorio generado por el UE; y

después de la adquisición, por el primer dispositivo del lado de la red, de un parámetro de entrada, el método comprende, además:

enviar, por el primer dispositivo del lado de la red, el número aleatorio generado por el primer dispositivo del lado de la red al equipo de usuario UE;

o,

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el primer dispositivo del lado de la red;

la adquisición, por el primer dispositivo del lado de la red, de un parámetro de entrada comprende:

adquirir, por el primer dispositivo del lado de la red, el número aleatorio generado por el primer dispositivo del lado de la red; y

después de la adquisición, por el primer dispositivo del lado de la red, de un parámetro de entrada, el método comprende, además:

enviar, por el primer dispositivo del lado de la red, el número aleatorio generado por el primer dispositivo del lado de la red hacia equipo de usuario UE;

o,

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el equipo de usuario UE;

la adquisición, por el primer dispositivo del lado de la red, de un parámetro de entrada comprende:

recibir, por el primer dispositivo del lado de la red, desde el equipo UE, el número aleatorio generado por el UE.

6. El método según la reivindicación 5, en donde el envío, por el primer dispositivo del lado de la red, del número aleatorio generado por el primer dispositivo del lado de la red hacia el equipo de usuario UE comprende:

enviar, por el primer dispositivo del lado de la red, un mensaje de configuración utilizado para configurar la segunda interfaz de aire hacia el equipo de usuario UE, en donde el mensaje de configuración incluye el número aleatorio generado por el primer dispositivo del lado de la red.

7. El método según la reivindicación 5, en donde la recepción del número aleatorio generado por el equipo de usuario UE desde el equipo UE comprende:

recibir un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está configurado de forma operativamente satisfactoria en la segunda interfaz de aire a partir del equipo UE, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo de usuario UE.

8. Un método para generar una clave de estrato de acceso en un sistema de comunicaciones, en donde un equipo de usuario, UE, en el sistema de comunicaciones accede a una red base por intermedio de un primer dispositivo del lado de la red utilizando una primera interfaz de aire, y se conecta al primer dispositivo del lado de la red por intermedio de un segundo dispositivo del lado de la red utilizando una segunda interfaz de aire para acceder a la red base y el método comprende:

adquirir (S310), por el equipo de usuario UE, un parámetro de entrada en donde el parámetro de entrada comprende un parámetro variable en el tiempo;

calcular (S320), por el equipo de usuario UE, una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la segunda interfaz de aire está situada entre el segundo dispositivo del lado de la red y el equipo de usuario UE; y

generar (S330), por el equipo de usuario UE, una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*.

9. El método según la reivindicación 8, en donde el parámetro variable en el tiempo comprende un valor de contador.

10. El método según la reivindicación 8,

en donde el parámetro variable en el tiempo incluye un número aleatorio generado por el primer dispositivo del lado de la red y un número aleatorio generado por el equipo de usuario UE;

la adquisición, por el equipo UE, de un parámetro de entrada comprende:

recibir, por el equipo de usuario UE, desde el primer dispositivo del lado de la red, el número aleatorio generado por el primer dispositivo del lado de la red y adquirir el número aleatorio generado por el equipo de usuario UE; y

después de la adquisición, por el equipo UE, de un parámetro de entrada, el método comprende, además:

enviar, por el equipo UE, el número aleatorio generado por el equipo UE al primer dispositivo del lado de la red;

o,

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el equipo UE;

la adquisición, por el equipo UE, de un parámetro de entrada comprende:

adquirir, por el equipo UE, el número aleatorio generado por el equipo UE; y

después de la adquisición, por el equipo UE, de un parámetro de entrada, el método comprende, además:

enviar, por el equipo UE, el número aleatorio generado por el equipo UE al primer dispositivo del lado de la red;

o,

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el primer dispositivo del

lado de la red;

la adquisición, por el equipo UE, de un parámetro de entrada comprende:

recibir, por el equipo UE, desde el primer dispositivo del lado de la red, el número aleatorio generado por el primer dispositivo del lado de la red.

11. El método según la reivindicación 10, en donde el envío, por el equipo UE, del número aleatorio generado por el equipo UE al primer dispositivo del lado de la red comprende:

enviar, por el equipo UE, un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está configurado de forma satisfactoria en la segunda interfaz de aire para el segundo dispositivo del lado de la red, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo de usuario UE.

12. El método según la reivindicación 10, en donde la recepción del número aleatorio generado por el primer dispositivo del lado de la red comprende:

recibir un mensaje de configuración que se envía por el primer dispositivo del lado de la red al equipo de usuario UE y se utiliza para configurar la segunda interfaz de aire, en donde el mensaje de configuración contiene el número aleatorio generado por el primer dispositivo del lado de la red.

13. Un dispositivo del lado de la red para un sistema de comunicaciones, en donde el dispositivo del lado de la red se conecta a un equipo de usuario, UE, por intermedio de una primera interfaz de aire y accede a una red base, CN, y el dispositivo del lado de la red se conecta a un segundo dispositivo del lado de la red, en donde el segundo dispositivo del lado de la red es un dispositivo que se conecta al equipo de usuario UE por intermedio de una segunda interfaz de aire, y el método comprende:

un módulo de adquisición (1510), configurado para adquirir un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo;

un módulo de cálculo (1520), configurado para calcular una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada adquirido por el el módulo de adquisición (1510) y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la segunda interfaz de aire está situada entre el segundo dispositivo del lado de la red y el equipo de usuario UE; y

un módulo de envío (1530'), configurado para enviar la clave KeNB* calculada por el módulo de cálculo al según dispositivo del lado de la red.

14. El dispositivo del lado de la red según la reivindicación 13, en donde el parámetro variable en el tiempo adquirido por el módulo de adquisición (1510) comprende un valor de contador.

15. El dispositivo del lado de la red según la reivindicación 13, en donde el parámetro variable en el tiempo adquirido por el módulo de adquisición (1510), comprende un valor de conteo de Protocolo de Convergencia de Datos por Paquetes, PDCP COUNT, de un soporte del equipo de usuario UE en la primera interfaz de aire.

16. El dispositivo del lado de la red según la reivindicación 15, en donde el valor de PDCP COUNT adquirido por el módulo de adquisición (1510) corresponde a un mensaje de configuración y el mensaje de configuración es un mensaje de configuración utilizado para el dispositivo del lado de la red para configurar la segunda interfaz de aire.

17. El dispositivo del lado de la red según la reivindicación 13,

en donde el parámetro variable en el tiempo adquirido por el módulo de adquisición (1510) comprende un número aleatorio generado por el dispositivo del lado de la red y un número aleatorio generado por el equipo de usuario UE;

el módulo de adquisición (1510) está concretamente configurado para adquirir el número aleatorio generado por el dispositivo del lado de la red y para recibir desde el equipo UE el número aleatorio generado por el equipo UE; y

el dispositivo del lado de la red comprende, además:

un módulo de transmisión (1650), configurado para enviar el número aleatorio que se genera por el dispositivo del lado de la red y se adquiere por el módulo de adquisición (1510) hacia el equipo UE; o

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el primer dispositivo del lado de la red;

el módulo de adquisición (1510) está concretamente configurado para adquirir el número aleatorio generado por el primer dispositivo del lado de la red; y

el dispositivo del lado de la red comprende, además:

un módulo de transmisión (1650), configurado para enviar el número aleatorio que se genera por el dispositivo del lado de la red y se adquiere por el módulo de adquisición (1510) hacia el equipo de usuario UE;

o,

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el equipo de usuario UE;

el módulo de adquisición (1510) está concretamente configurado para recibir desde el equipo UE el número aleatorio generado por el equipo UE.

18. El dispositivo del lado de la red según la reivindicación 17, en donde el módulo de transmisión (1650) está concretamente configurado para enviar un mensaje de configuración utilizado para configurar la segunda interfaz de aire hacia el equipo de usuario UE y el mensaje de configuración contiene el número aleatorio generado por el dispositivo del lado de la red; o

el módulo de transmisión (1650) está concretamente configurado para recibir un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está configurado satisfactoriamente en la segunda interfaz de aire procedente del equipo UE, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo de usuario UE.

19. Un equipo de usuario para un sistema de comunicaciones, en donde el equipo de usuario, UE, en el sistema de comunicaciones accede a una red base por intermedio de un primer dispositivo del lado de la red utilizando una primera interfaz de aire, y se conecta al primer dispositivo del lado de la red por intermedio de un segundo dispositivo del lado de la red utilizando una segunda interfaz de aire para acceder a la red base y el equipo de usuario UE comprende:

un módulo de adquisición (1710), configurado para adquirir un parámetro de entrada, en donde el parámetro de entrada incluye un parámetro variable en el tiempo;

un módulo de cálculo (1720), configurado para calcular una clave raíz de estrato de acceso KeNB* en la segunda interfaz de aire en conformidad con el parámetro de entrada adquirido por el módulo de adquisición y una clave raíz de estrato de acceso KeNB en la primera interfaz de aire, en donde la segunda interfaz de aire está situada entre el segundo dispositivo del lado de la red y el equipo de usuario UE; y

un módulo de generación (1730), configurado para generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB* calculada por el módulo de cálculo (1720).

20. El equipo de usuario según la reivindicación 19, en donde el parámetro variable en el tiempo adquirido por el módulo de adquisición (1710) comprende un valor de contador.

21. El equipo de usuario según la reivindicación 19,

en donde el parámetro variable en el tiempo adquirido por el módulo de adquisición (1710) comprende un número aleatorio generado por el primer dispositivo del lado de la red y un número aleatorio generado por el equipo de usuario UE;

el módulo de adquisición (1710) está concretamente configurado para:

recibir desde el primer dispositivo del lado de la red el número aleatorio generado por el primer dispositivo del lado de la red y para adquirir el número aleatorio generado por el equipo de usuario UE; y

el equipo de usuario comprende, además:

un módulo de transmisión (1840), configurado para enviar el número aleatorio que se genera por el equipo UE y se adquiere por el módulo de adquisición (1710) hacia el primer dispositivo del lado de la red;

o,

en donde el parámetro variable en el tiempo adquirido por el módulo de adquisición (1710) comprende un número aleatorio generado por el equipo UE;

el módulo de adquisición (1710) está concretamente configurado para: adquirir el número aleatorio generado por el equipo UE; y

el equipo de usuario comprende, además:

un módulo de transmisión (1840), configurado para enviar el número aleatorio que se genera por el equipo UE y se adquiere por el módulo de adquisición (1710) hacia el primer dispositivo del lado de la red; o

en donde el parámetro variable en el tiempo comprende un número aleatorio generado por el primer dispositivo del lado de la red;

el módulo de adquisición (1710) está concretamente configurado para: recibir desde el primer dispositivo del lado de la red el número aleatorio generado por el primer dispositivo del lado de la red.

22. El equipo de usuario según la reivindicación 21, en donde:

el módulo de transmisión (1840) está concretamente configurado para enviar un mensaje de terminación de configuración utilizado para indicar que un enlace de radio está configurado satisfactoriamente en la segunda interfaz de aire hacia el segundo dispositivo del lado de la red, en donde el mensaje de terminación de configuración contiene el número aleatorio generado por el equipo de usuario UE; o

el módulo de transmisión (1840) está concretamente configurado para recibir un mensaje de configuración que se envía por el primer dispositivo del lado de la red al equipo de usuario UE y utilizado para configurar la segunda interfaz de aire, en donde el mensaje de configuración contiene el número aleatorio generado por el primer dispositivo del lado de la red.

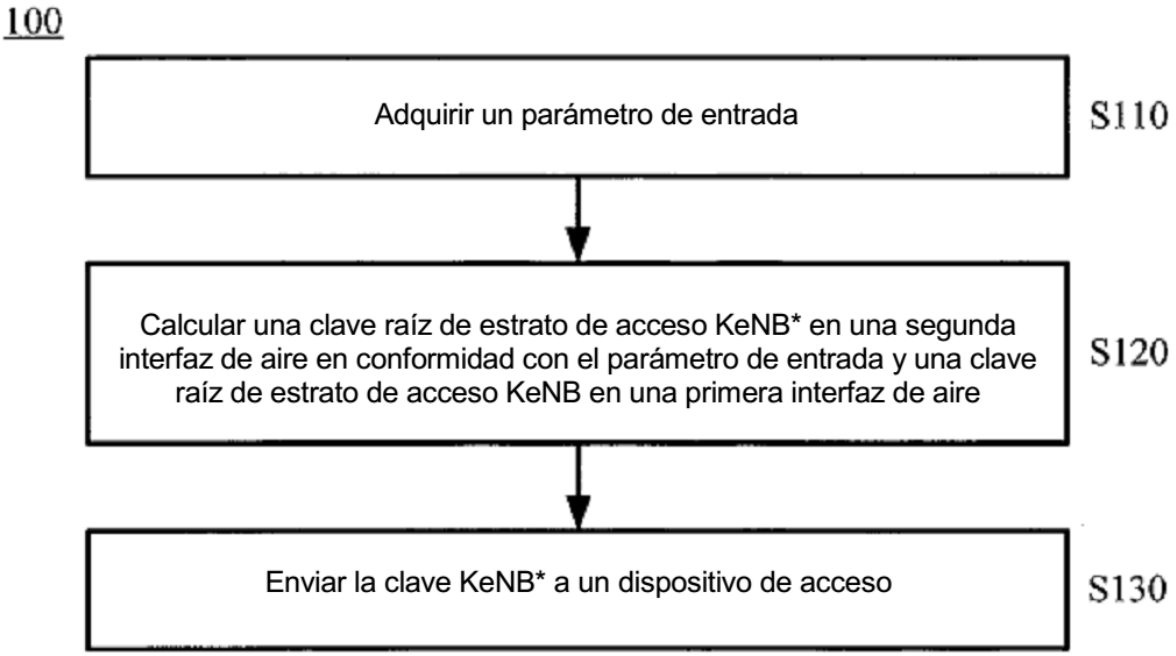
100
Adquirir un parámetro de entrada
S110
Calcular una clave raíz de estrato de acceso KeNB* en una segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en una primera interfaz de aire
S120
Enviar la clave KeNB* a un dispositivo de acceso
S130

FIG. 1

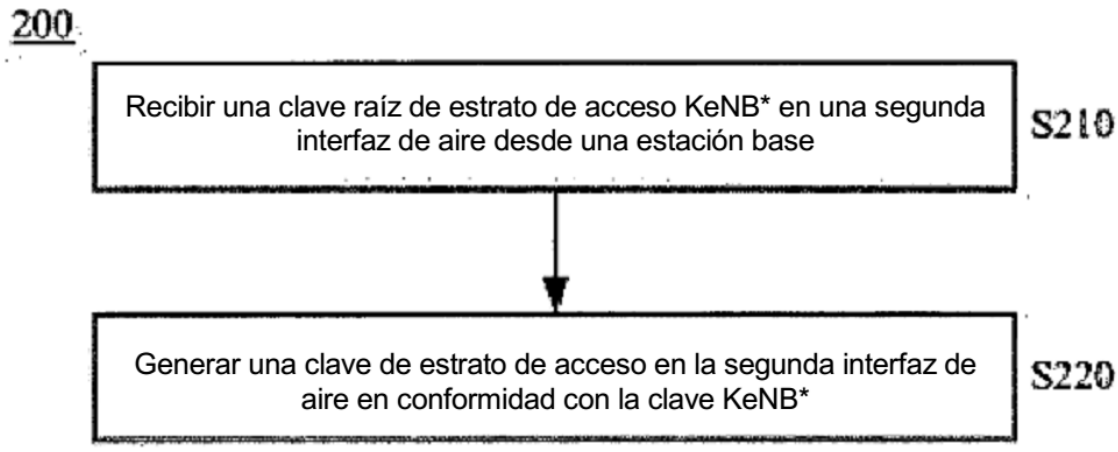
200
Recibir una clave raíz de estrato de acceso KeNB* en una segunda interfaz de aire desde una estación base
S210
Generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*
S220

FIG. 2

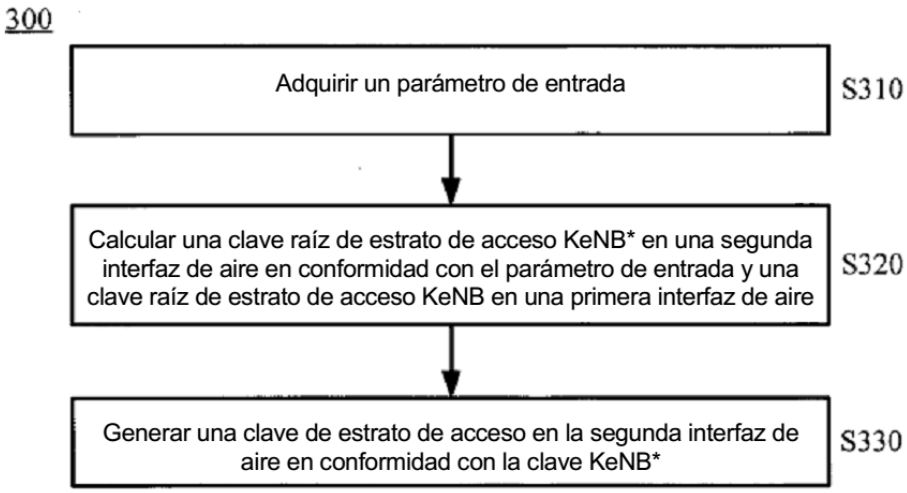
300
Adquirir un parámetro de entrada
S310
Calcular una clave raíz de estrato de acceso KeNB* en una segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en una primera interfaz de aire
S320
Generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*
S330

FIG. 3

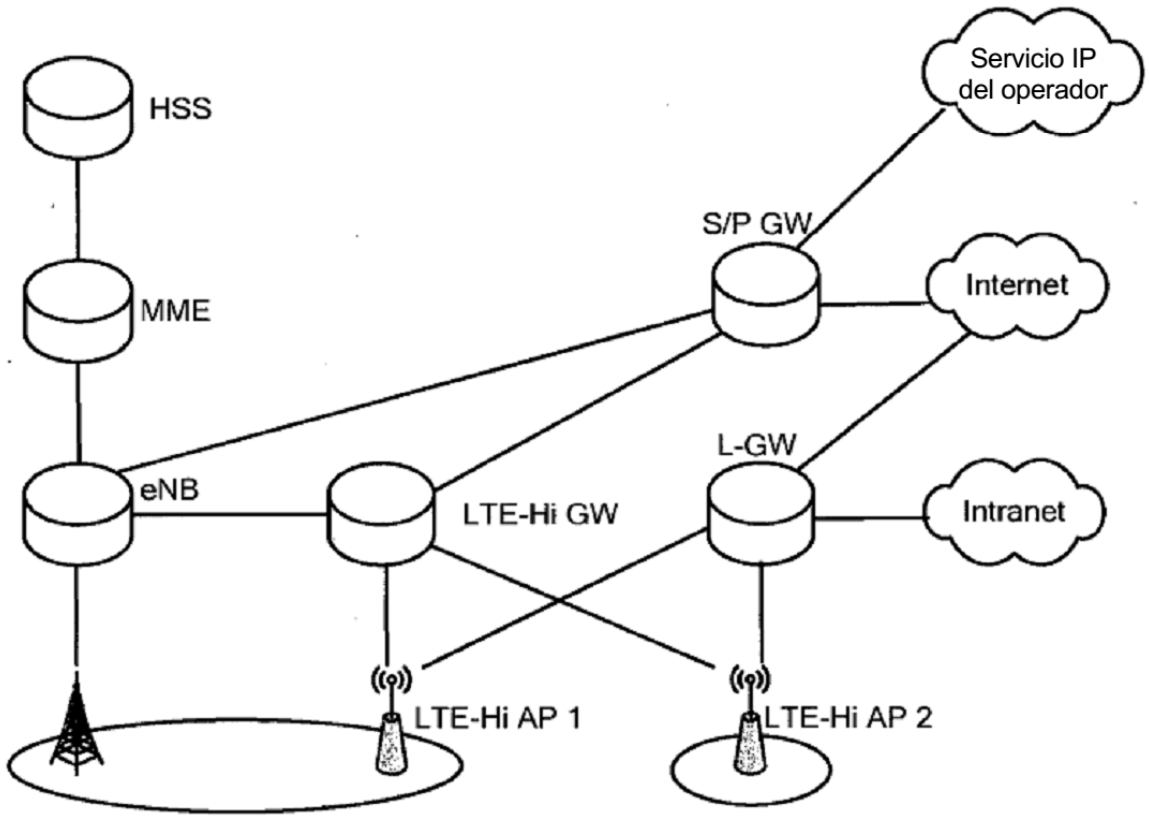
HSS
MME
eNB
LTE-Hi GW
S/P GW
L-GW
Servicio IP del operador
Internet
Intranet
LTE-Hi AP 1
LTE-Hi AP 2

FIG. 4

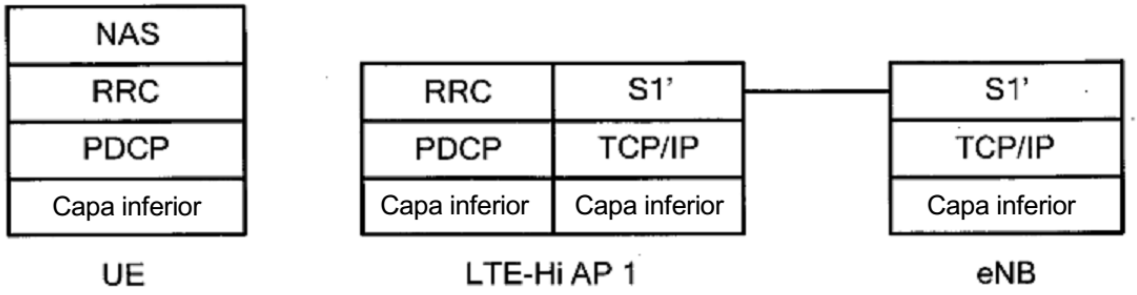
NAS
RRC
PDCP
Capa inferior
UE
RRC
S1'
PDCP
TCP/IP
Capa inferior
Capa inferior
LTE-Hi AP 1
S1'
TCP/IP
Capa inferior
eNB

FIG. 5

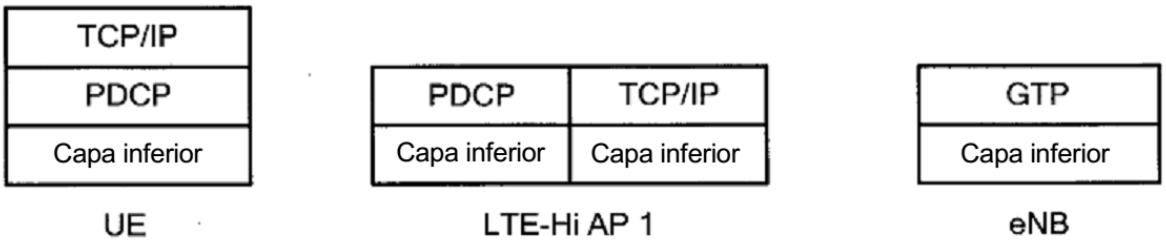
TCP/IP
PDCP
Capa inferior
UE
PDCP
TCP/IP
Capa inferior
Capa inferior
LTE-Hi AP 1
GTP
Capa inferior
eNB

FIG. 6

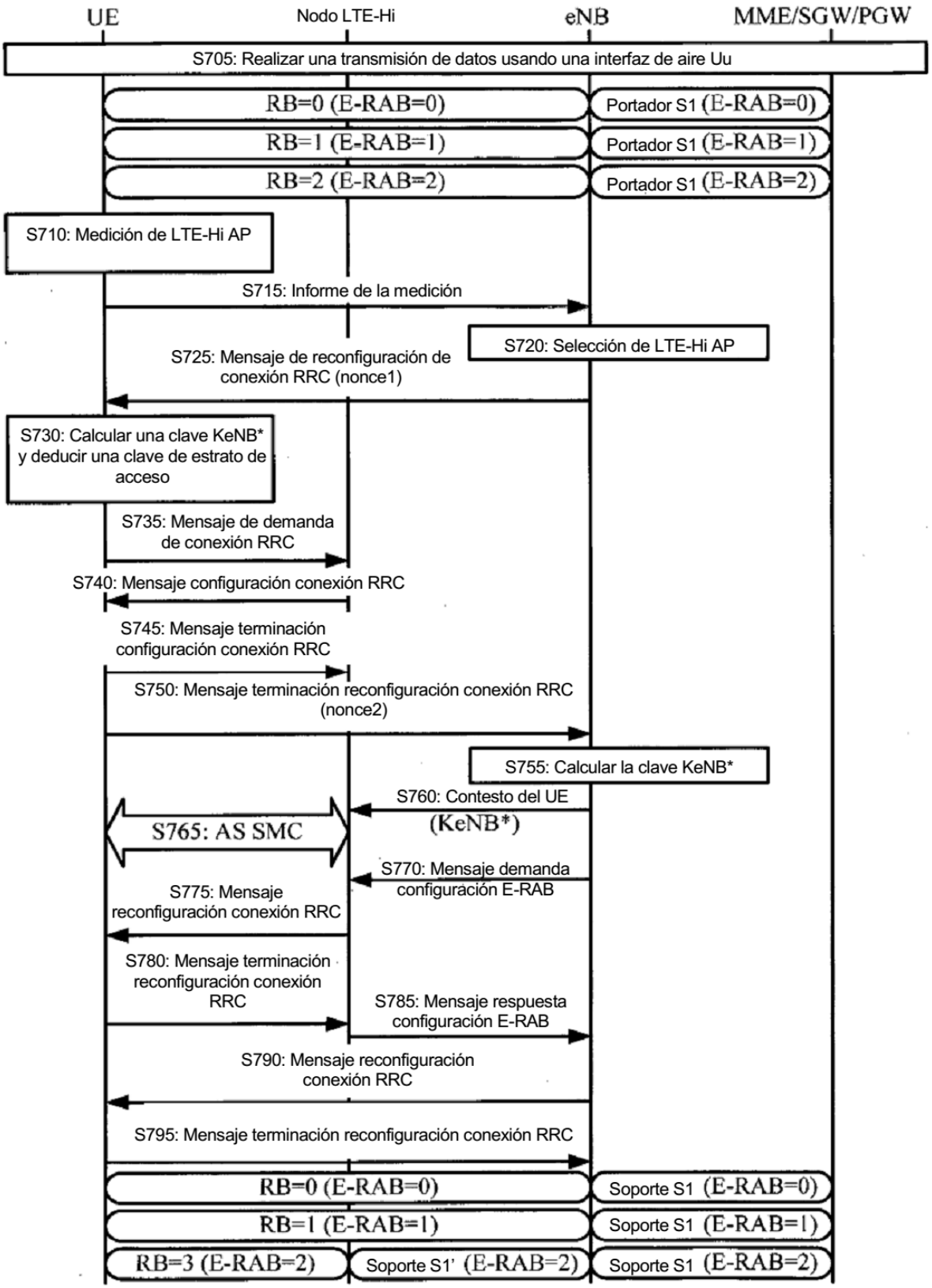
UE
Nodo LTE-Hi
eNB
MME/SGW/PGW
S705: Realizar una transmisión de datos usando una interfaz de aire Uu
RB=0 (E-RAB=0)
Portador S1 (E-RAB=0)
RB=1 (E-RAB=1)
Portador S1 (E-RAB=1)
RB=2 (E-RAB=2)
Portador S1 (E-RAB=2)
S710: Medición de LTE-Hi AP
S715: Informe de la medición
S720: Selección de LTE-Hi AP
S725: Mensaje de reconfiguración de conexión RRC (nonce1)
S730: Calcular una clave KeNB* y deducir una clave de estrato de acceso
S735: Mensaje de demanda de conexión RRC
S740: Mensaje configuración conexión RRC
S745: Mensaje terminación configuración conexión RRC
S750: Mensaje terminación reconfiguración conexión RRC (nonce2)
S755: Calcular la clave KeNB*
S760: Contesto del UE (KeNB*)
S765: AS SMC
S770: Mensaje demanda configuración E-RAB
S775: Mensaje reconfiguración conexión RRC
S780: Mensaje terminación reconfiguración conexión RRC
S785: Mensaje respuesta configuración E-RAB
S790: Mensaje reconfiguración conexión RRC
S795: Mensaje terminación reconfiguración conexión RRC
RB=0 (E-RAB=0)
Soporte S1 (E-RAB=0)
RB=1 (E-RAB=1)
Soporte S1 (E-RAB=1)
RB=3 (E-RAB=2)
Soporte S1' (E-RAB=2)
Soporte S1 (E-RAB=2)

FIG. 7

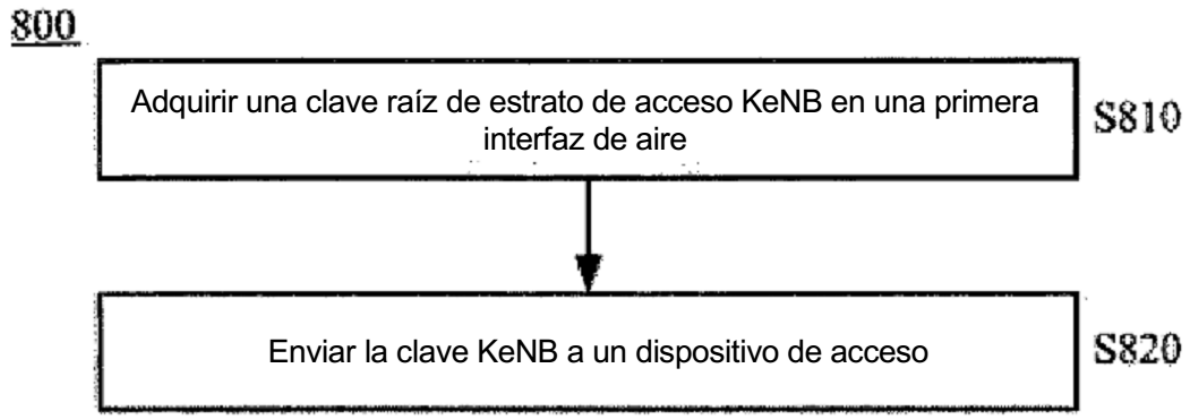
800
Adquirir una clave raíz de estrato de acceso KeNB en una primera interfaz de aire
S810
Enviar la clave KeNB a un dispositivo de acceso
S820

FIG. 8

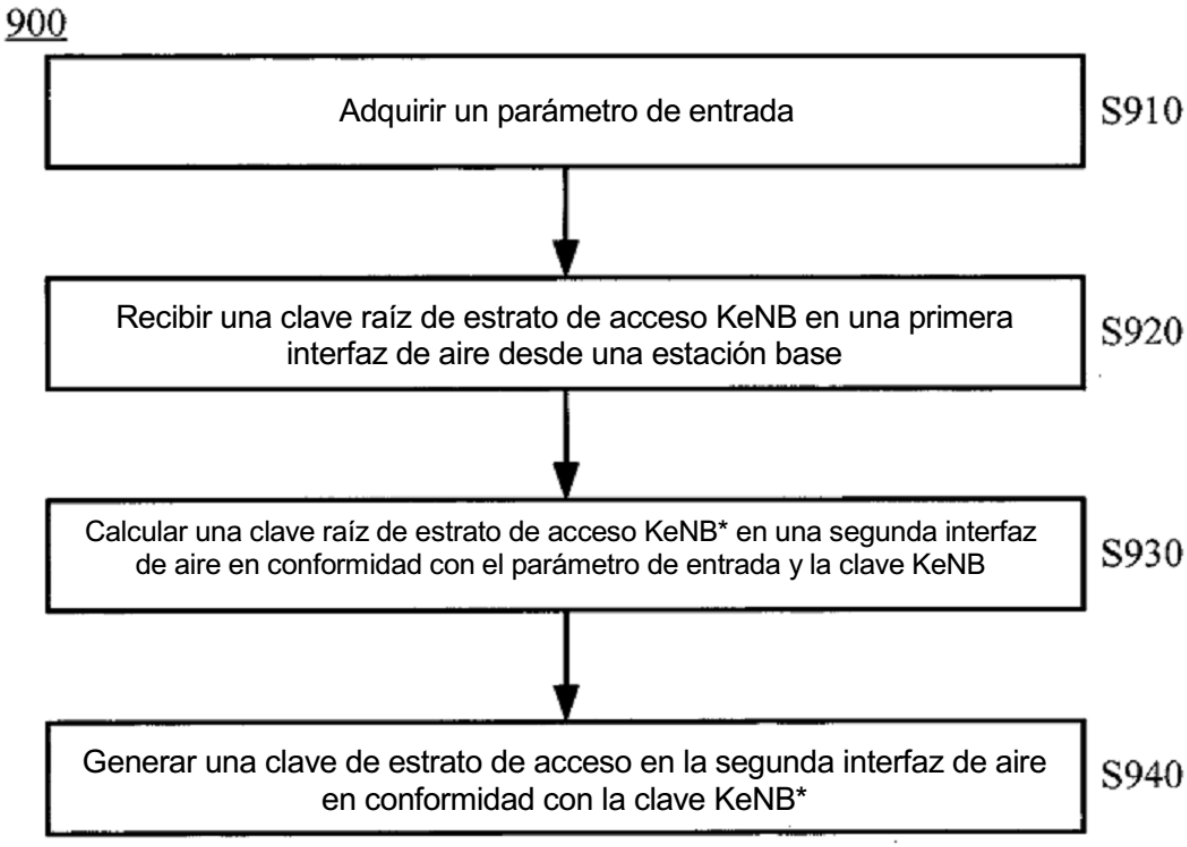
900
Adquirir un parámetro de entrada
S910
Recibir una clave raíz de estrato de acceso KeNB en una primera interfaz de aire desde una estación base
S920
Calcular una clave raíz de estrato de acceso KeNB* en una segunda interfaz de aire en conformidad con el parámetro de entrada y la clave KeNB
S930
Generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*
S940

FIG. 9

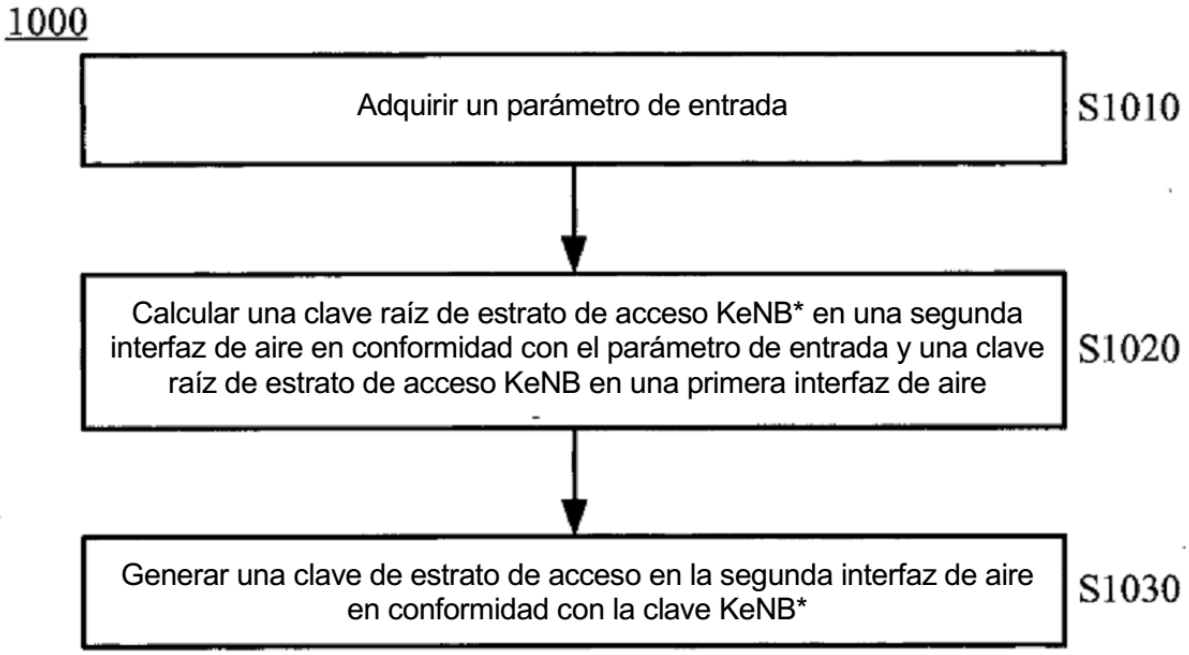
1000
Adquirir un parámetro de entrada
S1010
Calcular una clave raíz de estrato de acceso KeNB* en una segunda interfaz de aire en conformidad con el parámetro de entrada y una clave raíz de estrato de acceso KeNB en una primera interfaz de aire
S1020
Generar una clave de estrato de acceso en la segunda interfaz de aire en conformidad con la clave KeNB*
S1030

FIG. 10

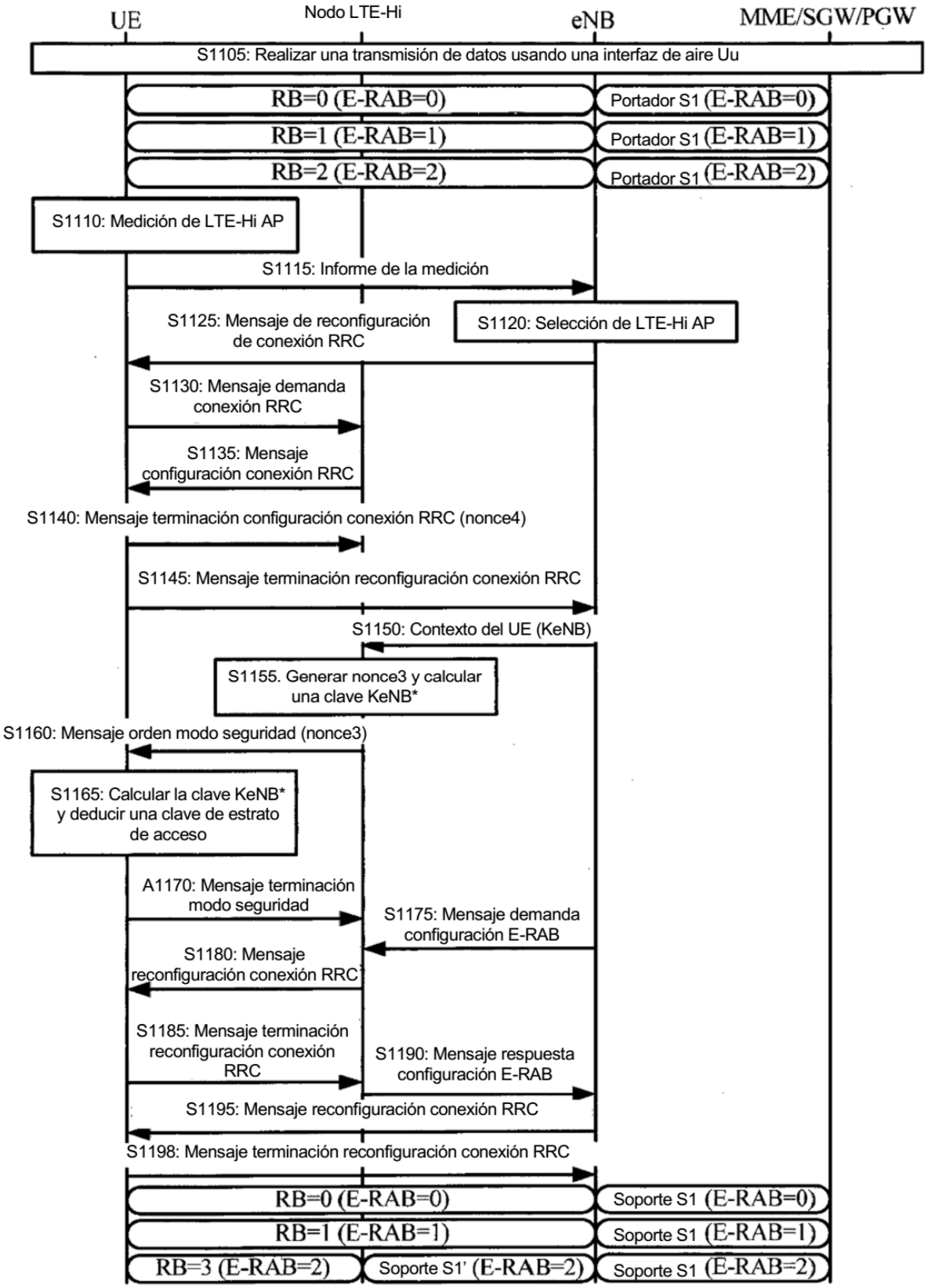
UE
Nodo LTE-Hi
eNB
MME/SGW/PGW
S1105: Realizar una transmisión de datos usando una interfaz de aire Uu
RB=0 (E-RAB=0)
Portador S1 (E-RAB=0)
RB=1 (E-RAB=1)
Portador S1 (E-RAB=1)
RB=2 (E-RAB=2)
Portador S1 (E-RAB=2)
S1110: Medición de LTE-Hi AP
S1115: Informe de la medición
S1125: Mensaje de reconfiguración de conexión RRC
S1120: Selección de LTE-Hi AP
S1130: Mensaje demanda conexión RRC
S1135: Mensaje configuración conexión RRC
S1140: Mensaje terminación configuración conexión RRC (nonce4)
S1145: Mensaje terminación reconfiguración conexión RRC
S1150: Contexto del UE (KeNB)
S1155. Generar nonce3 y calcular una clave KeNB*
S1160: Mensaje orden modo seguridad (nonce3)
S1165: Calcular la clave KeNB* y deducir una clave de estrato de acceso
A1170: Mensaje terminación modo seguridad
S1175: Mensaje demanda configuración E-RAB
S1180: Mensaje reconfiguración conexión RRC
S1185: Mensaje terminación reconfiguración conexión RRC
S1190: Mensaje respuesta configuración E-RAB
S1195: Mensaje reconfiguración conexión RRC
S1198: Mensaje terminación reconfiguración conexión RRC
RB=0 (E-RAB=0)
Soporte S1 (E-RAB=0)
RB=1 (E-RAB=1)
Soporte S1 (E-RAB=1)
RB=3 (E-RAB=2)
Soporte S1' (E-RAB=2)
Soporte S1 (E-RAB=2)

FIG. 11

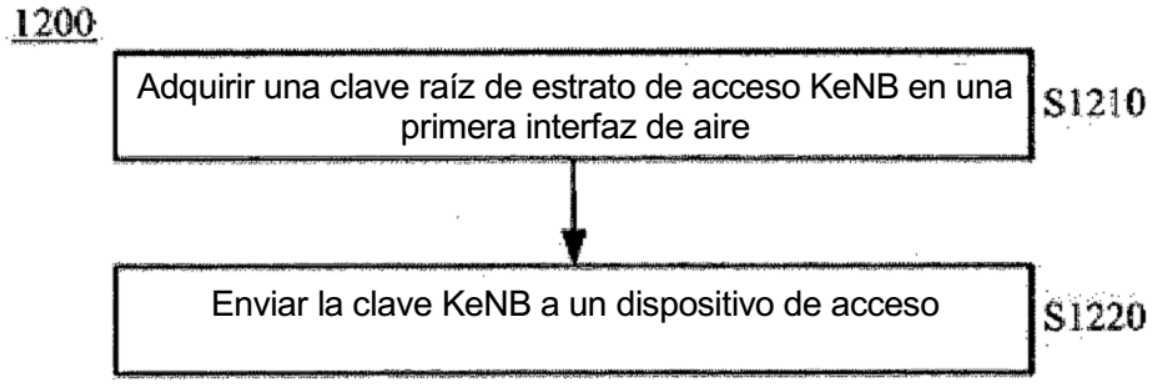

FIG. 12

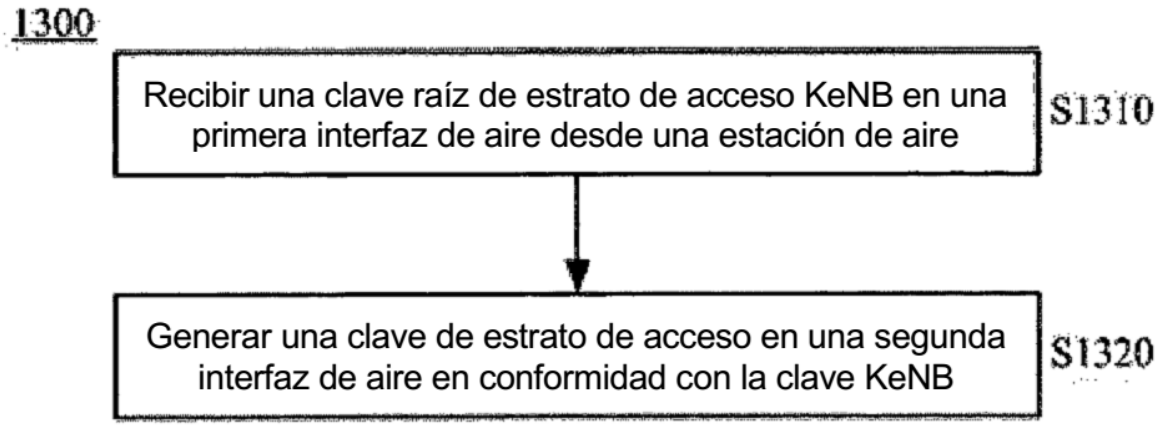

FIG. 13

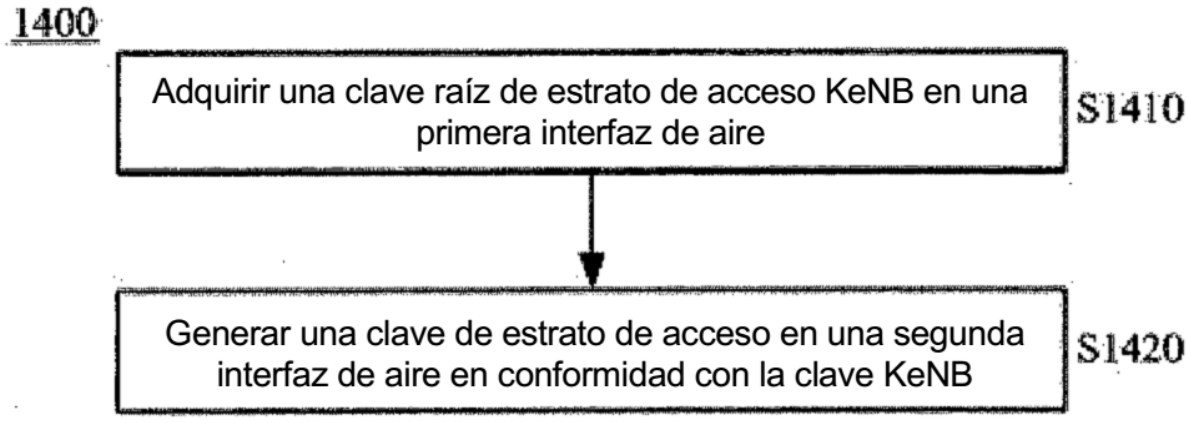

FIG. 14

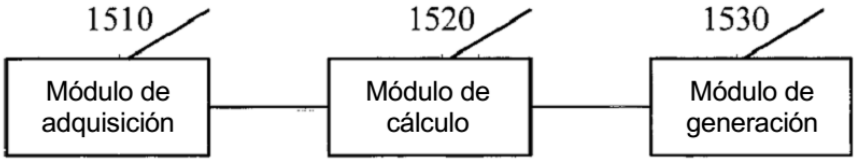

FIG. 15

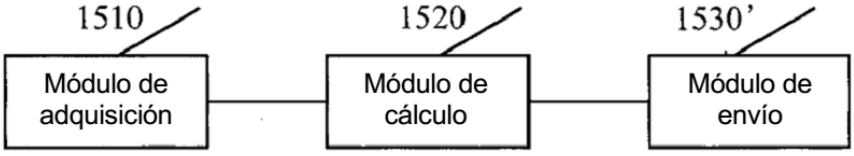

FIG. 15a

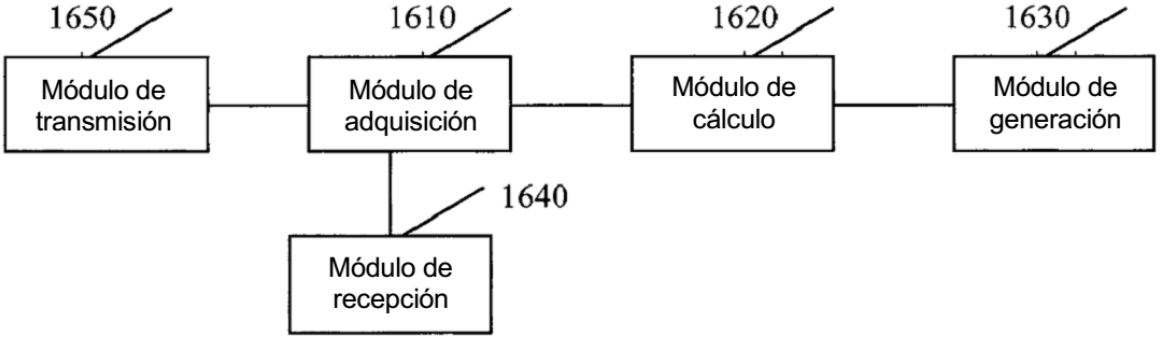

FIG. 16

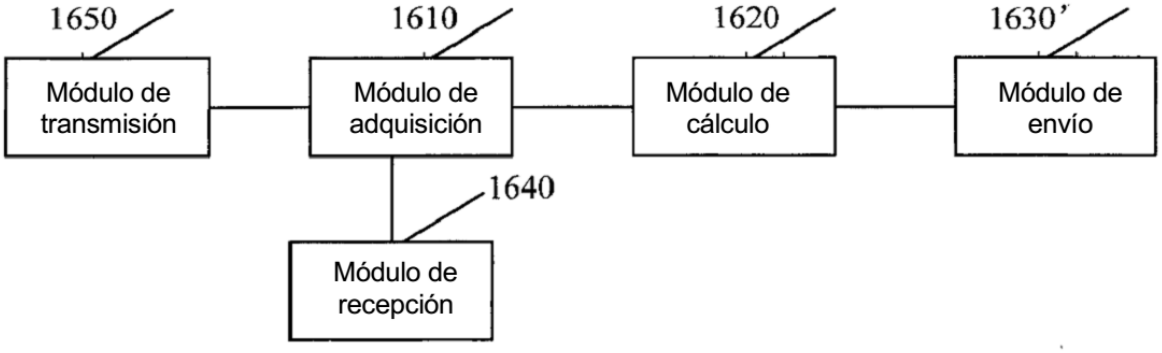

FIG. 16a

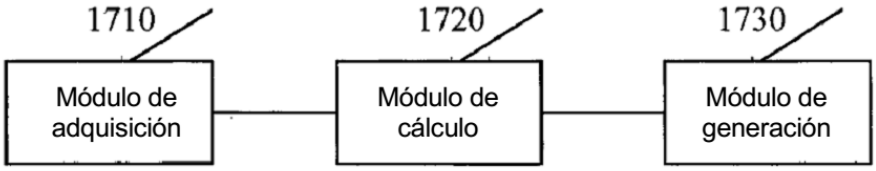
1710
Módulo de adquisición
1720
Módulo de cálculo
1730
Módulo de generación

FIG. 17

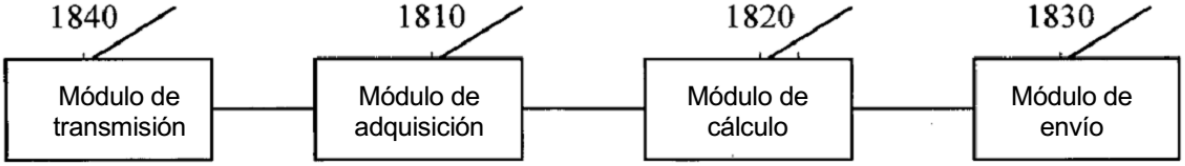
1840
Módulo de transmisión
1810
Módulo de adquisición
1820
Módulo de cálculo
1830
Módulo de envío

FIG. 18