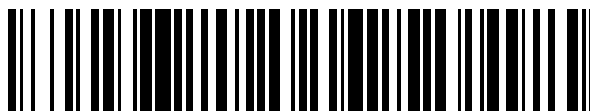


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 652 314**

51 Int. Cl.:

**H04W 74/08** (2009.01)

**H04W 88/00** (2009.01)

**H04W 76/02** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **03.07.2008 E 15190585 (8)**

97 Fecha y número de publicación de la concesión europea: **13.09.2017 EP 2991432**

54 Título: **Cifrado de enlace ascendente durante acceso aleatorio**

30 Prioridad:

**08.08.2007 US 835782**

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

**01.02.2018**

73 Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)  
(100.0%)  
164 83 Stockholm, SE**

72 Inventor/es:

**PARKVALL, STEFAN;  
TYNDERFELDT, TOBIAS y  
DAHLMAN, ERIK**

74 Agente/Representante:

**LINAGE GONZÁLEZ, Rafael**

**ES 2 652 314 T3**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Cifrado de enlace ascendente durante acceso aleatorio

5 **Campo técnico**

El campo técnico se refiere a las comunicaciones de radio móviles y, en particular, a las comunicaciones de enlace ascendente que implican terminales de radio móviles en un sistema de comunicaciones de radio móvil.

10 **Antecedentes**

El sistema universal de telecomunicaciones móviles (UMTS) es un sistema de comunicación móvil asíncrono de tercera generación (3G) que opera en acceso múltiple por división de código de banda ancha (WCDMA) basado en sistemas europeos, sistema global para las comunicaciones móviles (GSM) y servicios generales de paquetes vía radio (GPRS). La evolución a largo plazo (LTE) de UMTS está en desarrollo por el proyecto asociación de tercera generación (3GPP) que estandarizó UMTS. Hay muchas especificaciones técnicas alojadas en el sitio web de 3GPP relacionadas con el acceso radio terrestre universal evolucionado (E-UTRA) y la red de acceso radio terrestre universal evolucionada (E-UTRAN), por ejemplo, 3GPP TS 36.300. El objetivo del trabajo de LTE es desarrollar un marco para la evolución de la tecnología de acceso de radio 3GPP hacia una tecnología de acceso radio de alta velocidad de datos, baja latencia y paquetes optimizados. En particular, LTE apunta a soportar servicios provistos desde el dominio de paquetes conmutados (PS). Un objetivo clave de la tecnología LTE de 3GPP es permitir comunicaciones de paquetes de alta velocidad a 100 Mbps o por encima.

La figura 1 ilustra un ejemplo de un sistema 10 de comunicaciones móviles de tipo LTE. Una E-UTRAN 12 incluye E-NodoB (los eNodoB o eNB) 18 de UTRAN que proporcionan el plano de usuario E-UTRA y las terminaciones de protocolo del plano de control hacia el equipo 20 de usuario (UE) a través de una interfaz de radio. Aunque un eNB es un nodo lógico, implementado a menudo pero no necesariamente por una estación base física, el término estación base se utiliza aquí para cubrir generalmente tanto nodos lógicos como físicos. Un UE a veces se denomina terminal de radio móvil y, en estado inactivo, monitoriza la información del sistema transmitida por los eNB dentro del alcance para informarse a sí misma de las estaciones base "candidatas" en el área de servicio. Cuando un UE necesita acceso a servicios desde una red de acceso radio, envía una solicitud a través de un canal de acceso aleatorio (RACH) a un eNB adecuado, típicamente un eNB con las condiciones de radio más favorables. Los eNB están interconectados entre sí por medio de una interfaz X2. Los eNB también están conectados por medio de la interfaz S1 a un núcleo 14 de paquetes evolucionado (EPC) que incluye una entidad de gestión de movilidad (MME) por un S1-MME y a una pasarela de evolución de arquitectura de sistema (SAE) por un S1-U. La pasarela MME/SAE son referenciadas como un único nodo 22 en este ejemplo. La interfaz S1 admite una relación de muchos a muchos entre pasarelas de MME/SAE y eNB. La E-UTRAN 12 y el EPC 14 juntos forman una red móvil terrestre pública (PLMN). Las pasarelas MME/SAE 22 están conectados directa o indirectamente a Internet 16 y a otras redes.

Para poder operar en diferentes asignaciones de espectro, por ejemplo para migrar sin problemas de los sistemas celulares existentes al nuevo sistema de alta velocidad de datos de alta capacidad en el espectro de radio existente, es necesario operar en un ancho de banda flexible, por ejemplo, anchos de banda que van desde 1,25 MHz a 20 MHz para transmisiones de enlace descendente de red a UE. Deben admitirse los servicios de datos de alta velocidad, los servicios de baja velocidad como la voz, y dado que la LTE de 3G está diseñada para TCP/IP, es probable que VoIP sea el servicio que transmita el habla.

La transmisión del enlace ascendente de LTE se basa en la transmisión OFDM de extensión de transformada de Fourier discreta (DFTS-OFDM), una relación de potencia de pico bajo a media (PAPR), esquema de transmisión de portadora única (SC) que permite asignación de ancho de banda flexible y acceso múltiple ortogonal no solo en el dominio del tiempo sino también en el dominio de la frecuencia. Por lo tanto, el esquema de transmisión de enlace ascendente de LTE también se denomina a menudo FDMA de portadora única (SC-FDMA).

El procesamiento del canal de transporte del enlace ascendente de LTE se describe en la figura 2. Un bloque de transporte de tamaño dinámico se entrega desde la capa de control de acceso al medio (MAC). Se calcula un código de redundancia cíclica (CRC) a usar para la detección de errores en el receptor de la estación base para el bloque y se adjunta al mismo. La codificación de canal de enlace ascendente se realiza luego mediante un codificador de canal que puede usar cualquier técnica de codificación adecuada. En LTE, el código puede ser un código turbo que incluye un intercalador interno basado en el polinomio de permutación cuadrática (QPP) para realizar el intercalado de bloques como parte del turbocodificador. La solicitud de repetición automática (ARQ) híbrida de enlace ascendente de LTE extrae, del bloque de bits codificados entregados por el codificador de canal, el conjunto exacto de bits a transmitir en cada instante de transmisión/retransmisión. Un codificador cifra los bits codificados en el enlace ascendente de LTE (por ejemplo, cifrado a nivel de bits) con el fin de aleatorizar la interferencia y así garantizar que la ganancia de procesamiento provista por el código del canal se pueda usar completamente.

Para lograr esta aleatorización de la interferencia, el cifrado del enlace ascendente es específico del terminal móvil,

es decir, los diferentes terminales móviles (los UE) utilizan diferentes secuencias de cifrado. El cifrado específico del terminal también proporciona al planificador la libertad de planificar múltiples usuarios en el mismo recurso de tiempo-frecuencia y confiar en el procesamiento del receptor de la estación base para separar las transmisiones de los múltiples usuarios. El cifrado específico del terminal aleatoriza la interferencia de otros terminales móviles en la misma célula que resulta que está planificada en el mismo recurso y mejora el rendimiento.

Después del cifrado, los datos se modulan para transformar un bloque de bits codificados/cifrados en un bloque de símbolos de modulación complejos. El conjunto de esquemas de modulación soportados para el ejemplo de enlace ascendente de LTE incluye QPSK, 16QAM y 64QAM, que corresponden a dos, cuatro y seis bits por símbolo de modulación, respectivamente. El bloque de símbolos de modulación se aplica luego a un modulador DFTS-OFDM, que también mapea la señal a un recurso de radio asignado, por ejemplo, una subbanda de frecuencia.

Junto con los símbolos de datos modulados, la señal mapeada a la banda de frecuencia asignada también contiene señales de referencia de demodulación. Las señales de referencia conocidas de antemano tanto por el terminal móvil (UE) como por la estación base (eNodoB) son utilizadas por el receptor para la estimación del canal y la demodulación de los símbolos de datos. Se pueden asignar diferentes señales de referencia a un terminal de usuario por razones similares. Se pueden usar códigos de cifrado específicos del terminal, es decir, planificar inteligentemente a múltiples usuarios en el mismo recurso de tiempo-frecuencia y así realizar el denominado MIMO multiusuario. En el caso de MIMO multiusuario, depende del procesamiento eNodoB separar las señales transmitidas desde los dos (o más) UE planificados simultáneamente en el mismo recurso de frecuencia en la misma célula. A los terminales planificados simultáneamente en el mismo recurso de frecuencia se les asignan típicamente secuencias de señal de referencia diferentes (por ejemplo, ortogonales) para que el eNodo B estime los canales de radio en cada uno de esos UE.

Un requisito básico para cualquier sistema celular u otro de comunicaciones de radio es proporcionar a un terminal de usuario la capacidad de solicitar una configuración de conexión. Esta capacidad se conoce comúnmente como acceso aleatorio y tiene dos propósitos principales en LTE, a saber, establecimiento de sincronización de enlace ascendente con la temporización de estación base y establecimiento de una única identidad de terminal de usuario, por ejemplo, un identificador temporal de red de radio celular (C-RNTI) en LTE, conocido tanto por la red como por el terminal de usuario que se utiliza en las comunicaciones para distinguir la comunicación del usuario de otras comunicaciones.

Pero durante el procedimiento de acceso aleatorio (inicial), las transmisiones de enlace ascendente desde el terminal de usuario no pueden emplear secuencias de cifrado o números de referencia específicos del terminal para aleatorizar la interferencia porque el mensaje inicial de solicitud de acceso aleatorio desde el terminal de usuario acaba de comenzar a comunicarse con la red y ni el código de cifrado específico del terminal ni un número de referencia específico del terminal se han asignado a ese terminal de usuario. Lo que se necesita es un mecanismo que permita a los mensajes de acceso aleatorio enviados a través de un canal de enlace ascendente compartido ser cifrado hasta que se pueda asignar un código de cifrado específico del terminal al terminal de usuario. Una razón para cifrar los mensajes de acceso aleatorio es aleatorizar la interferencia intercelular, que también es el caso para el cifrado durante la transmisión de datos de enlace ascendente "normal". En el último caso, el cifrado también se puede usar para suprimir la interferencia intracelular en el caso de que se planifiquen múltiples UE en el mismo recurso de tiempo-frecuencia. De manera similar, también sería deseable poder tener terminales de usuario que transmitan señales de referencia conocidas durante el acceso aleatorio para permitir que el receptor de la estación base estime el canal de enlace ascendente. Las señales de referencia deben incluirse en los mensajes de acceso aleatorio, así como en las transmisiones de datos de enlace ascendente "normales" para permitir la estimación de canal en el eNodoB y la correspondiente demodulación coherente.

El documento EP 0565507 A2 describe una estación móvil que tiene medios para seleccionar un código de cifrado de una lista de códigos de cifrado disponibles transmitidos desde otra estación base de radio para generar un mensaje de acceso aleatorio.

**Sumario**

La tecnología que se describe a continuación facilita el acceso aleatorio de un terminal de usuario con una estación base de radio. Un terminal de usuario determina uno de un primer tipo de secuencias de cifrado de enlace ascendente y genera un mensaje de acceso aleatorio utilizando el determinado del primer tipo de secuencias de cifrado de enlace ascendente. Su transmisor transmite el mensaje de acceso aleatorio a la estación base de radio. El receptor del terminal de usuario recibe entonces de la estación base un segundo tipo diferente de secuencia de cifrado de enlace ascendente. El terminal utiliza ese segundo tipo diferente de secuencia de cifrado de enlace ascendente para una comunicación posterior con la estación base de radio. En una realización de ejemplo no limitativa, el primer tipo de secuencias de cifrado de enlace ascendente puede asociarse específicamente con el área de la célula de la estación base de radio o un canal de radio de acceso aleatorio asociado a la estación base de radio, pero no están específicamente asignadas a ningún terminal de usuario, y el segundo tipo diferente de secuencia de cifrado de enlace ascendente se puede seleccionar a partir de un segundo conjunto de secuencias de cifrado de enlace ascendente específicamente asignables a los terminales de usuario. El uso de estos dos tipos

diferentes de secuencias de cifrado permite a los terminales de usuario cifrar sus transmisiones de señal de enlace ascendente incluso aunque los códigos de cifrado específicos de terminal no puedan usarse en el enlace ascendente durante el acceso aleatorio por los terminales de usuario.

5 El terminal de usuario transmite un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio utilizando un recurso de radio de canal de acceso aleatorio. A continuación, se recibe un segundo mensaje de respuesta de acceso aleatorio desde la estación base de radio que indica un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario temporal. El terminal ajusta una temporización en el terminal de usuario para transmitir señales a la estación base de radio basándose en la información recibida en el mensaje de respuesta de acceso aleatorio, y basándose en la temporización ajustada, transmite un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad de usuario completa del usuario del terminal a la estación base de radio a través del recurso de radio identificado. El tercer mensaje es cifrado utilizando el determinado del primer tipo de secuencia de cifrado de enlace ascendente, se modula y se mapea a un recurso de canal de radio. El terminal recibe un cuarto mensaje de resolución de contención desde la estación base de radio para completar los procedimientos de acceso aleatorio y siguen las comunicaciones normales.

20 Varias realizaciones no limitativas mapean el primer conjunto de secuencias de cifrado de enlace ascendente a algún otro parámetro conocido por el terminal de usuario y la estación base. Por ejemplo, el primer conjunto de secuencias de cifrado de enlace ascendente puede ser mapeadas a secuencias de preámbulo de acceso aleatorio correspondientes. Uno de los primeros conjuntos de secuencias de cifrado de enlace ascendente puede entonces seleccionarse basándose en el preámbulo de acceso aleatorio incluido en el primer mensaje de solicitud de acceso aleatorio y el mapeo. Otro ejemplo mapea el primer conjunto de secuencias de cifrado de enlace ascendente con los identificadores de terminal de usuario correspondientes y selecciona uno de los primeros conjuntos de secuencias de cifrado de enlace ascendente basándose en el identificador de terminal de usuario incluido en el segundo mensaje de respuesta de acceso aleatorio y el mapeo. Un tercer ejemplo mapea el primer conjunto de secuencias de cifrado de enlace ascendente a recursos de radio correspondientes utilizados para transmitir el mensaje de solicitud de acceso aleatorio y selecciona uno de los primeros conjuntos de secuencias de cifrado de enlace ascendente basándose en el recurso de radio de canal de acceso aleatorio utilizado para enviar un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio y el mapeo.

35 El enfoque de secuencia de cifrado de dos tipos también puede usarse para señales de referencia incorporadas en mensajes de acceso aleatorio de enlace ascendente enviados a la estación base que son utilizados por la estación base para estimar el canal de enlace ascendente, por ejemplo, para fines de equalización, etc. Se selecciona una de un primer conjunto de secuencias de referencia de enlace ascendente, por ejemplo, secuencias de referencia de enlace ascendente específicamente asociadas con un área de célula de estación base de radio o un canal de acceso aleatorio pero que no están específicamente asignadas a ningún terminal de usuario. Se genera un mensaje de acceso aleatorio utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente y la seleccionada del primer conjunto de secuencias de referencia de enlace ascendente. El terminal de usuario transmite el mensaje de acceso aleatorio a la estación base de radio. Después de eso, la estación base informa al terminal de usuario de un segundo tipo diferente de secuencia de referencia para usar en comunicaciones posteriores de enlace ascendente, por ejemplo, un número de referencia asignado específicamente a ese terminal de usuario.

45 En una implementación de ejemplo no limitativa, el terminal de usuario y la estación base están configurados para comunicarse con una red de radiocomunicaciones de evolución a largo plazo (LTE) con el terminal de usuario transmitiendo el primer mensaje de solicitud de acceso aleatorio a través de un canal de acceso aleatorio (RACH) y el tercer mensaje a través de un canal compartido de enlace ascendente (UL-SCH). El identificador de terminal de usuario enviado por la estación base en el segundo mensaje puede ser un identificador de terminal de usuario temporal utilizado hasta que se asigne un identificador de terminal de red de radio (RNTI) al terminal de usuario.

**Breve descripción de los dibujos**

55 La figura 1 es un ejemplo del sistema de comunicaciones de radio móvil de LTE;

la figura 2 es un diagrama de flujo que ilustra procedimientos de ejemplo no limitativos para preparar un bloque de transporte entregado desde la capa de acceso a medios de un terminal de usuario para la transmisión a través de la interfaz de radio a la red en un sistema de comunicaciones de radio móvil de LTE;

60 la figura 3 es un diagrama de flujo que ilustra procedimientos de ejemplo no limitativos para que un terminal de usuario haga un acceso aleatorio en la red de radio;

65 la figura 4 es un diagrama de flujo que ilustra procedimientos de ejemplo no limitativos para que una estación base reciba y procese un acceso aleatorio de terminal de usuario en la red de radio;

las figuras 5A y 5B ilustran un mapeo entre el transporte y los canales físicos en el enlace descendente y el enlace ascendente, respectivamente;

la figura 6 es un diagrama que ilustra tres estados básicos de un terminal de usuario;

5 la figura 7 es un diagrama de señalización que ilustra un procedimiento de acceso aleatorio de ejemplo no limitativo;

la figura 8 ilustra un ejemplo no limitativo de una transmisión de preámbulo de acceso aleatorio; y

10 la figura 9 es un diagrama de bloques de funciones de ejemplo no limitativo de un terminal de usuario y una estación base eNodo B.

### Descripción detallada

15 En la siguiente descripción, con fines explicativos y no limitativos, se establecen detalles específicos, tales como nodos particulares, entidades funcionales, técnicas, protocolos, estándares, etc. con el fin de proporcionar una comprensión de la tecnología descrita. En otros casos, se omiten descripciones detalladas de métodos, dispositivos, técnicas, etc. bien conocidos para no ocultar la descripción con detalles innecesarios. Los bloques de funciones individuales se muestran en las figuras. Los expertos en la técnica apreciarán que las funciones de esos bloques  
20 pueden implementarse utilizando circuitos de hardware individuales, utilizando programas de software y datos junto con un microprocesador u ordenador de propósito general adecuadamente programado, utilizando circuitos integrados de aplicación específica (ASIC), matrices lógicas programables y/o el uso de uno o más procesadores de señal digital (DSP).

25 Será evidente para un experto en la técnica que pueden realizarse otras realizaciones aparte de los detalles específicos divulgados a continuación. La tecnología se describe en el contexto de un sistema UMTS de 3GPP evolucionado, tal como LTE, a fin de proporcionar un contexto de ejemplo y no limitativo para la explicación. Véase por ejemplo el diagrama del sistema de LTE que se muestra en la figura 1. Pero esta tecnología no se limita a LTE y puede usarse en cualquier sistema moderno de comunicaciones de radio. Además, el enfoque a continuación que  
30 emplea dos tipos diferentes de secuencias de cifrado, una para fines de acceso aleatorio y una para comunicaciones después de que se complete el acceso aleatorio, también se puede aplicar a señales de referencia de estimación de canal conocidas (a veces denominadas señales piloto). Sin embargo, la explicación detallada se proporciona utilizando secuencias de cifrado con el entendimiento de que se aplican detalles similares a las señales de referencia. Para facilitar la descripción, un equipo de usuario (UE) se denomina a menudo, sin limitación, como un  
35 terminal de usuario o un terminal móvil, y se hace referencia a un eNodoB utilizando la estación base de términos más general y familiar.

La figura 3 es un diagrama de flujo que ilustra procedimientos de ejemplo no limitativos para que un terminal de usuario haga un acceso aleatorio a la red de radio utilizando un código de cifrado de enlace ascendente que está  
40 generalmente disponible para todos los terminales de usuario que desean acceder aleatoriamente al servicio en una célula particular. El terminal de usuario detecta un primer tipo de secuencias de cifrado de enlace ascendente, por ejemplo, secuencias de cifrado de enlace ascendente específicamente asociadas con un área de célula de la estación base de radio o canal de acceso aleatorio pero que no están específicamente asignadas a ningún terminal de usuario (paso S1). Se determina una seleccionada del primer tipo de secuencias de cifrado de enlace ascendente  
45 (paso S2), y se genera un mensaje de acceso aleatorio utilizando la seleccionada del primer tipo de secuencias de cifrado de enlace ascendente (paso S3). El terminal de usuario transmite el mensaje de acceso aleatorio a la estación base de radio (paso S4). Después de transmitir el mensaje de acceso aleatorio, el terminal de usuario recibe de la estación base de radio un segundo tipo diferente de secuencia de cifrado de enlace ascendente, por ejemplo, una secuencia de cifrado de enlace ascendente seleccionada de un segundo conjunto de secuencias de cifrado de enlace ascendente asignables específicamente a terminales de usuario (paso S5). El terminal de usuario  
50 utiliza el segundo tipo de secuencia de cifrado de enlace ascendente para la comunicación posterior con la estación base de radio. Se pueden usar procedimientos similares para las señales de referencia de enlace ascendente conocidas.

55 La figura 4 es un diagrama de flujo que ilustra procedimientos de contrapartida de ejemplo no limitativos, para que una estación base reciba y procese un acceso aleatorio del terminal de usuario a la red de radio. Cada estación base en la red tiene su propio conjunto de secuencias de preámbulo, señales de referencia y códigos o secuencias de cifrado específicos no terminales. La estación base transmite, implícita o explícitamente, a través de un canal de transmisión, por ejemplo, BCH, su conjunto de preámbulos y secuencias de cifrado de enlace ascendente (paso S10). Si la estación base no transmite explícitamente la secuencia de cifrado a usar, la identidad de la célula a partir de la cual se puede derivar la secuencia de cifrado a usar, por ejemplo, mediante un mapeo entre la secuencia y el  
60 identificador de célula. Las secuencias de cifrado de enlace ascendente pueden estar, por ejemplo, asociadas específicamente con un área de célula de una estación base de radio o un canal de acceso aleatorio y no están asignadas específicamente a ningún terminal de usuario. La estación base espera a recibir un primer mensaje de solicitud de acceso aleatorio desde un terminal de usuario que incluye uno de los preámbulos de la estación base.  
65 En respuesta, la estación base transmite un segundo mensaje de respuesta de acceso aleatorio a un terminal de

usuario que indica un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario. Un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad del terminal de usuario es descifrada utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente (paso S11). A continuación, la estación base transmite al terminal de usuario un cuarto mensaje que incluye un segundo tipo diferente de secuencia de cifrado de enlace ascendente seleccionada de un segundo conjunto de secuencias de cifrado de enlace ascendente, por ejemplo, secuencias de cifrado de enlace ascendente que son asignables específicamente a terminales de usuario (paso S12). El terminal de usuario utiliza la segunda secuencia de cifrado del enlace ascendente para la comunicación posterior con la estación base de radio. Se pueden aplicar procedimientos similares para las señales de referencia de enlace ascendente conocidas.

Para comprender mejor el siguiente procedimiento de acceso aleatorio de LTE de ejemplo no limitativo, se hace referencia a las figuras 5A y 5B que ilustran un mapeo entre los canales de transporte y físicos en el enlace descendente y el enlace ascendente, respectivamente. Los siguientes son canales de transporte de enlace descendente: el canal de transmisión (BCH), el canal de búsqueda (PCH), el canal compartido de enlace descendente (DL-SCH) y el canal de transmisión múltiple (MCH). El BCH se mapea al canal de transmisión física (PBCH), y el PCH y el DL-SCH se mapean al canal compartido de enlace descendente físico (PDSH). Los canales de transporte de enlace ascendente incluyen el canal de acceso aleatorio (RACH) y el canal compartido de enlace ascendente (UL-SCH). El RACH se mapea al canal de acceso aleatorio físico (PRACH) y el UL-SCH mapea al canal compartido de enlace ascendente físico (PUSCH).

En LTE, como en otros sistemas de comunicación de radio móvil, un terminal móvil puede estar en varios estados de funcionamiento diferentes. La figura 6 ilustra esos estados para LTE. En el encendido, el terminal móvil entra en el estado LTE\_DETACHED. En este estado, la red no conoce el terminal móvil. Antes de que pueda tener lugar cualquier otra comunicación entre el terminal móvil y la red, el terminal móvil necesita registrarse en la red utilizando el procedimiento de acceso aleatorio para entrar en el estado LTE\_ACTIVE. El estado LTE\_DETACHED es principalmente un estado utilizado en el encendido. Una vez que el terminal móvil se registra con la red, por lo general se encuentra en uno de los otros estados: LTE\_ACTIVE o LTE\_IDLE.

LTE\_ACTIVE es el estado utilizado cuando el terminal móvil está activo con la transmisión y recepción de datos. En este estado, el terminal móvil está conectado a una célula específica dentro de la red. Se han asignado uno o varios protocolos de Internet (IP) u otro tipo de direcciones de paquetes de datos al terminal móvil, así como una identidad del terminal, un identificador temporal de red de radio celular (C-RNTI), utilizado para fines de señalización entre el móvil terminal y la red. El estado LTE\_ACTIVE incluye dos subestados, IN\_SYNC y OUT\_OF\_SYNC, dependiendo de si el enlace ascendente está sincronizado a la red o no. Siempre que el enlace ascendente esté en IN\_SYNC, son posibles las transmisiones del enlace ascendente de los datos del usuario y la señalización de control de la capa inferior. Si no ha tenido lugar una transmisión de enlace ascendente dentro de una franja de tiempo dada, se declara que el enlace ascendente está fuera de sincronización, en cuyo caso, el terminal móvil debe realizar un procedimiento de acceso aleatorio para restablecer la sincronización de enlace ascendente.

LTE\_IDLE es un estado de baja actividad en el que el terminal móvil duerme la mayor parte del tiempo para reducir el consumo de batería. La sincronización del enlace ascendente no se mantiene, y por lo tanto, la única actividad de transmisión del enlace ascendente que puede tener lugar es el acceso aleatorio para pasar a LTE\_ACTIVE. El terminal móvil mantiene su dirección o dirección de IP y otra información interna para moverse rápidamente a LTE\_ACTIVE cuando sea necesario. La posición del terminal móvil se conoce parcialmente en la red de modo que la red conoce al menos el grupo de células en el que se debe realizar la búsqueda del terminal móvil.

Un procedimiento de acceso aleatorio de ejemplo no limitativo se ilustra en la figura 7 e incluye cuatro pasos denominados pasos 1-4 con cuatro mensajes de señalización asociados a los que se hace referencia como mensajes 1-4. La estación base transmite un conjunto de preámbulos asociados con esa estación base, información de recursos de RACH y otra información en un mensaje de transmisión enviado regularmente a través de un canal de transmisión que exploran regularmente los terminales móviles activos. En el paso uno, después de que el terminal de usuario recibe y decodifica la información transmitida por la estación base (eNodoB), selecciona uno de los preámbulos de acceso aleatorio de la estación base y lo transmite por el RACH. La estación base monitoriza el RACH y detecta el preámbulo que permite a la estación base estimar el tiempo de transmisión del terminal de usuario. La sincronización de enlace ascendente es necesaria para permitir que el terminal transmita datos de enlace ascendente a la estación base.

El preámbulo de acceso aleatorio incluye una secuencia conocida, seleccionada aleatoriamente por el terminal móvil a partir de un conjunto de secuencias de preámbulo conocidas disponibles para fines de acceso aleatorio con una estación base particular. Cuando se realiza un intento de acceso aleatorio, el terminal selecciona una secuencia de preámbulo aleatoriamente del conjunto de secuencias de preámbulo asignadas a la célula a la que el terminal está tratando de acceder. Siempre que ningún otro terminal esté realizando un intento de acceso aleatorio utilizando la misma secuencia de preámbulo en el mismo instante de tiempo, no se producirán colisiones, y la estación base detectará muy probablemente la solicitud de acceso aleatorio. El preámbulo es transmitido por un terminal de usuario en un recurso de canal de radio, por ejemplo, un recurso de tiempo/frecuencia, asignado para fines de acceso aleatorio, por ejemplo, un RACH.

La figura 8 ilustra conceptualmente una transmisión de preámbulo de acceso aleatorio de acuerdo con la especificación de LTE a partir de este escrito. Un ejemplo no limitativo para generar preámbulos adecuados se basa en las secuencias de Zadoff-Chu (ZC) y sus secuencias cíclicas desplazadas. Las secuencias Zadoff-Chu también se pueden usar, por ejemplo, para crear las señales de referencia de enlace ascendente incluidas en cada trama de datos para fines de estimación de canal.

Un terminal de usuario que lleva a cabo un intento de acceso aleatorio, antes de la transmisión del preámbulo, obtuvo la sincronización de enlace descendente desde un procedimiento de búsqueda de célula utilizando la información de temporización transmitida por la estación base. Pero como se explicó anteriormente, el tiempo de enlace ascendente aún no está establecido. El inicio de una trama de transmisión de enlace ascendente en el terminal se define con relación al inicio de la trama de transmisión de enlace descendente en el terminal. Debido al retraso de propagación entre la estación base y el terminal, la transmisión de enlace ascendente se retrasará con respecto a la temporización de transmisión de enlace descendente en la estación base. Debido a que no se conoce la distancia entre la estación base y el terminal, existe una incertidumbre en la temporización del enlace ascendente que corresponde al doble de la distancia entre la estación base y el terminal. Para tener en cuenta esta incertidumbre y evitar la interferencia con subtramas posteriores que no se utilizan para el acceso aleatorio, se utiliza un tiempo de guardia.

Volviendo al segundo paso de señalización de acceso aleatorio mostrado en la figura 7, en respuesta al intento de acceso aleatorio detectado, la estación base transmite un mensaje 2 de respuesta de solicitud de acceso aleatorio en el canal compartido de enlace descendente (DL-SCH). El mensaje 2 contiene un índice u otro identificador de la secuencia de preámbulo de acceso aleatorio que la estación base detectó y para la cual la respuesta es válida, una corrección de temporización de enlace ascendente u orden de avance de temporización calculada por la estación base después de procesar el preámbulo de acceso aleatorio recibido, una concesión de planificación que indica recursos que el terminal de usuario usará para la transmisión del mensaje en el tercer mensaje enviado desde el terminal móvil a la estación base, y una identidad de terminal de usuario temporal utilizada para la comunicación adicional entre el terminal de usuario y la estación base. Después de que se complete el paso 2, el terminal de usuario es sincronizado en el tiempo.

Si la estación base detecta múltiples intentos de acceso aleatorio (desde diferentes terminales de usuario), entonces los mensajes 2 de respuesta de solicitud de acceso aleatorio a múltiples terminales móviles pueden combinarse en una única transmisión. Por lo tanto, el mensaje 2 de respuesta de solicitud de acceso aleatorio es planificado en el DL-SCH y se indica en el canal de control de enlace descendente físico (PDCCH) utilizando una identidad común reservada para la respuesta de acceso aleatorio. El PDCCH es un canal de control utilizado para informar al terminal si hay datos en el DL-SCH destinados a ese terminal y, de ser así, en qué recursos de tiempo-frecuencia encontrar el DL-SCH. Todos los terminales de usuario que transmitieron un preámbulo monitorizan el PDCCH para una respuesta de acceso aleatorio transmitida utilizando la identidad común predefinida utilizada por la estación base para todas las respuestas de acceso aleatorio.

En el tercer paso 3, el terminal de usuario transmite la información necesaria en el mensaje 3 a la red utilizando los recursos de enlace ascendente planificados asignados en el mensaje 2 de respuesta de acceso aleatorio y sincronizado en el enlace ascendente. La transmisión del mensaje de enlace ascendente en el paso 3 de la misma manera que los datos de enlace ascendente planificados "normales", es decir, en el UL-SCH, en lugar de vincularlo al preámbulo en el primer paso, es beneficiosa por varias razones. En primer lugar, la cantidad de información transmitida en ausencia de sincronización de enlace ascendente debería minimizarse ya que la necesidad de un tiempo de guarda grande hace que tales transmisiones sean relativamente costosas. En segundo lugar, el uso de un esquema de transmisión de enlace ascendente "normal" para transmisión de mensajes permite que el tamaño de concesión y el esquema de modulación se ajusten, por ejemplo, a diferentes condiciones de radio. En tercer lugar, permite ARQ híbrido con combinación suave para el mensaje de enlace ascendente que puede ser valioso, especialmente en escenarios de cobertura limitada, ya que permite confiar en una o varias retransmisiones para recopilar suficiente energía para la señalización de enlace ascendente para asegurar una probabilidad suficientemente alta de transmisión de éxito. El terminal móvil transmite su identidad de terminal móvil temporal, por ejemplo, un C-RNTI temporal, en el tercer paso a la red utilizando el UL-SCH. El contenido exacto de esta señalización depende del estado del terminal, por ejemplo, si la red lo conoce previamente o no.

Siempre que los terminales que realizan un acceso aleatorio al mismo tiempo utilicen diferentes secuencias de preámbulo, no se produce ninguna colisión. Pero existe una cierta probabilidad de contención cuando múltiples terminales utilizan el mismo preámbulo de acceso aleatorio al mismo tiempo. En este caso, múltiples terminales reaccionan al mismo mensaje de respuesta de enlace descendente en el paso 2 y se produce una colisión en el paso 3. La resolución de colisión o contención se realiza en el paso 4.

En el paso 4, se transmite un mensaje de resolución de contención desde la estación base al terminal en el DL-SCH. Este paso resuelve la contención en caso de que múltiples terminales intenten acceder al sistema en el mismo recurso, identificando qué terminal de usuario se detectó en el tercer paso. Múltiples terminales que realizan intentos de acceso aleatorio simultáneos utilizando la misma secuencia de preámbulo en el paso 1 escuchan el mismo

- mensaje de respuesta en el paso 2, y por lo tanto, tienen el mismo identificador de terminal de usuario temporal. Por lo tanto, en el paso 4, cada terminal que recibe el mensaje de enlace descendente compara la identidad del terminal de usuario en el mensaje con la identidad del terminal de usuario que transmitieron en el tercer paso. Solo un terminal de usuario que observa una coincidencia entre la identidad recibida en el cuarto paso y la identidad transmitida como parte del tercer paso determina el procedimiento de acceso aleatorio como exitoso. Si aún no se le asignó un C-RNTI al terminal, la identidad temporal del segundo paso se promueve al C-RNTI; de lo contrario, el terminal de usuario conserva su C-RNTI ya asignado. Los terminales que no encuentran una coincidencia con la identidad recibida en el cuarto paso deben reiniciar el procedimiento de acceso aleatorio desde el primer paso.
- 10 Como se explicó anteriormente, la identidad del terminal de usuario incluida en el mensaje 3 se utiliza como parte del mecanismo de resolución de contención en el cuarto paso. Continuando en el ejemplo no limitativo de LTE, si el terminal de usuario está en el estado LTE\_ACTIVE, es decir, está conectado a una célula conocida y por lo tanto tiene un C-RNTI asignado, este C-RNTI se utiliza como la identidad del terminal en el mensaje de enlace ascendente. De lo contrario, se utiliza un identificador de terminal de red central, y la estación base necesita involucrar a la red central antes de responder al mensaje de enlace ascendente en el paso tres.
- 15 En este ejemplo de LTE no limitativo, solo el primer paso utiliza el procesamiento de capa física específicamente diseñado para el acceso aleatorio. Los últimos tres pasos utilizan el mismo procesamiento de capa física que para la transmisión de datos de enlace ascendente y de enlace descendente "normal", lo que simplifica la implementación tanto del terminal como de la estación base. Debido a que el esquema de transmisión utilizado para la transmisión de datos está diseñado para garantizar una alta flexibilidad espectral y alta capacidad, es deseable beneficiarse de estas características también al intercambiar mensajes de acceso aleatorio.
- 20 En el contexto de LTE no limitativo de ejemplo, los pasos generales de procesamiento descritos en la figura 2 que incluyen CRC, codificación, HARQ, aleatorización, modulación y modulación de DFTS-OFDM son aplicados por el terminal de usuario al mensaje 3 en la figura 7 y las transmisiones de enlace ascendente posteriores desde ese terminal de usuario a la estación base (no hay cifrado en el mensaje de acceso aleatorio de enlace ascendente inicial en el paso 1). Las diferentes secuencias de cifrado de enlace ascendente en el terminal dependen del tipo de transmisión de enlace ascendente. Para el mensaje 3 de acceso aleatorio, se utiliza un primer tipo de secuencia de cifrado, por ejemplo, un código de cifrado específico del canal de acceso aleatorio o específico de la célula. Para transmisiones de datos "normales" posteriores en el enlace ascendente, es decir, cuando la estación base ha asignado una identidad no temporal al terminal, se utiliza un segundo tipo de secuencia de cifrado, por ejemplo, un código de cifrado específico del terminal. Un enfoque similar de dos tipos puede usarse para las señales de referencia de enlace ascendente utilizadas por la estación base para la estimación de canal: un primer tipo, por ejemplo, una señal de referencia específica de acceso aleatorio o celular para el mensaje 3 de acceso aleatorio, seguido de un segundo tipo, por ejemplo, una secuencia de señal de referencia de enlace ascendente asignada o asociada a una estación base para el seguimiento de transmisiones de datos "normales".
- 25 30 35 40 Cuando la estación base asigna una secuencia de cifrado y/o secuencia de referencia al terminal móvil, esa secuencia de cifrado y/o secuencia de referencia específica del terminal se utiliza para todas las transmisiones de datos de enlace ascendente posteriores para esa conexión de enlace ascendente particular. La secuencia de cifrado y/o la secuencia de referencia a usar pueden configurarse explícitamente en el terminal móvil o estar unidas a la identidad del terminal (por ejemplo, un C-RNTI) que la estación base asigna a un terminal móvil.
- 45 En lo anterior, el terminal de usuario utiliza una secuencia de cifrado específica de la célula para cifrar el mensaje 3 porque antes de realizar el acceso aleatorio, el terminal de usuario ha decodificado la información de transmisión de la estación base/célula y, por lo tanto, conoce la identidad de la célula a la que está accediendo, los preámbulos de acceso aleatorio asociados con esa célula, y secuencias de cifrado y/o números de referencia específicos de la célula. Siempre que múltiples terminales que realizan acceso aleatorio al mismo tiempo tengan asignados diferentes recursos de tiempo/frecuencia para su respectivo mensaje 3 de acceso aleatorio de enlace ascendente, no existe interferencia entre estos usuarios y la falta de aleatorización entre usuarios no es un problema.
- 50 En una realización no limitativa, se introduce un mapeo de uno a uno entre la secuencia de preámbulo de acceso aleatorio utilizada en el mensaje de solicitud de acceso aleatorio enviado en el paso 1 de la figura 7 y la secuencia de cifrado utilizada para cifrar el mensaje de acceso aleatorio enviado en el paso 3. Debido a que tanto la estación base como el terminal de usuario saben que el preámbulo utilizado para el mensaje de solicitud de acceso aleatorio enviado en el paso 1 por el mensaje 3 de tiempo se va a transmitir, ambos saben qué secuencia de cifrado usar.
- 55 En otra realización no limitativa, la estación base asigna la secuencia de cifrado para que el terminal de usuario utilice para cifrar el mensaje 3 como parte de la respuesta de solicitud de acceso aleatorio transmitida en el paso 2 de la figura 7 (es decir, antes de la transmisión del mensaje 3) Como un ejemplo, esto se puede hacer estableciendo un mapeo de uno a uno entre el identificador de usuario temporal enviado en el mensaje 2, por ejemplo, un C-RNTI temporal, y la secuencia de cifrado a usar.
- 60 65 Todavía otra realización no limitativa vincula la secuencia de cifrado a usar por el terminal de usuario para cifrar el mensaje 3 a los recursos de tiempo-frecuencia utilizados por el terminal de usuario para transmitir el preámbulo de



acceso aleatorio (mensaje 1). En este caso, la secuencia de cifrado será conocida tanto por la estación base como por el terminal de usuario porque ambos conocen los recursos de tiempo-frecuencia utilizados para el primer mensaje de solicitud de acceso aleatorio. Para esta realización, la secuencia de cifrado se compartirá entre todos los terminales de usuario que transmiten un preámbulo de solicitud de acceso aleatorio en el mismo recurso o recursos de tiempo-frecuencia. Pero mientras a todos esos terminales se les asignen recursos de tiempo/frecuencia diferentes para su propio mensaje 3 de acceso aleatorio, no hay interferencia entre estos usuarios y la falta de aleatorización entre usuarios no es un problema.

También se pueden usar combinaciones de una o más de las cuatro formas de realización de ejemplo diferentes. De nuevo, los principios descritos en el ejemplo de secuencia de cifrado anterior y las cuatro realizaciones también se pueden usar para los números de referencia de enlace ascendente utilizados para la estimación del canal de enlace ascendente. En otras palabras, se puede usar un tipo de número de referencia general o compartida para el mensaje 3 de acceso aleatorio de enlace ascendente, y se puede usar otro número de referencia de tipo específico del terminal para las posteriores comunicaciones de enlace ascendente asociadas con la conexión.

Puede haber situaciones en las que al terminal de usuario ya se le haya asignado una identidad, pero aún tendrá que realizar un acceso aleatorio. Un ejemplo es cuando el terminal se registra con la red, pero pierde la sincronización en el enlace ascendente y, en consecuencia, necesita realizar un intento de acceso aleatorio para recuperar la sincronización del enlace ascendente. Aunque el terminal de usuario tiene una identidad asignada, el cifrado específico del terminal no se puede usar para el mensaje 3 en este caso ya que la red no sabe por qué el terminal está realizando el intento de acceso aleatorio hasta que se recibe el mensaje 3. Como resultado, se necesita usar una secuencia de cifrado asociada a la célula en lugar de una secuencia de cifrado específica del terminal obsoleto.

De acuerdo con esto, los beneficios del cifrado específico del terminal para la transmisión de datos normal se mantienen sin afectar la funcionalidad del procedimiento de acceso aleatorio. Como se describió anteriormente, el cifrado específico del terminal aleatoriza la interferencia que mejora el rendimiento de transmisión del enlace ascendente y proporciona flexibilidad adicional en el diseño de planificación.

Aunque se han mostrado y descrito varias realizaciones en detalle, las reivindicaciones no están limitadas a ninguna realización o ejemplo particular. Por ejemplo, aunque descrito principalmente en términos de secuencias aleatorias, el enfoque de dos tipos descrito para secuencias de cifrado de acceso aleatorio también puede usarse para determinar secuencias de señales de referencia enviadas en cada trama de enlace ascendente que son utilizadas por el receptor de la estación base con fines de estimación de canales de enlace ascendente. Ninguna de las descripciones anteriores debe interpretarse como que implica que un elemento, paso, rango o función en particular es esencial, de modo que debe incluirse en el alcance de las reivindicaciones. El alcance de la materia patentada se define solo por las reivindicaciones. El alcance de la protección legal se define por las palabras que se enumeran en las reivindicaciones permitidas y sus equivalentes. Todos los equivalentes estructurales y funcionales de los elementos de la realización preferida descrita anteriormente que son conocidos por los expertos en la técnica se incorporan expresamente en el presente documento como referencia y se pretende que estén abarcados por las presentes reivindicaciones. Además, no es necesario que un dispositivo o método aborde todos y cada uno de los problemas que se pretende resolver mediante la presente invención, para que estén abarcados por las presentes reivindicaciones. Ninguna reivindicación tiene la intención de invocar el párrafo 6 de 35 USC §112 a menos que se utilicen las palabras "medios para" o "paso para". Además, ninguna realización, característica, componente o paso en esta especificación está destinado a ser dedicado al público independientemente de si la realización, característica, componente o paso se enumera en las reivindicaciones.

#### Realizaciones enumeradas

1. Un método implementado en un terminal de usuario para acceder a un canal de radio, que comprende:

detectar un primer conjunto de secuencias de cifrado de enlace ascendente específicamente asociadas con un área de célula de estación base de radio o canal de acceso aleatorio pero que no están específicamente asignadas a ningún terminal de usuario;

determinar una seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente;

generar un mensaje de acceso aleatorio utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente; y

transmitir el mensaje de acceso aleatorio a la estación base de radio.

2. El método en la realización 1, que comprende además:

después de transmitir el mensaje de solicitud de acceso aleatorio, recibir de la estación base de radio una secuencia de cifrado de enlace ascendente específica del terminal de usuario seleccionada de un segundo conjunto de

secuencias de cifrado de enlace ascendente asignables específicamente a terminales de usuario,

en el que el terminal de usuario utiliza la secuencia de cifrado de enlace ascendente específica del terminal de usuario seleccionada para la comunicación posterior con la estación base de radio.

5 3. El método en la realización 1, en el que el paso de generación incluye información de cifrado en el mensaje de acceso aleatorio que utiliza la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente.

10 4. El método en la realización 3, en el que la transmisión incluye modular el mensaje de acceso aleatorio cifrado y mapear el mensaje modulado a un recurso de canal de radio.

5. El método en la realización 1, en el que el primer conjunto de secuencias de cifrado de enlace ascendente son secuencias de cifrado específicas de la célula correspondientes a una célula asociada a la estación base de radio.

15 6. El método en la realización 1, que comprende además:

enviar un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio utilizando un recurso de radio de canal de acceso aleatorio;

20 recibir un segundo mensaje de respuesta de acceso aleatorio desde la estación base de radio que indica un cambio de temporización, un recurso de radio identificado, y un identificador de terminal de usuario;

ajustar una temporización en el terminal de usuario para transmitir señales a la estación base de radio basándose en la información recibida en el mensaje de respuesta de acceso aleatorio;

25 basándose en la temporización ajustada, transmitir un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad del terminal de usuario a la estación base de radio a través del recurso de radio identificado, en el que el tercer mensaje es cifrado utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente; y

30 recibir un cuarto mensaje de resolución de contención desde la estación base de radio.

7. El método en la realización 6, en el que:

35 el primer conjunto de secuencias de cifrado de enlace ascendente es mapeado a las secuencias de preámbulo de acceso aleatorio correspondientes, y el método comprende además:

seleccionar uno de los primeros conjuntos de secuencias de cifrado de enlace ascendente basándose en el preámbulo de acceso aleatorio incluido en el primer mensaje de solicitud de acceso aleatorio y el mapeo.

40 8. El método en la realización 6, donde el primer conjunto de secuencias de cifrado de enlace ascendente es mapeado a los identificadores de terminal de usuario correspondientes, y el método comprende además:

45 seleccionar uno de los primeros conjuntos de secuencias de cifrado de enlace ascendente basándose en el identificador de terminal de usuario incluido en el segundo mensaje de respuesta de acceso aleatorio y el mapeo.

9. El método en la realización 6, en el que el primer conjunto de secuencias de cifrado de enlace ascendente es mapeado a los recursos de radio correspondientes utilizados para transmitir el mensaje de solicitud de acceso aleatorio, y el método comprende además:

50 seleccionar uno de los primeros conjuntos de secuencias de cifrado de enlace ascendente basándose en el recurso de radio de canal de acceso aleatorio utilizado para enviar un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio y el mapeo.

55 10. El método en la realización 1, que comprende además:

seleccionar uno de un primer conjunto de secuencias de referencia de enlace ascendente específicamente asociadas con un área de célula de la estación base de radio o un canal de acceso aleatorio pero que no están específicamente asignadas a ningún terminal de usuario;

60 generar un mensaje de acceso aleatorio utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente y la seleccionada del primer conjunto de secuencias de referencia de enlace ascendente; y

transmitir el mensaje de acceso aleatorio a la estación base de radio.

65 11. Un método implementado en una estación base para responder a terminales de usuario que solicitan servicio

desde la estación base a través de un canal de radio, que comprende:

5 transmitir un primer conjunto de secuencias de cifrado de enlace ascendente específicamente asociadas con un área de célula de la estación base de radio o canal de acceso aleatorio pero que no están específicamente asignadas a cualquier terminal de usuario;

recibir de uno de los terminales de usuario un mensaje de acceso aleatorio utilizando el del primer conjunto de secuencias de cifrado de enlace ascendente;

10 transmitir al terminal de usuario una secuencia de cifrado de enlace ascendente específica del terminal de usuario seleccionada de un segundo conjunto de secuencias de cifrado de enlace ascendente asignables específicamente a los terminales de usuario; y

15 recibir una comunicación posterior desde el terminal de usuario cifrado con la secuencia de cifrado de enlace ascendente específica del terminal de usuario seleccionada para la comunicación posterior con la estación base de radio.

12. El método en la realización 11, que comprende además:

20 recibir un primer mensaje de solicitud de acceso aleatorio desde el terminal de usuario que incluye un preámbulo de acceso aleatorio que utiliza un recurso de radio de canal de acceso aleatorio;

25 transmitir un segundo mensaje de respuesta de acceso aleatorio al terminal de usuario que indica un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario;

recibir a través del recurso de radio identificado un tercer mensaje correspondiente al mensaje de acceso aleatorio generado, en el que el tercer mensaje incluye la identidad del terminal de usuario y es cifrado utilizando la seleccionada del primer conjunto de secuencias de cifrado del enlace ascendente; y

30 transmitir un cuarto mensaje de resolución de contención al terminal de usuario.

35 13. Un terminal de usuario para solicitar servicio desde una estación base que tiene un área celular donde la estación base ofrece servicio de comunicaciones de radio, que comprende circuitería de procesamiento electrónico configurada para:

determinar uno de un primer tipo de secuencias de cifrado de enlace ascendente, y

40 generar un mensaje de acceso aleatorio utilizando el determinado del primer tipo de secuencias de cifrado de enlace ascendente, y

circuitería de transmisión de radio para transmitir el mensaje de acceso aleatorio a la estación base de radio, y circuitería receptora de radio para recibir de la estación base de radio un segundo tipo diferente de secuencia de cifrado de enlace ascendente,

45 en el que la circuitería electrónica de procesamiento está configurada para usar el segundo tipo diferente de secuencia de cifrado de enlace ascendente para la comunicación posterior con la estación base de radio.

50 14. El terminal de usuario en la realización 13, en el que el primer tipo de secuencias de cifrado de enlace ascendente están específicamente asociadas con el área de célula de la estación base de radio o un canal de radio de acceso aleatorio asociado con la estación base de radio pero que no están asignadas específicamente a ningún terminal de usuario, y un segundo tipo diferente de secuencia de cifrado de enlace ascendente se selecciona de un conjunto de secuencias de cifrado de enlace ascendente específicamente asignables a los terminales de usuario.

55 15. El terminal de usuario en la realización 13, en el que la circuitería de procesamiento electrónico está configurada para cifrar información en el mensaje de acceso aleatorio utilizando el determinado del primer tipo de secuencias de cifrado de enlace ascendente.

60 16. El terminal de usuario en la realización 15, en el que el transmisor está configurado para modular el mensaje de acceso aleatorio cifrado y mapear el mensaje modulado con un recurso de canal de radio.

17. El terminal de usuario en la realización 13, en el que:

65 el transmisor está configurado para transmitir un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio utilizando un recurso de radio de canal de acceso aleatorio;

el receptor está configurado para recibir un segundo mensaje de respuesta de acceso aleatorio desde la estación base de radio que indica un cambio de temporización, un recurso de radio identificado, y un identificador de terminal de usuario;

5 la circuitería de procesamiento electrónico está configurada para ajustar una temporización en el terminal de usuario para transmitir señales a la estación base de radio basándose en la información recibida en el mensaje de respuesta de acceso aleatorio;

10 basándose en la temporización ajustada, el transmisor está configurado para transmitir un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad del terminal de usuario a la estación base de radio a través del recurso de radio identificado, en el que el tercer mensaje es cifrado utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente; y

15 el receptor está configurado para recibir un cuarto mensaje de resolución de contención desde la estación base de radio.

18. El terminal de usuario en la realización 17, en el que la circuitería de procesamiento electrónico está configurada para:

20 mapear el primer conjunto de secuencias de cifrado de enlace ascendente a secuencias de preámbulo de acceso aleatorio correspondientes, y

seleccionar uno del primer conjunto de secuencias de cifrado de enlace ascendente basándose en el preámbulo de acceso aleatorio incluido en el primer mensaje de solicitud de acceso aleatorio y el mapeo.

25 19. El terminal de usuario en la realización 17, en el que la circuitería de procesamiento electrónico está configurada para:

30 mapear el primer conjunto de secuencias de cifrado de enlace ascendente a los identificadores de terminal de usuario correspondientes, y

seleccionar uno del primero conjunto de secuencias de cifrado de enlace ascendente basándose en el identificador de terminal de usuario incluido en el segundo mensaje de respuesta de acceso aleatorio y el mapeo.

35 20. El terminal de usuario en la realización 17, en el que la circuitería de procesamiento electrónico está configurada para:

mapear el primer conjunto de secuencias de cifrado de enlace ascendente a los recursos de radio correspondientes utilizados para transmitir el mensaje de solicitud de acceso aleatorio, y

40 seleccionar uno del primer conjunto de secuencias de cifrado de enlace ascendente basándose en el recurso de radio del canal de acceso aleatorio utilizado para enviar un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio y el mapeo.

45 21. El terminal de usuario en la realización 17, en el que la circuitería de procesamiento electrónico está configurada para:

seleccionar uno de un primer conjunto de secuencias de referencia de enlace ascendente asociadas específicamente con un área de célula de la estación base de radio o canal de acceso aleatorio pero que no están específicamente asignadas a ningún terminal de usuario; y

50 generar un mensaje de acceso aleatorio utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente y la seleccionada del primer conjunto de secuencias de referencia de enlace ascendente, y

55 en el que el transmisor está configurado para transmitir el mensaje de acceso aleatorio a la estación base de radio.

60 22. El terminal de usuario en la realización 17, en el que el terminal de usuario está configurado para comunicarse con una red de radiocomunicaciones de evolución a largo plazo (LTE), y el transmisor está configurado para transmitir el primer mensaje de solicitud de acceso aleatorio a través de un canal de acceso aleatorio (RACH) y el tercer mensaje a través de un canal compartido de enlace ascendente (UL\_SCH).

23. El terminal de usuario en la realización 22, en el que el identificador de terminal de usuario es un identificador de terminal de usuario temporal utilizado hasta que se asigna un identificador de terminal de red de radio (RNTI) al terminal de usuario.

65 24. Una estación base de radio para responder a los terminales de usuario que solicitan servicio desde la estación

## ES 2 652 314 T3

base a través de un canal de radio, que comprende circuitería configurada para:

transmitir un primer conjunto de secuencias de cifrado de enlace ascendente específicamente asociadas con un área de célula de la estación base de radio o canal de acceso aleatorio pero que no son específicamente asignadas a cualquier terminal de usuario;

5 recibir de uno de los terminales de usuario un mensaje de acceso aleatorio utilizando el del primer conjunto de secuencias de cifrado de enlace ascendente;

10 transmitir al terminal de usuario una secuencia de cifrado de enlace ascendente específica del terminal de usuario seleccionada de un segundo conjunto de secuencias de cifrado de enlace ascendente específicamente asignables a los terminales de usuario; y

15 recibir una comunicación posterior desde el terminal de usuario codificado con la secuencia de cifrado de enlace ascendente específica del terminal de usuario seleccionada para la posterior comunicación con la estación base de radio.

25. La estación base de radio en la realización 24, en la que la circuitería está configurada además para:

20 recibir un primer mensaje de solicitud de acceso aleatorio desde el terminal de usuario que incluye un preámbulo de acceso aleatorio que utiliza un recurso de radio de canal de acceso aleatorio;

transmitir un segundo mensaje de respuesta de acceso aleatorio al terminal de usuario que indica un cambio de temporización, un recurso de radio identificado, y un identificador de terminal de usuario;

25 recibir a través del recurso de radio identificado un tercer mensaje correspondiente al mensaje de acceso aleatorio generado, en el que el tercer mensaje incluye la identidad del terminal de usuario y es cifrado utilizando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente; y

30 transmitir un cuarto mensaje de resolución de contención al terminal de usuario.

26. La estación base de radio en la realización 25, en la que la estación base es parte de una red de radiocomunicaciones de evolución a largo plazo (LTE), el primer mensaje de solicitud de acceso aleatorio se recibe a través de un canal de acceso aleatorio (RACH) y el tercer mensaje se recibe a través de un canal compartido de enlace ascendente (UL\_SCH).

35 27. La estación base de radio en la realización 26, en la que el identificador de terminal de usuario es un identificador de terminal de usuario temporal utilizado hasta que se asigna un identificador de terminal de red de radio (RNTI) al terminal de usuario.

40

**REIVINDICACIONES**

- 1.- Un método implementado en un terminal de usuario para solicitar servicio desde una estación base que tiene un área de célula donde la estación base ofrece servicio de radiocomunicaciones, comprendiendo el método:
- 5
- determinar (S1, S2) una primera secuencia de cifrado de enlace ascendente, en el que dicha primera secuencia de cifrado de enlace ascendente es una secuencia de cifrado específica de acceso aleatorio o específica de la célula, y
  - generar (S3) un mensaje de acceso aleatorio utilizando la primera secuencia de cifrado de enlace ascendente determinada, y
  - 10 - transmitir (S4) el mensaje de acceso aleatorio a una estación base de radio, y
  - recibir (S5) desde la estación base una asignación de una segunda secuencia de cifrado de enlace ascendente, en el que dicha segunda secuencia de cifrado de enlace ascendente es una secuencia de cifrado específica de terminal, y
  - 15 - usar (S5) la segunda secuencia de cifrado de enlace ascendente para la comunicación posterior con la estación base de radio.
- 20
- 2.- El método de la reivindicación 1, en el que el paso de generación incluye información de cifrado en el mensaje de acceso aleatorio utilizando la primera secuencia de cifrado de enlace ascendente determinada.
- 3.- El método de la reivindicación 1, en el que la transmisión incluye modular el mensaje de acceso aleatorio cifrado y mapear el mensaje modulado a un recurso de canal de radio.
- 25
- 4.- El método de la reivindicación 1, en el que la primera secuencia de cifrado del enlace ascendente es una secuencia de cifrado específica de la célula correspondiente a una célula asociada con la estación base de radio.
- 30
- 5.- Un método implementado en una estación base para responder a terminales de usuario que solicitan servicio desde la estación base a través de un canal de radio, que comprende:
- recibir un primer mensaje correspondiente a un mensaje de solicitud de acceso aleatorio desde un terminal de usuario incluyendo un preámbulo de acceso aleatorio utilizando un recurso de radio de canal de acceso aleatorio;
- 35
- transmitir (S10) un segundo mensaje correspondiente a un mensaje de respuesta de acceso aleatorio al terminal de usuario indicando un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario que indica una secuencia de cifrado de un conjunto de secuencias de cifrado de enlace ascendente no asignadas específicamente a un terminal de usuario;
- 40
- recibir (S11) a través del recurso de radio identificado un tercer mensaje correspondiente a una transmisión de enlace ascendente planificada desde el terminal de usuario que incluye una identidad de terminal de usuario específica al terminal de usuario al menos dentro de la célula, en el que el mensaje de acceso aleatorio es cifrado utilizando uno de los conjuntos de secuencias de cifrado de enlace ascendente seleccionadas utilizando el identificador de terminal de usuario; y
- 45
- transmitir (S12) un cuarto mensaje correspondiente a un mensaje de resolución de contención al terminal de usuario.
- 6.- Un terminal (20) de usuario para solicitar servicio desde una estación base (18) que tiene un área de célula donde la estación base ofrece servicio de comunicaciones de radio, que comprende circuitería (30) de procesamiento electrónico configurada para:
- 50
- determinar una primera secuencia de cifrado de enlace ascendente en el que dicha primera secuencia de cifrado de enlace ascendente es una secuencia de cifrado específica de acceso aleatorio o específica de célula, y
- 55
- genera un mensaje de acceso aleatorio utilizando la secuencia de cifrado de enlace ascendente de primer tipo determinada, y
- la circuitería (32) de transmisión de radio para transmitir el mensaje de acceso aleatorio a la estación base de radio;
- 60
- la circuitería (36) de recepción de radio para recibir de la estación base de radio una asignación de una segunda secuencia de cifrado de enlace ascendente, en el que dicha segunda secuencia de cifrado de enlace ascendente es una secuencia de cifrado específica de terminal,
- 65
- en el que la circuitería (30) de procesamiento electrónico está configurada para usar la segunda secuencia de cifrado de enlace ascendente para la comunicación posterior con la estación base de radio.

- 5 7.- El terminal de usuario en la reivindicación 6, en el que la primera secuencia de cifrado de enlace ascendente está específicamente asociada con el área de célula de la estación base de radio o un canal de radio de acceso aleatorio asociado a la estación base de radio pero no asignado específicamente a ningún terminal de usuario, y la segunda
- 10 8.- El terminal de usuario de la reivindicación 6, en el que la circuitería de procesamiento electrónico está configurada para cifrar información en el mensaje de acceso aleatorio utilizando la primera secuencia de cifrado de enlace ascendente determinada.
- 15 9.- El terminal de usuario de la reivindicación 8, en el que el transmisor está configurado para modular el mensaje de acceso aleatorio cifrado y mapear el mensaje modulado a un recurso de canal de radio.
- 20 10.- Una estación base (18) de radio para responder a los terminales (20) de usuario que solicitan servicio desde la estación base a través de un canal de radio, que comprende circuitería (40) configurada para:
- 25 recibir un primer mensaje correspondiente a un mensaje de solicitud de acceso aleatorio desde un terminal de usuario que incluye un preámbulo de acceso aleatorio que utiliza un recurso de radio de canal de acceso aleatorio;
- 30 transmitir un segundo mensaje correspondiente a un mensaje de respuesta de acceso aleatorio al terminal de usuario indicando un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario que indica una secuencia de cifrado de un conjunto de secuencias de cifrado de enlace ascendente que no están específicamente asignadas a un terminal de usuario;
- recibir a través del recurso de radio identificado un tercer mensaje correspondiente a una transmisión de enlace ascendente planificada desde el terminal de usuario incluyendo una identidad de terminal de usuario específica al terminal de usuario al menos dentro de la célula, en el que el mensaje de acceso aleatorio es cifrado utilizando uno de los conjuntos de secuencias de cifrado de enlace ascendente seleccionadas utilizando el identificador de terminal de usuario; y
- transmitir un cuarto mensaje correspondiente a un mensaje de resolución de contención al terminal de usuario.

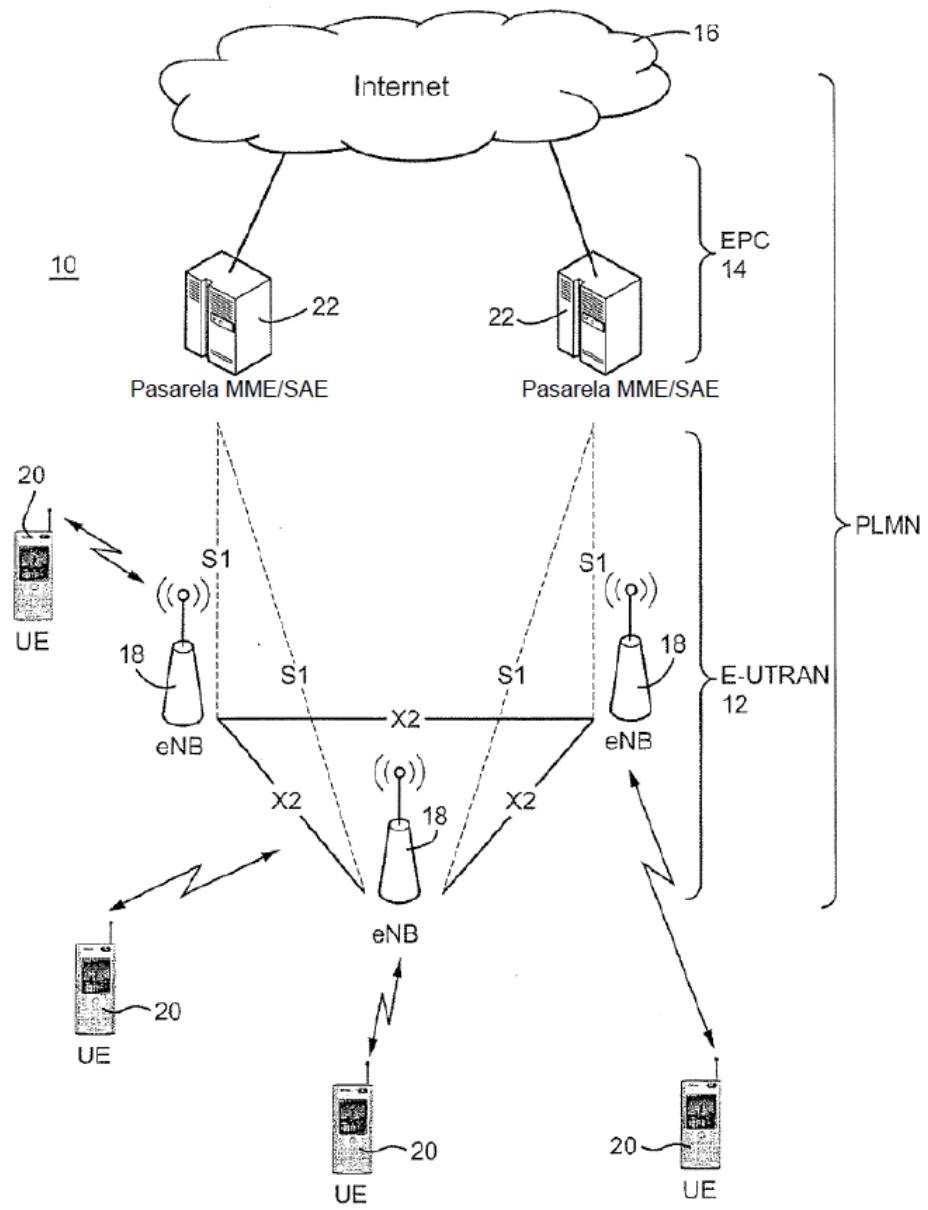
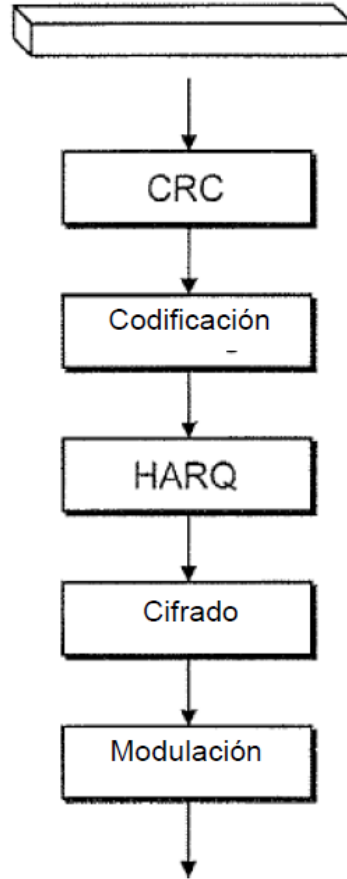


Figura 1



Bloque de transporte con tamaño dinámico  
repartido desde capa MAC



A modulación OFDM de DFTS incluido mapeo a  
recurso de frecuencia asignado

Figura 2

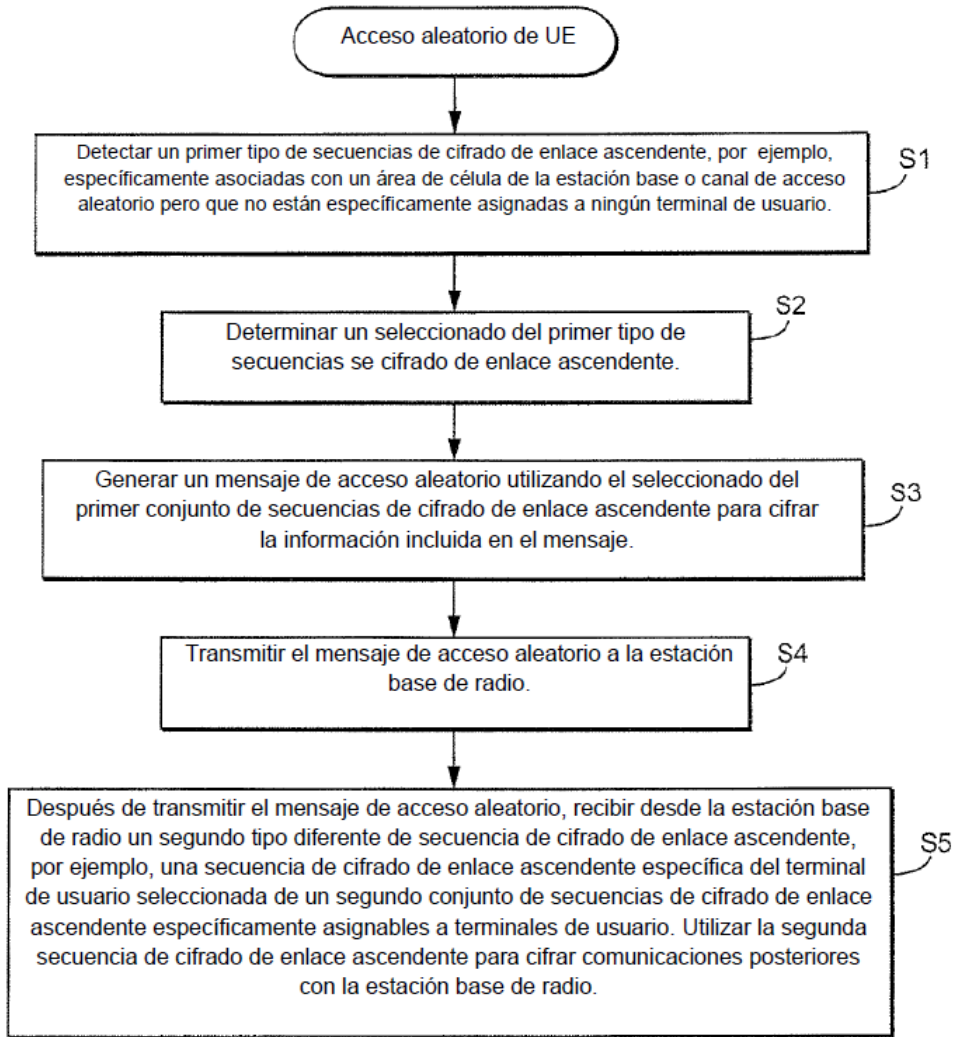


Figura 3

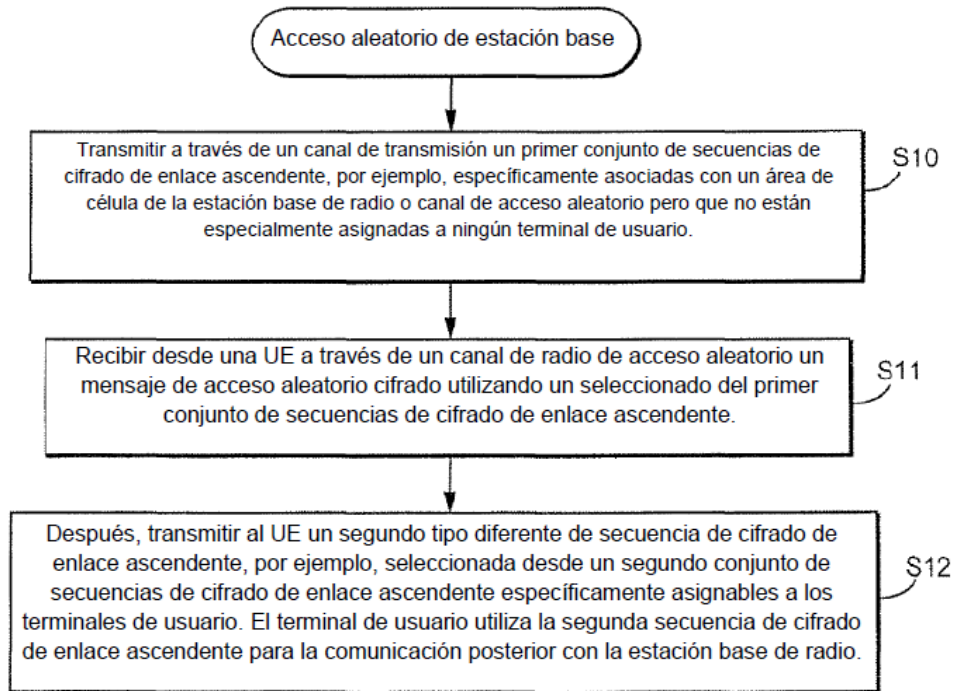


Figura 4

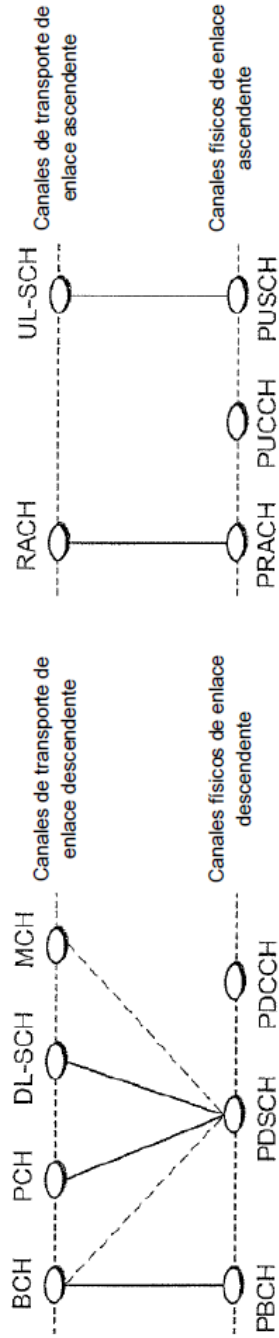


Figura 5A

Figura 5B

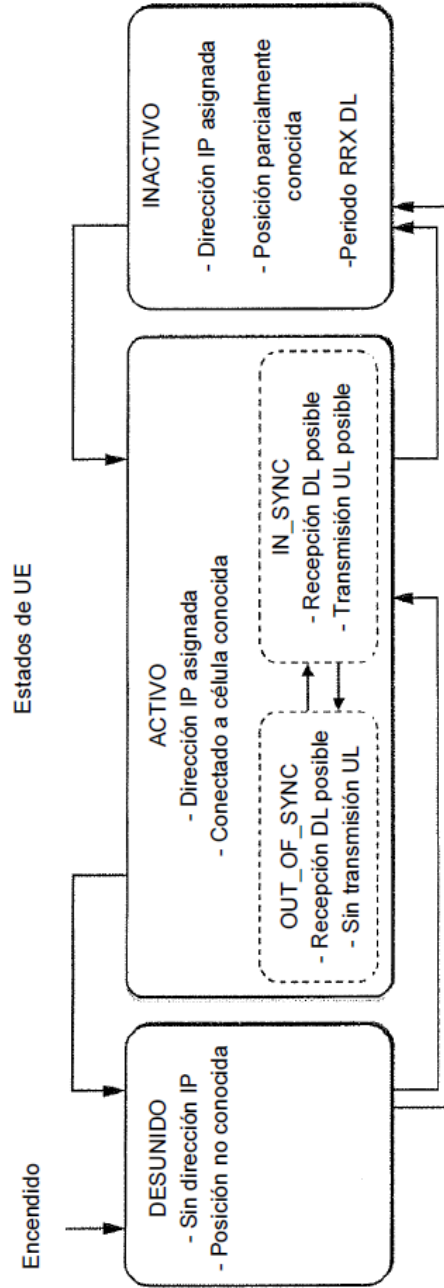


Figura 6

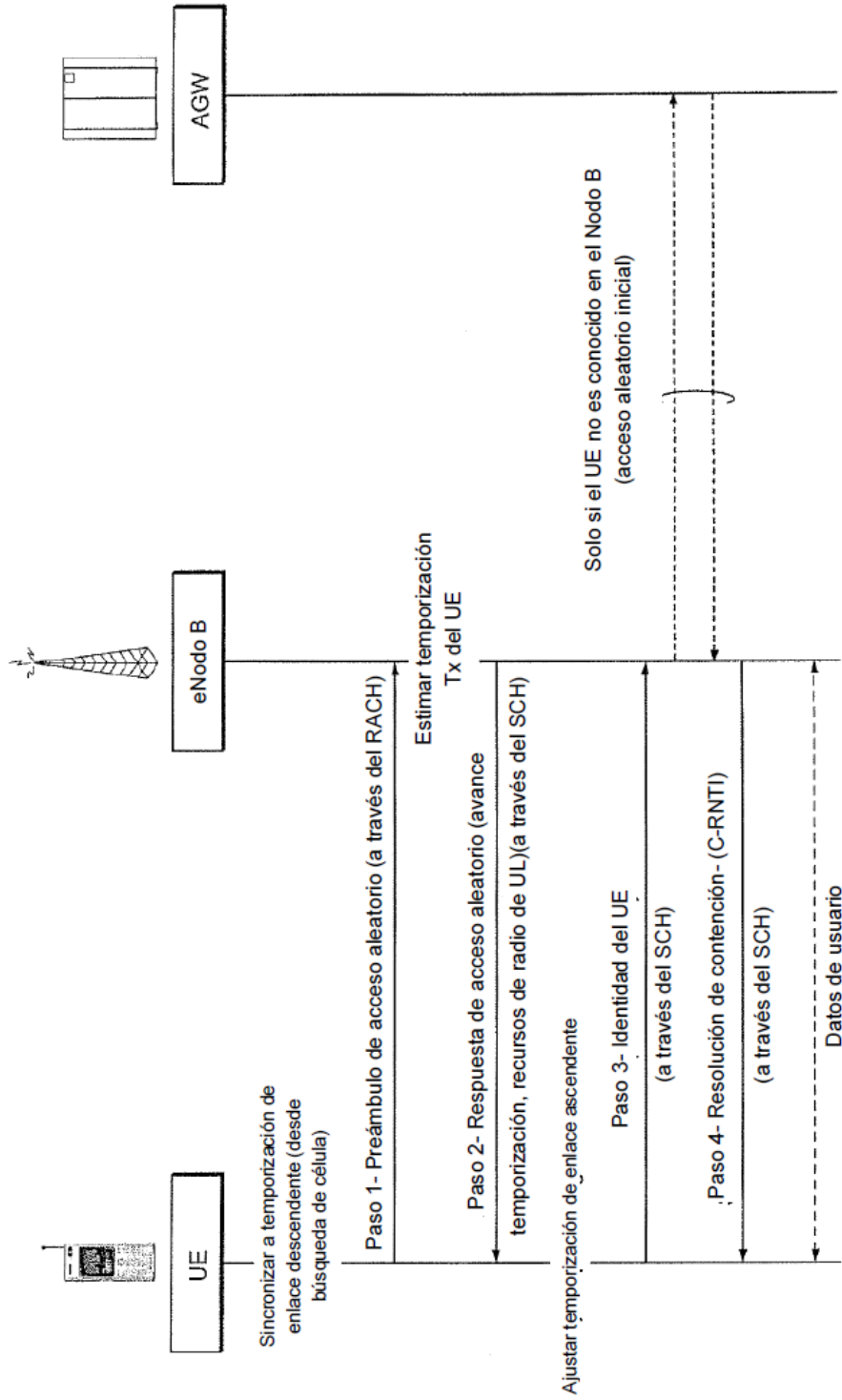


Figura 7

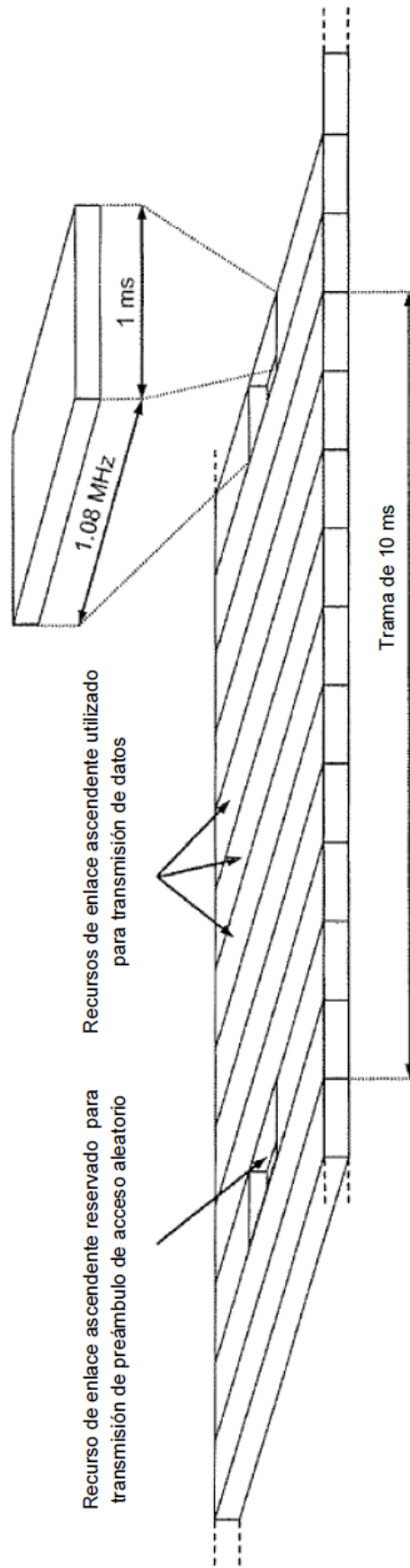


Figura 8

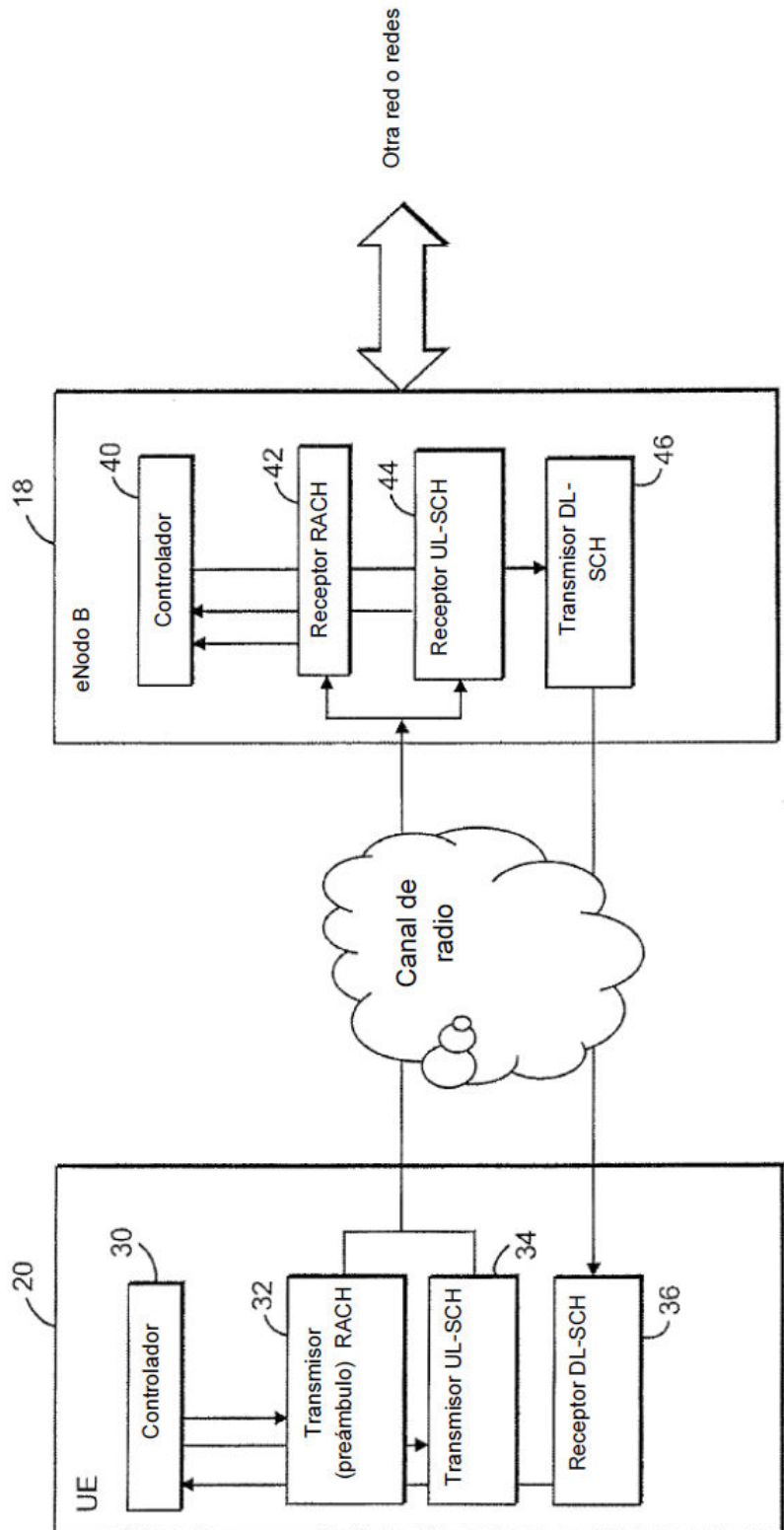


Figura 9