(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 897 125**

(51) Int. CI.:

H04W 74/08 (2009.01)
H04W 76/10 (2008.01)
H04W 74/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.07.2008 E 18208514 (2)**

(97) Fecha y número de publicación de la concesión europea: **01.09.2021 EP 3496503**

(54) Título: **Cifrado del enlace ascendente durante un acceso aleatorio**

(30) Prioridad:

08.08.2007 US 83578207

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.02.2022

(73) Titular/es:

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

(72) Inventor/es:

PARKVALL, STEFAN;
DAHLMAN, ERIK y
TYNDERFELDT, TOBIAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Cifrado del enlace ascendente durante un acceso aleatorio

Campo técnico

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

Antecedentes

El Sistema Universal de Telecomunicaciones Móviles (UMTS) es un sistema de comunicación móvil asíncrono de 3ª Generación (3G) que opera en Acceso Múltiple por División de Código de Banda Ancha (WCDMA) basándose en sistemas Europeos, el Sistema Global para Comunicaciones Móviles (GSM) y los Servicios Generales de Radio por Paquetes (GPRS). La Evolución a Largo Plazo (LTE) de UMTS está siendo desarrollada por el Proyecto de Asociación de 3ª Generación (3GPP) que estandarizó UMTS. Hay muchas especificaciones técnicas alojadas en el sitio web del 3GPP relacionadas con el Acceso Radio Terrestre Universal Evolucionado (E-UTRA) y con la Red de Acceso Radio Terrestre Universal Evolucionada (E-UTRAN), p. ej., el documento TS 36.300 del 3GPP. El objetivo del trabajo LTE es desarrollar un marco de trabajo para la evolución de la tecnología de acceso por radio 3GPP hacia una tecnología de acceso por radio de alta velocidad de datos, baja latencia y optimizada para paquetes. En particular, LTE tiene como objetivo soportar los servicios proporcionados desde el dominio de paquetes conmutados (PS). Un objetivo clave de la tecnología LTE del 3GPP es permitir comunicaciones de paquetes de alta velocidad a aproximadamente 100 Mbps o más.

La Figura 1 ilustra un ejemplo de un sistema 10 de comunicaciones móvil de tipo LTE. Una E-UTRAN 12 incluye un NodoB E-UTRAN (eNodoBs o eNBs) 18 que proporciona terminaciones del protocolo del plano de usuario y del plano de control E-UTRA hacia el equipo 20 de usuario (UE) sobre una interfaz radio. Aunque un eNB es un nodo lógico, a menudo, pero no necesariamente, implementado por una estación base física, el término estación base se utiliza aquí para cubrir, generalmente, tanto los nodos lógicos como los físicos. Un UE se denomina a veces terminal de radio móvil y en un estado inactivo, monitoriza la información del sistema emitida por los eNBs al alcance, para informarse sobre las estaciones base "candidatas" en el área de servicio. Cuando un UE necesita acceso a servicios desde una red de acceso por radio, envía una solicitud sobre un canal de acceso aleatorio (RACH) a un eNB adecuado, normalmente un eNB con las condiciones de radio más favorables. Los eNBs están interconectados entre sí mediante una interfaz X2. Los eNBs también están conectados mediante la interfaz S1 a un Núcleo 14 de Paquetes Evolucionado (EPC) que incluye una Entidad de Gestión de la Movilidad (MME) de una S1-MME y a una Pasarela de Evolución de la Arquitectura del Sistema (SAE) de una S1-U. En este ejemplo, se hace referencia a la pasarela MME/SAE como un solo nodo 22. La interfaz S1 soporta una relación de varios a varios entre las Pasarelas MMEs / SAE y los eNBs. La E-UTRAN 12 y el EPC 14 juntos forman una Red Móvil Terrestre Pública (PLMN). Las pasarelas 22 MMEs / SAE están conectadas, directa o indirectamente, a Internet 16 y a otras redes.

Para permitir el funcionamiento en diferentes asignaciones del espectro, por ejemplo para tener una migración 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 el funcionamiento en un ancho de banda flexible, p. ej., anchos de banda que van desde 1,25 MHz a 20 MHz para transmisiones del enlace descendente desde la red al UE. Tanto los servicios de datos de alta velocidad como los servicios de baja velocidad, como voz, deben ser soportados y, dado que LTE de 3G está diseñado para TCP/IP, es probable que VoIP sea el servicio que transmita la voz.

La transmisión del enlace ascendente LTE se basa en la denominada transmisión de Difusión de la Transformada de Fourier Discreta-OFDM (DFTS-OFDM), un esquema de transmisión de portadora única (SC), de relación de potencia media de pico bajo (PAPR), que permite una asignación de ancho de banda flexible y un acceso múltiple ortogonal no solo en el dominio del tiempo, sino también en el dominio de la frecuencia. Así, el esquema de transmisión del enlace ascendente LTE también se denomina a menudo FDMA de Portadora Única (SC-FDMA).

El procesamiento del canal de transporte del enlace ascendente 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 para el bloque un código de redundancia cíclica (CRC) que se utilizará para la detección de errores en el receptor de la estación base y se adjunta al mismo. A continuación, se realiza la codificación del canal del enlace ascendente mediante un codificador de canal que puede utilizar cualquier técnica de codificación adecuada. En LTE, el código puede ser un código turbo que incluye un intercalador interno basado en Polinomios de Permutación Cuadrática (QPP) para realizar el entrelazado de bloques como parte del turbo-codificador. La Solicitud de Repetición Automática (ARQ) híbrida del enlace ascendente LTE extrae, a partir del bloque de bits codificados entregado por el codificador de canal, el conjunto exacto de bits que se transmitirán en cada instante de transmisión/retransmisión. Un codificador codifica los bits codificados en el enlace ascendente LTE (p. ej., cifrado a nivel de bits) para aleatorizar la interferencia y así garantizar que la ganancia de procesamiento proporcionada por el código del canal pueda utilizarse por completo.

Para lograr esta aleatorización de la interferencia, el cifrado del enlace ascendente es específico del terminal móvil, es decir, diferentes terminales móviles (UEs) utilizan diferentes secuencias de cifrado. El cifrado específico del terminal, también proporciona al programador la libertad para programar 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 celda que están programados 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 del enlace ascendente LTE incluye QPSK, 16QAM, y 64QAM, correspondientes 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, p. ej., una sub-banda 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. Señales de referencia conocidas de antemano tanto por el terminal móvil (UE) como por la estación base (eNodoB) y son utilizadas por el receptor para la estimación del canal y para la demodulación de los símbolos de datos. Pueden asignarse diferentes señales de referencia a un terminal de usuario por razones similares, pueden utilizarse códigos de cifrado específicos del terminal, es decir, para programar de manera inteligente múltiples usuarios en el mismo recurso de tiempo-frecuencia y así realizar la denominada MIMO multiusuario. En el caso de MIMO multiusuario, depende del procesamiento del eNodoB separar las señales transmitidas desde los dos (o más) UEs programados simultáneamente en el mismo recurso de frecuencia en la misma celda. A los terminales programados simultáneamente en el mismo recurso de frecuencia se les asignan normalmente diferentes secuencias de la señal de referencia (p. ej., ortogonales) para que el eNodoB estime los canales de radio para cada uno de esos UEs.

Un requisito básico para cualquier sistema de comunicaciones por radio celular o de otro tipo, es proporcionar a un terminal de usuario la capacidad de solicitar un establecimiento de conexión. Esta capacidad se conoce comúnmente como acceso aleatorio y sirve para dos propósitos principales en LTE, a saber, el establecimiento de la sincronización del enlace ascendente con la temporización de la estación base y el establecimiento de una identidad del terminal de usuario única, p. ej., 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 comunicaciones para distinguir la comunicación del usuario de otras comunicaciones.

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

El documento EP 0 565 507 A2 describe una estación móvil que tiene medios para seleccionar un código de cifrado de una lista de códigos de cifrado disponibles emitidos desde otra estación de radio para generar un mensaje de acceso aleatorio.

Compendio

La tecnología que se describe a continuación facilita un acceso aleatorio por parte de un terminal de usuario con una estación base de radio. Un terminal de usuario determina una de un primer tipo de secuencias de cifrado del enlace ascendente y genera un mensaje de acceso aleatorio utilizando la determinada del primer tipo de secuencias de cifrado del 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 del enlace ascendente. El terminal utiliza ese segundo tipo diferente de secuencia de cifrado del enlace ascendente para la comunicación posterior con la estación base de radio. En una realización de ejemplo no limitante, el primer tipo de secuencias de cifrado del enlace ascendente puede estar asociado, específicamente, con el área de celda de la estación base de radio o con un canal de radio de acceso aleatorio asociado con la estación base de radio, pero no están específicamente asignados a ningún terminal de usuario, y el segundo tipo diferente de secuencia de cifrado del enlace ascendente puede seleccionarse de un segundo conjunto de secuencias de cifrado del enlace ascendente asignables, específicamente, a 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 del enlace ascendente aunque los códigos de cifrado específicos del terminal no puedan ser utilizados en el enlace ascendente, durante el acceso aleatorio, por los terminales de usuario.

El terminal de usuario transmite un primer mensaje de solicitud de acceso aleatorio, que incluye un preámbulo de acceso aleatorio para la estación base de radio, utilizando un recurso de radio del 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 temporal del terminal de usuario. El terminal ajusta una temporización en el terminal de usuario para transmitir señales a la estación base de radio en función de la información recibida en el mensaje de respuesta de acceso aleatorio y, en función de la temporización ajustada, transmite un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad completa del terminal de usuario para la estación base de radio sobre el recurso de radio identificado. El tercer mensaje se cifra utilizando la determinada del primer tipo de secuencia de cifrado del enlace ascendente, se modula, y se mapea a un recurso del canal de radio. El terminal recibe un cuarto mensaje de resolución de disputas de la estación base de radio para completar los procedimientos de acceso aleatorio y seguir las comunicaciones normales.

Varias realizaciones no limitantes mapean el primer conjunto de secuencias de cifrado del 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 del enlace ascendente puede mapearse a las correspondientes secuencias del preámbulo de acceso aleatorio. A continuación, puede seleccionarse una del primer conjunto de secuencias de cifrado del enlace ascendente en función del preámbulo de acceso aleatorio incluido en el primer mensaje de solicitud de acceso aleatorio y en el mapeo. Otro ejemplo mapea el primer conjunto de secuencias de cifrado del enlace ascendente a los identificadores del terminal de usuario correspondientes y selecciona una del primer conjunto de secuencias de cifrado del enlace ascendente basándose en el identificador del terminal de usuario incluido en el segundo mensaje de respuesta de acceso aleatorio y en el mapeo. Un tercer ejemplo mapea el primer conjunto de secuencias de cifrado del enlace ascendente a los recursos de radio correspondientes utilizados para transmitir el mensaje de solicitud de acceso aleatorio y selecciona una del primer conjunto de secuencias de cifrado del enlace ascendente en función del 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 para la estación base de radio y el mapeo.

El enfoque de la secuencia de cifrado de dos tipos también puede utilizarse para señales de referencia incrustadas en los mensajes de acceso aleatorio del enlace ascendente enviados a la estación base, que son utilizados por la estación base para estimar el canal del enlace ascendente, p. ej., con fines de ecualización, etc. Una de un primer conjunto de secuencias de referencia del enlace ascendente, p. ej., secuencias de referencia del enlace ascendente asociadas, específicamente, con el área de celda de una estación base de radio o con un canal de acceso aleatorio, pero que no están asignadas, específicamente, a ningún terminal de usuario. Se genera un mensaje de acceso aleatorio utilizando la secuencia seleccionada del primer conjunto de secuencias de cifrado del enlace ascendente y la secuencia seleccionada del primer conjunto de secuencias de referencia del enlace ascendente. El terminal de usuario transmite el mensaje de acceso aleatorio a la estación base de radio. Después, la estación base informa al terminal de usuario de un segundo tipo diferente de secuencia de referencia para utilizar en comunicaciones del enlace ascendente posteriores, p. ej., un número de referencia asignado, específicamente, a ese terminal de usuario.

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

Breve descripción de los dibujos

La Figura 1 es un sistema de comunicaciones por radio móvil LTE de ejemplo;

La Figura 2 es un diagrama de flujo que ilustra procedimientos no limitantes, de ejemplo, para preparar un bloque de transporte entregado desde la capa de acceso al medio de un terminal de usuario para su transmisión sobre la interfaz radio a la red en un sistema de comunicaciones por radio móvil LTE;

La Figura 3 es un diagrama de flujo que ilustra procedimientos no limitantes, de ejemplo, para que un terminal de usuario realice un acceso aleatorio a la red de radio;

La Figura 4 es un diagrama de flujo que ilustra procedimientos no limitantes, de ejemplo, para que una estación base reciba y procese un acceso aleatorio del terminal de usuario a la red de radio;

Las Figuras 5A y 5B ilustran un mapeo entre los canales de transporte y físico en el enlace descendente y en el enlace ascendente, respectivamente;

La Figura 6 es un diagrama que ilustra tres estados básicos de un terminal de usuario;

La Figura 7 es un diagrama de señalización que ilustra un procedimiento de acceso aleatorio de ejemplo no limitante;

La Figura 8 ilustra un ejemplo no limitante de una transmisión del preámbulo de acceso aleatorio; y

La Figura 9 es un diagrama de bloques de función no limitante, de ejemplo, de un terminal de usuario y de una estación base eNodo B.

Descripción detallada

En la siguiente descripción, con fines explicativos y no de limitación se establecen detalles específicos, como nodos particulares, entidades funcionales, técnicas, protocolos, estándares, etc., para proporcionar una comprensión de la tecnología descrita. En otros casos, se omiten descripciones detalladas de métodos, dispositivos, técnicas, etc., bien conocidos para no oscurecer 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 se pueden implementar utilizando circuitos hardware individuales, utilizando programas software y datos junto con un microprocesador adecuadamente programado u ordenador de propósito general, utilizando un circuito integrado específico de aplicaciones (ASIC), matrices lógicas programables, y/o utilizando uno o más procesadores de señales digitales (DSPs).

Será evidente para un experto en la técnica que pueden ponerse en práctica otras realizaciones aparte de los detalles específicos que se describen a continuación. La tecnología se describe en el contexto de un sistema UMTS del 3GPP evolucionado, como LTE, para proporcionar un ejemplo y un contexto no limitante para su explicación. Véase, por ejemplo, el diagrama del sistema LTE mostrado en la Figura 1. Pero esta tecnología no se limita a LTE y puede utilizarse en cualquier sistema de comunicaciones por radio moderno. Además, el enfoque siguiente, que emplea dos tipos diferentes de secuencias de cifrado, una para fines de acceso aleatorio y otra para comunicaciones después de que se complete el acceso aleatorio, también puede aplicarse a señales de referencia de estimación del canal conocidas (a veces llamadas 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, a menudo se hace referencia a un equipo de usuario (UE), sin limitación, como un terminal de usuario o un terminal móvil, y se hace referencia a un eNodoB para utilizar el término, más general y familiar, de estación base.

La Figura 3 es un diagrama de flujo que ilustra procedimientos no limitantes, de ejemplo, para que un terminal de usuario realice un acceso aleatorio a la red de radio utilizando un código de cifrado del enlace ascendente que generalmente está disponible para todos los terminales de usuario que deseen acceder aleatoriamente al servicio en una celda particular. El terminal de usuario detecta un primer tipo de secuencias de cifrado del enlace ascendente, p. ej., secuencias de cifrado del enlace ascendente asociadas, específicamente, con un área de celda de la estación base de radio o con un canal de acceso aleatorio, pero que no están asignadas, específicamente, a ningún terminal de usuario (paso S1). Se determina una secuencia seleccionada del primer tipo de secuencias de cifrado del enlace ascendente (paso S2), y se genera un mensaje de acceso aleatorio usando la secuencia seleccionada del primer tipo de secuencias de cifrado del 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 del enlace ascendente, p. ej., una secuencia de cifrado del enlace ascendente seleccionada de un segundo conjunto de secuencias de cifrado del enlace ascendente asignables, específicamente, a terminales de usuario (paso S5). El terminal de usuario utiliza el segundo tipo de secuencia de cifrado del enlace ascendente para la comunicación posterior con la estación base de radio. Pueden utilizarse procedimientos similares para señales de referencia del enlace ascendente conocidas.

La Figura 4 es un diagrama de flujo que ilustra los procedimientos equivalentes no limitantes, de ejemplo, 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 no específicos del terminal. La estación base emite, implícita o explícitamente, sobre un canal de difusión, p. ej., BCH, su conjunto de secuencias de preámbulos y de cifrado del enlace ascendente (paso S10). Si la estación base no emite explícitamente la secuencia de cifrado a utilizar, la identidad de la celda a partir de la cual puede derivarse la secuencia de cifrado a utilizar, por ejemplo, a través de un mapeo entre la secuencia y el identificador de celda. Las secuencias de cifrado del enlace ascendente pueden estar, por ejemplo, asociadas específicamente con un área de celda de la estación base de radio o con un canal de acceso aleatorio y no están asignadas, específicamente, a ningún terminal de usuario. La estación base espera entonces recibir un primer mensaje de solicitud de acceso aleatorio de un terminal de usuario que incluye uno de los preámbulos de la estación base. En respuesta, la estación base transmite 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 del terminal de usuario. Un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad del terminal de usuario se descifra utilizando la secuencia seleccionada del primer conjunto de secuencias de cifrado del enlace ascendente (paso S11). Después, la estación base transmite al terminal de usuario un cuarto mensaje que incluye un segundo tipo diferente de secuencia de cifrado del enlace ascendente seleccionada de un segundo conjunto de secuencias de cifrado del enlace ascendente, p. ej., secuencias de cifrado del enlace ascendente que se pueden asignar, 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. Pueden aplicarse procedimientos similares para señales de referencia del enlace ascendente conocidas.

Para comprender mejor el siguiente ejemplo y procedimiento de acceso aleatorio LTE no limitante, se hace referencia a las Figuras 5A y 5B que ilustran un mapeo entre los canales de transporte y físico en el enlace descendente y en el enlace ascendente, respectivamente. Los siguientes son canales de transporte del enlace descendente: el canal de difusión (BCH), el canal de búsqueda (PCH), el canal compartido del enlace descendente (DL-SCH), y el canal de multidifusión (MCH). El BCH se mapea al Canal de Difusión Físico (PBCH), y el PCH y el DL-SCH se mapean al Canal Compartido del Enlace Descendente Físico (PDSH). Los canales de transporte del enlace ascendente incluyen el canal de acceso aleatorio (RACH) y el canal compartido del enlace ascendente (UL-SCH). El RACH se mapea al canal de Acceso Aleatorio Físico (PRACH), y el UL-SCH se mapea al Canal Compartido del Enlace Ascendente Físico (PUSCH).

En LTE, como en otros sistemas de comunicaciones por radio móviles, un terminal móvil puede estar en varios estados operativos 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 al terminal móvil. Antes de que pueda tener lugar cualquier otra comunicación entre el terminal móvil y la red, el terminal móvil debe registrarse en la red utilizando el procedimiento de acceso aleatorio para ingresar al estado LTE_ACTIVE. El estado LTE_DETACHED es principalmente un estado utilizado en el encendido. Una vez que el terminal móvil se registra en la red, normalmente se encuentra en uno de los otros estados: LTE_ATIVE o LTE_IDLE.

LTE_ACTIVE es el estado utilizado cuando el terminal móvil está activo transmitiendo y recibiendo datos. En este estado, el terminal móvil está conectado a una celda específica dentro de la red. Se han asignado al terminal móvil una o varias direcciones de paquetes de datos del Protocolo de Internet (IP) o de otro tipo, así como una identidad del terminal, un Identificador Temporal de Red de Radio Celular (C-RNTI), que se utiliza con fines de señalización entre terminal y la red. El estado LTE_ACTIVE incluye dos sub-estados, IN_SYNC y OUT_OF_SYNC, dependiendo de si el enlace ascendente está sincronizado con la red o no. Siempre que el enlace ascendente esté en IN_SYNC, son posibles las transmisiones del enlace ascendente de datos de usuario y la señalización de control de la capa inferior. Si no ha tenido lugar una transmisión del enlace ascendente dentro de una ventana de tiempo determinada, el enlace ascendente se declara fuera de sincronización, en cuyo caso, el terminal móvil debe realizar un procedimiento de acceso aleatorio para restaurar la sincronización del 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 un acceso aleatorio para pasar a LTE_ACTIVE. El terminal móvil mantiene su(s) dirección(es) IP y otra información interna para pasar rápidamente a LTE_ACTIVE cuando sea necesario. La posición del terminal móvil es parcialmente conocida por la red, de manera que la red sabe, al menos, el grupo de células en las que se va a realizar la búsqueda del terminal móvil.

Un ejemplo de procedimiento de acceso aleatorio no limitante se ilustra en la Figura 7 e incluye cuatro pasos denominados pasos 1-4 con cuatro mensajes de señalización asociados denominados mensajes 1-4. La estación base transmite un conjunto de preámbulos asociados con esa estación base, información de recursos RACH, y otra información en un mensaje de difusión enviado regularmente sobre un canal de difusión que los terminales móviles activos escanean regularmente. En el paso uno, después de que el terminal de usuario reciba y decodifique la información emitida por la estación base (eNodoB), selecciona uno de los preámbulos de acceso aleatorio de la estación base y lo transmite sobre el RACH. La estación base monitorea el RACH y detecta el preámbulo que permite a la estación base estimar la temporización de transmisión del terminal de usuario. La sincronización del enlace ascendente es necesaria para permitir que el terminal transmita datos del enlace ascendente a la estación base.

El preámbulo de acceso aleatorio incluye una secuencia conocida, seleccionada aleatoriamente por el terminal móvil de un conjunto de secuencias de preámbulo conocidas disponibles para propósitos de acceso aleatorio con una estación base particular. Cuando se realiza un intento de acceso aleatorio, el terminal selecciona una secuencia de preámbulo al azar del conjunto de secuencias de preámbulo asignado a la celda a la que el terminal está intentando 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 será muy probable que la estación base detecte la solicitud de acceso aleatorio. El preámbulo es transmitido por un terminal de usuario en un recurso del canal de radio, p. ej., un recurso de tiempo/frecuencia, asignado para propósitos de acceso aleatorio, p. ej., un RACH.

La Figura 8 ilustra conceptualmente una transmisión del preámbulo de acceso aleatorio según la especificación LTE al momento de escribir este artículo. Un ejemplo no limitante para la generación de preámbulos adecuados se basa en secuencias de Zadoff-Chu (ZC) y secuencias cíclicas desplazadas de las mismas. Las secuencias de Zadoff-Chu también pueden utilizarse, por ejemplo, para crear las señales de referencia del enlace ascendente incluidas en cada trama de datos para fines de estimación del canal.

Un terminal de usuario que lleva a cabo un intento de acceso aleatorio ha obtenido, antes de la transmisión del preámbulo, la sincronización del enlace descendente a partir de un procedimiento de búsqueda de celda utilizando la información de temporización emitida por la estación base. Pero como se explicó anteriormente, la temporización del enlace ascendente aún no está establecida. El inicio de una trama de transmisión del enlace ascendente en el terminal se define en relación con el inicio de la trama de transmisión del enlace descendente en el terminal. Debido al retardo

de propagación entre la estación base y el terminal, la transmisión del enlace ascendente se retrasará en relación con la temporización de la transmisión del 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 correspondiente al doble de la distancia entre la estación base y el terminal. Para tener en cuenta esta incertidumbre y para evitar interferencias con subtramas posteriores que no se utilizan para el acceso aleatorio, se utiliza un tiempo de guarda.

Volviendo al segundo paso de señalización del 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 del 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 la temporización del enlace ascendente o un comando de avance de tiempo calculado por la estación base después de procesar el preámbulo de acceso aleatorio recibido, una concesión de planificación que indica los recursos que el terminal de usuario utilizará para la transmisión del mensaje en el tercer mensaje enviado desde el terminal móvil a la estación base, y una identidad temporal del terminal de usuario utilizada para la comunicación adicional entre el terminal de usuario y la estación base. Después de completar el paso 2, el terminal de usuario está sincronizado en 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 los múltiples terminales móviles pueden combinarse en una única transmisión. Por lo tanto, el mensaje 2 de respuesta de solicitud de acceso aleatorio se programa en el DL-SCH y se indica en el Canal Físico de Control del Enlace Descendente (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 programados del enlace ascendente, asignados en el mensaje 2 de respuesta de acceso aleatorio, y sincronizados en el enlace ascendente. La transmisión del mensaje del enlace ascendente en el paso 3 de la misma manera que los datos del enlace ascendente programados "normales", es decir, en el UL-SCH, en lugar de adjuntarlo al preámbulo en el primer paso, es beneficioso por varias razones. Primera, la cantidad de información transmitida en ausencia de sincronización del enlace ascendente debe minimizarse ya que la necesidad de un tiempo de guarda grande hace que dichas transmisiones sean relativamente costosas. En segundo lugar, la utilización de un esquema de transmisión del enlace ascendente "normal" para la transmisión de mensajes permite ajustar el tamaño de la concesión y el esquema de modulación, por ejemplo, a diferentes condiciones de radio. Tercera, permite ARQ híbrido con una combinación suave para el mensaje del enlace ascendente que puede ser valiosa, especialmente en escenarios de cobertura limitada, ya que permite depender de una o varias retransmisiones para acumular suficiente energía para la señalización del enlace ascendente a fin de garantizar una probabilidad suficientemente alta de transmisión exitosa. El terminal móvil transmite su identidad temporal de terminal móvil, p. ej., 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, p. ej., si es conocido previamente por la red o no.

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

En el paso 4, se transmite un mensaje de resolución de disputas desde la estación base al terminal en el DL-SCH. Este paso resuelve la disputa en caso de que múltiples terminales intentaran acceder al sistema en el mismo recurso, identificando que 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 temporal del terminal de usuario. Por tanto, en el paso 4, cada terminal que recibe el mensaje del 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 observe una coincidencia entre la identidad recibida en el cuarto paso y la identidad transmitida como parte del tercer paso determina que el procedimiento de acceso aleatorio es exitoso. Si el terminal aún no tiene asignado un C-RNTI, la identidad temporal del segundo paso se promueve al C-RNTI; de lo contrario, el terminal de usuario mantiene su C-RNTI ya asignado. Los terminales que no encuentren una coincidencia con la identidad recibida en el cuarto paso deben reiniciar el procedimiento de acceso aleatorio desde el primer paso.

Como se explicó anteriormente, la identidad del terminal de usuario incluida en el mensaje 3 se utiliza como parte del mecanismo de resolución de disputas en el cuarto paso. Continuando en el ejemplo no limitante de LTE, si el terminal de usuario está en el estado LTE_ACTIVE, es decir, está conectado a una celda conocida y, por lo tanto, tiene un C-RNTI asignado, este C-RNTI se utiliza como la identidad del terminal en el mensaje del enlace ascendente. De lo

contrario, se utiliza un identificador del terminal de la red central, y la estación base necesita involucrar a la red central antes de responder al mensaje del enlace ascendente en el paso tres.

En este ejemplo de LTE no limitante, solo el primer paso utiliza el procesamiento de capa física diseñado específicamente para el acceso aleatorio. Los últimos tres pasos utilizan el mismo procesamiento de capa física que para la transmisión de datos del enlace ascendente y 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 una alta capacidad, es deseable beneficiarse de estas características también al intercambiar mensajes de acceso aleatorio.

En el contexto LTE no limitante de ejemplo, el terminal de usuario aplica los pasos de procesamiento general descritos en la Figura 2, incluyendo CRC, codificación, HARQ, cifrado, modulación y modulación DFT-S-OFDM al mensaje 3 en la Figura 7 y en las transmisiones del enlace ascendente posteriores desde ese terminal de usuario a la estación base (no hay cifrado en el mensaje inicial de acceso aleatorio del enlace ascendente en el paso 1). Las diferentes secuencias de cifrado del enlace ascendente en el terminal dependen del tipo de transmisión del enlace ascendente. Para el mensaje 3 de acceso aleatorio, se utiliza un primer tipo de secuencia de cifrado, p. ej., un código de cifrado específico de la celda o específico del canal de acceso aleatorio. 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, p. ej., un código de cifrado específico del terminal. Se puede utilizar un enfoque similar de dos tipos para las señales de referencia del enlace ascendente utilizadas por la estación base para la estimación del canal: un primer tipo, p. ej., una señal de referencia específica de la celda o del acceso aleatorio, para el mensaje 3 de acceso aleatorio, seguido de un segundo tipo, p. ej., una secuencia de la señal de referencia del enlace ascendente asociada o asignada a una estación base para seguir las transmisiones de datos "normales".

Cuando la estación base asigna una secuencia de cifrado y/o una secuencia de referencia al terminal móvil, esa secuencia de cifrado específica del terminal y/o la secuencia de referencia se utiliza(n) para todas las transmisiones de datos del enlace ascendente posteriores para esa conexión del enlace ascendente en particular. La secuencia de cifrado y/o la secuencia de referencia que se utilizará puede configurarse explícitamente en el terminal móvil o vincularse a la identidad del terminal (p. ej., un C-RNTI) que la estación base asigna a un terminal móvil.

En lo anterior, el terminal de usuario utiliza una secuencia de cifrado específica de la celda para cifrar el mensaje 3 porque antes de realizar el acceso aleatorio, el terminal de usuario ha decodificado la información de difusión de la estación base/celda y, por lo tanto, conoce la identidad de la celda a la que está accediendo, los preámbulos de acceso aleatorio asociados con esa celda, y las secuencias de cifrado específicas de la celda y/o los números de referencia. Siempre que a múltiples terminales que realizan acceso aleatorio al mismo tiempo se les asignen diferentes recursos de tiempo/frecuencia para su respectivo mensaje 3 de acceso aleatorio del enlace ascendente, no habrá interferencias entre estos usuarios y la falta de aleatorización entre usuarios no es un problema.

En una realización no limitante, 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 conocen el preámbulo utilizado para el mensaje de solicitud de acceso aleatorio enviado en el paso 1 para cuando el mensaje 3 se va a transmitir, ambos saben qué secuencia de cifrado utilizar.

En otra realización no limitante, la estación base asigna la secuencia de cifrado para que el terminal de usuario la 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 puede hacerse estableciendo un mapeo de uno a uno entre el identificador temporal del usuario enviado en el mensaje 2, p. ej., un C-RNTI temporal, y la secuencia de cifrado a utilizar.

En otra realización no limitante, vincula la secuencia de cifrado que será utilizada por el terminal de usuario para cifrar el mensaje 3 con el recurso(s) de tiempo-frecuencia utilizado(s) 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/los mismo(s) recurso(s) de tiempo-frecuencia. Pero siempre que a todos esos terminales se les asignen diferentes recursos de tiempo/frecuencia para su propio mensaje 3 de acceso aleatorio, no habrá interferencias entre estos usuarios y la falta de aleatorización entre usuarios no es un problema.

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

Puede haber situaciones en las que al terminal de usuario ya se le haya asignado una identidad, pero aún necesitará realizar un acceso aleatorio. Un ejemplo es cuando el terminal se registra en 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 puede utilizarse 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, es necesario utilizar una secuencia de cifrado asociada a la celda en lugar de una secuencia de cifrado obsoleta específica del terminal.

En consecuencia, 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, lo que mejora el rendimiento de transmisión del enlace ascendente y proporciona flexibilidad adicional en el diseño de la planificación.

Aunque se han mostrado y descrito en detalle varias realizaciones, las reivindicaciones no se limitan a ninguna realización o ejemplo particular. Por ejemplo, aunque principalmente descrito en términos de secuencias de cifrado, el enfoque de dos tipos descrito para secuencias de cifrado de acceso aleatorio también puede utilizarse para determinar secuencias de la señal de referencia enviadas en cada trama del enlace ascendente que son utilizadas por el receptor de la estación base para fines de estimación del canal del enlace ascendente. Nada de la descripción anterior debe interpretarse como que implica que cualquier elemento, paso, rango o función en particular sea esencial, de manera que deba incluirse en el alcance de las reivindicaciones. El alcance de la materia patentada está definido únicamente por las reivindicaciones. El alcance de la protección legal está definido por las palabras mencionadas en las reivindicaciones permitidas.

Además, no es necesario que un dispositivo o método aborde todos y cada uno de los problemas que se pretenden resolver mediante la presente invención, para que quede abarcado por las presentes reivindicaciones.

Además, ninguna realización, característica, componente, o paso en esta especificación está dedicada al público independientemente de si la realización, característica, componente o paso se menciona en las reivindicaciones.

REIVINDICACIONES

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

recibir un mensaje de respuesta de acceso aleatorio de una estación base de radio, en donde el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador del terminal de usuario que indica una secuencia de cifrado que no está asignada específicamente a un terminal de usuario, en donde el mensaje de respuesta de acceso aleatorio se recibe utilizando una identidad común predefinida asociada con un preámbulo transmitido por el terminal de usuario;

transmitir un mensaje 3 a la estación base de radio, en donde el mensaje 3 incluye una identidad del terminal de usuario, y en donde el mensaje 3 se transmite sobre el recurso de radio identificado, y en donde el mensaje 3 se cifra utilizando una secuencia de cifrado del enlace ascendente en función del identificador del terminal de usuario incluido en el mensaje de respuesta de acceso aleatorio;

recibir un mensaje de la estación base de radio, que incluye la identidad del terminal de usuario; y

transmitir una transmisión de datos posterior cifrada con una secuencia de cifrado del enlace ascendente, asignada específicamente al terminal de usuario, en función de la identidad del terminal de usuario.

2. El método según la reivindicación 1, que comprende además transmitir un preámbulo de acceso aleatorio utilizando un recurso de radio del canal de acceso aleatorio para una estación base de radio.

3. El método según la reivindicación 1, en donde el preámbulo de acceso aleatorio se transmite sobre un canal de acceso aleatorio y en donde el mensaje 3 se transmite sobre un canal compartido del enlace ascendente.

4. El método según cualquiera de las reivindicaciones 1-3, en donde el mensaje de respuesta de acceso aleatorio indica además un cambio de temporización y en donde el método comprende además:

ajustar una temporización en el terminal de usuario para transmitir señales a la estación base de radio en función del cambio de temporización recibido en el mensaje de respuesta de acceso aleatorio; y

en donde el mensaje 3 se transmite en función de la temporización ajustada.

5. El método según cualquiera de las reivindicaciones 1-4, en donde la secuencia de cifrado del enlace ascendente, en función del identificador del terminal de usuario, tiene un mapeo de uno a uno entre el identificador del terminal de usuario y la secuencia de cifrado del enlace ascendente.

6. Un método implementado en una estación base de radio para responder a terminales de usuario que solicitan servicio desde la estación base de radio sobre un canal de radio, que comprende:

transmitir un mensaje de respuesta de acceso aleatorio al terminal de usuario, en donde el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador del terminal de usuario, en donde el identificador del terminal de usuario indica una secuencia de cifrado del enlace ascendente que no está específicamente asignada a un terminal de usuario;

recibir sobre el recurso de radio identificado un mensaje 3 del terminal de usuario que incluye una identidad del terminal de usuario, en donde el mensaje 3 se cifra con una secuencia de cifrado del enlace ascendente como se indica en el mensaje de respuesta de acceso aleatorio;

transmitir un mensaje al terminal de usuario que incluye la identidad del terminal de usuario; y

recibir una transmisión de datos posterior del terminal de usuario cifrada con una secuencia de cifrado del enlace ascendente, asignada específicamente al terminal de usuario, en función de la identidad del terminal de usuario.

7. El método según la reivindicación 6, que comprende además recibir un preámbulo de acceso aleatorio sobre un recurso de radio del canal de acceso aleatorio de un terminal de usuario.

8. El método según la reivindicación 7, en donde el preámbulo de acceso aleatorio se recibe sobre canal de acceso aleatorio y en donde el mensaje 3 se recibe sobre un canal compartido del enlace ascendente.

9. El método según cualquiera de las reivindicaciones 6-8, en donde el mensaje de respuesta de acceso aleatorio indica además un cambio de temporización.

10. Un terminal de usuario para solicitar servicio de una estación base de radio, comprendiendo el terminal de usuario:

un receptor de radio configurado para recibir un mensaje de respuesta de acceso aleatorio de la estación base de radio, en donde el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador del terminal de usuario que indica una secuencia de cifrado que no está específicamente

asignada a un terminal de usuario, en donde el receptor de radio se configura además para recibir el mensaje de respuesta de acceso aleatorio utilizando una identidad común predefinida asociada con un preámbulo transmitido por el terminal de usuario;

en donde un transmisor de radio se configura para transmitir un mensaje 3 a la estación base de radio, en donde el mensaje 3 incluye una identidad del terminal de usuario, el mensaje 3 se transmite sobre el recurso de radio identificado, y el mensaje 3 se cifra utilizando una secuencia de cifrado del enlace ascendente, en función del identificador del terminal de usuario incluido en el mensaje de respuesta de acceso aleatorio;

en donde el receptor de radio se configura para recibir un mensaje de la estación base de radio, que incluye la identidad del terminal de usuario; y

en donde el transmisor de radio se configura para transmitir una transmisión de datos posterior en el enlace ascendente cifrada con una secuencia de cifrado del enlace ascendente, asignada específicamente al terminal de usuario, en función de la identidad del terminal de usuario.

11. El terminal de usuario según la reivindicación 10, en donde el terminal de usuario comprende además un transmisor de radio configurado para transmitir un preámbulo de acceso aleatorio utilizando un recurso de radio del canal de acceso aleatorio para la estación base de radio;

12. El terminal de usuario en la reivindicación 11, en donde el transmisor de radio se configura para transmitir el preámbulo de acceso aleatorio sobre un canal de acceso aleatorio y el mensaje 3 sobre un canal compartido del enlace ascendente.

13. El terminal de usuario según cualquiera de las reivindicaciones 10-12, en donde el mensaje de respuesta de acceso aleatorio indica además un cambio de temporización, y en donde el circuito de procesamiento electrónico se configura para ajustar una temporización en el terminal de usuario, para transmitir señales a la estación base de radio en función del cambio de temporización recibido en el mensaje de respuesta de acceso aleatorio por radio, y en donde el transmisor de radio se configura para transmitir el mensaje 3 en función de la temporización ajustada.

14. El terminal de usuario según cualquiera de las reivindicaciones 10-13, en donde el circuito de procesamiento electrónico se configura para determinar la secuencia de cifrado del enlace ascendente estableciendo un mapeo de uno a uno entre el identificador del terminal de usuario y la secuencia de cifrado del enlace ascendente.

15. Una estación base de radio configurada para asociarse con una celda para responder a terminales de usuario que solicitan servicio de la estación base de radio sobre un canal de radio, que comprende un circuito configurado para:

transmitir un mensaje de respuesta de acceso aleatorio al terminal de usuario, en donde el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador del terminal de usuario, y en donde el identificador del terminal de usuario indica una secuencia de cifrado del enlace ascendente que no está específicamente asignada al terminal de usuario, en donde el mensaje de respuesta de acceso aleatorio se transmite utilizando una identidad común predefinida asociada con un preámbulo recibido por la estación base de radio;

recibir del terminal de usuario, sobre el recurso de radio identificado, un mensaje 3 cifrado con la secuencia de cifrado del enlace ascendente, en donde el mensaje 3 incluye una identidad del terminal de usuario;

transmitir un mensaje al terminal de usuario, que incluye la identidad del terminal de usuario; y

recibir una transmisión de datos posterior del terminal de usuario cifrada con una secuencia de cifrado del enlace ascendente, específicamente asignada al terminal de usuario, en función de la identidad del terminal de usuario.

16. La estación base de radio según la reivindicación 15, configurada además para recibir un preámbulo de acceso aleatorio sobre un recurso de radio del canal de acceso aleatorio de un terminal de usuario.

17. La estación base de radio según la reivindicación 16, en donde el circuito se configura para recibir el preámbulo de acceso aleatorio sobre un canal de acceso aleatorio y el mensaje 3 sobre un canal compartido del enlace ascendente.

18. La estación base de radio según cualquiera de las reivindicaciones 15-17, en donde el mensaje de respuesta de acceso aleatorio indica además un cambio de temporización.

19. Un método o dispositivo según cualquiera de las reivindicaciones precedentes, en donde el identificador del terminal de usuario es un Identificador Temporal de la Red de Radio Celular Temporal y/o en donde la identidad del terminal de usuario es un Identificador Temporal de la Red de Radio Celular.

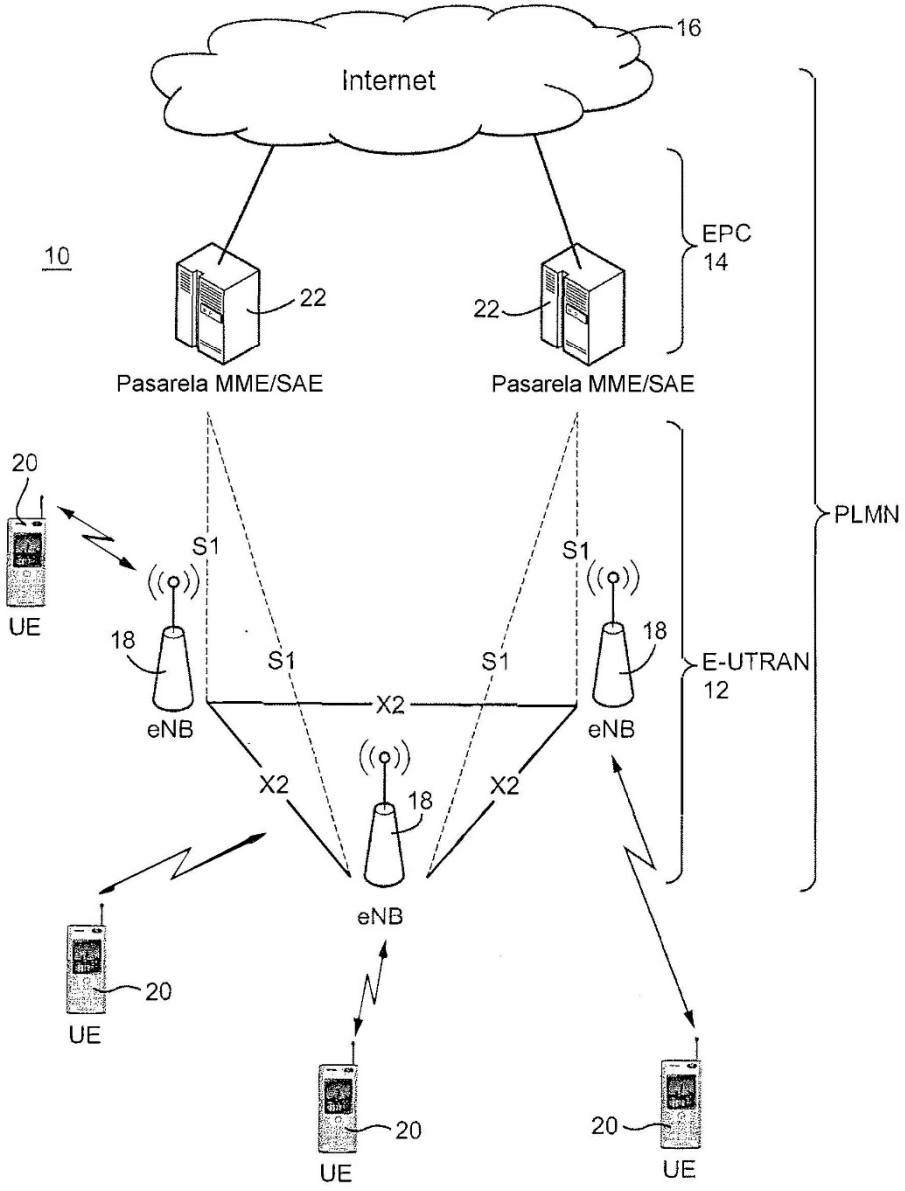
16
Internet
EPC
14
10
22
22
Pasarela MME/SAE
Pasarela MME/SAE
20
PLMN
S1
S1
UE
18
S1
S1
18
E-UTRAN
12
X2
eNB
eNB
X2
X2
18
eNB
20
UE
20
UE
20
UE

Figura 1

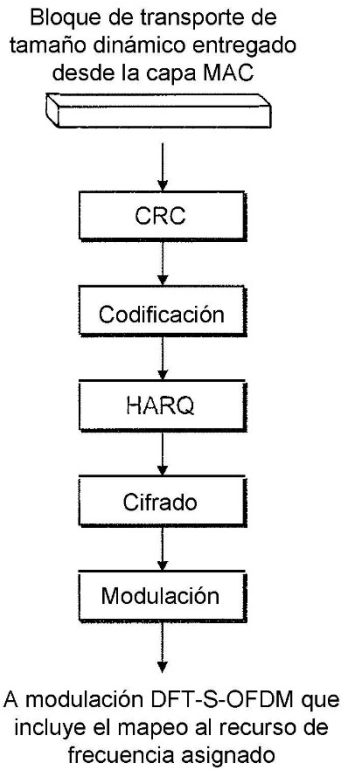
Bloque de transporte de tamaño dinámico entregado desde la capa MAC
CRC
Codificación
HARQ
Cifrado
Modulación
A modulación DFT-S-OFDM que incluye el mapeo al recurso de frecuencia asignado

Figura 2

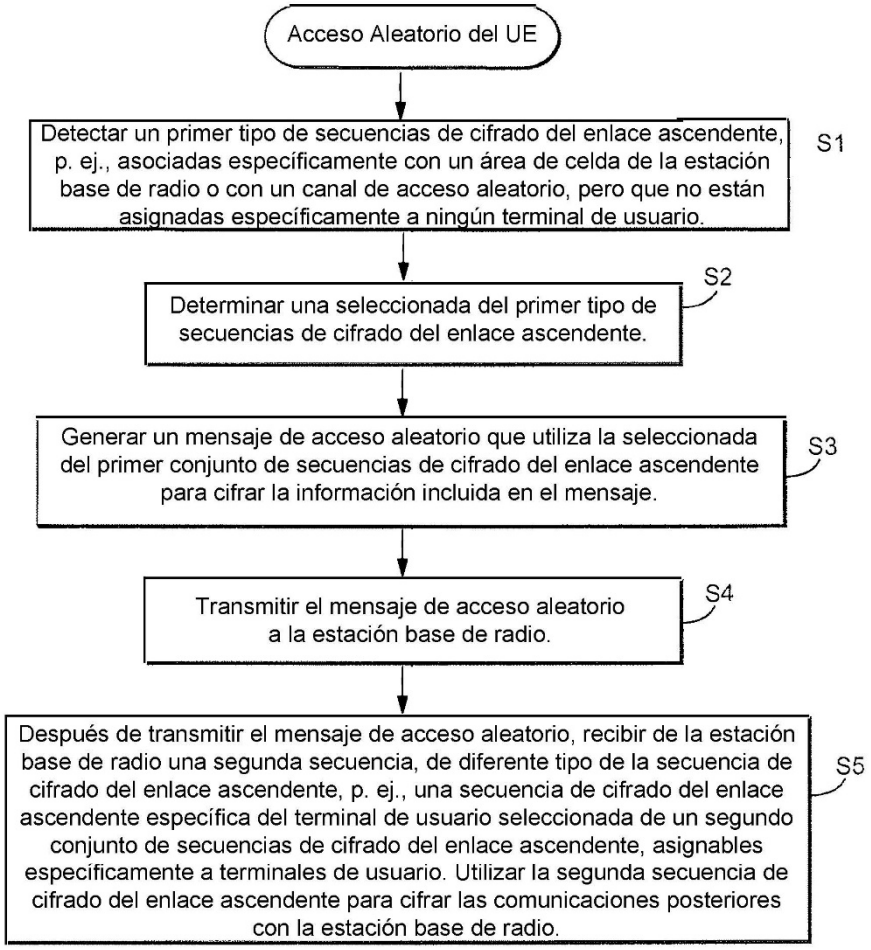
Acceso Aleatorio del UE
Detectar un primer tipo de secuencias de cifrado del enlace ascendente, p. ej., asociadas específicamente con un área de celda de la estación base de radio o con un canal de acceso aleatorio, pero que no están asignadas específicamente a ningún terminal de usuario.
S1
Determinar una seleccionada del primer tipo de secuencias de cifrado del enlace ascendente.
S2
Generar un mensaje de acceso aleatorio que utiliza la seleccionada del primer conjunto de secuencias de cifrado del enlace ascendente para cifrar la información incluida en el mensaje.
S3
Transmitir el mensaje de acceso aleatorio a la estación base de radio.
S4
Después de transmitir el mensaje de acceso aleatorio, recibir de la estación base de radio una segunda secuencia, de diferente tipo de la secuencia de cifrado del enlace ascendente, p. ej., una secuencia de cifrado del enlace ascendente específica del terminal de usuario seleccionada de un segundo conjunto de secuencias de cifrado del enlace ascendente, asignables específicamente a terminales de usuario. Utilizar la segunda secuencia de cifrado del enlace ascendente para cifrar las comunicaciones posteriores con la estación base de radio.
S5

Figura 3

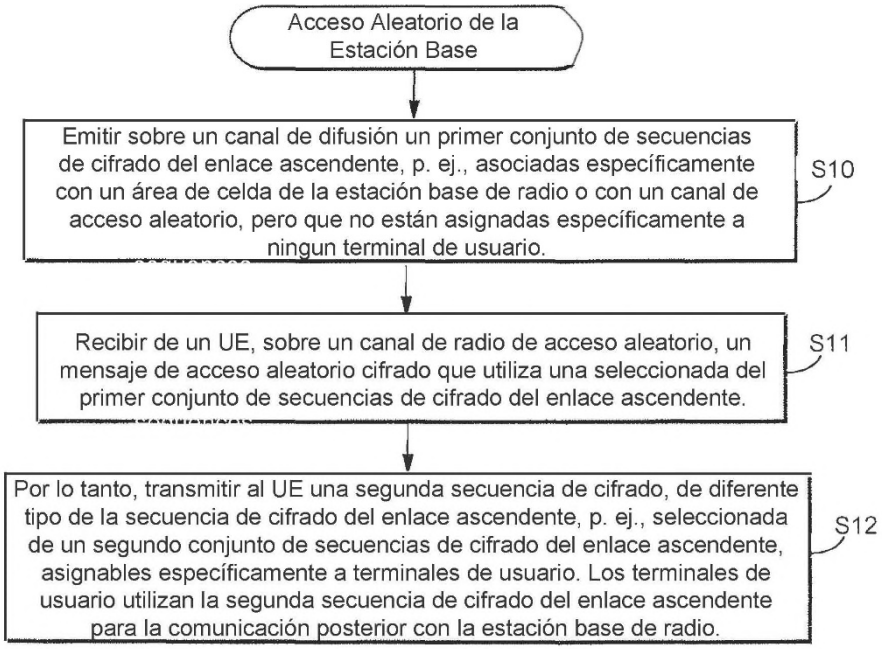
Acceso Aleatorio de la Estación Base
Emitir sobre un canal de difusión un primer conjunto de secuencias de cifrado del enlace ascendente, p. ej., asociadas específicamente con un área de celda de la estación base de radio o con un canal de acceso aleatorio, pero que no están asignadas específicamente a ningun terminal de usuario.
S10
Recibir de un UE, sobre un canal de radio de acceso aleatorio, un mensaje de acceso aleatorio cifrado que utiliza una seleccionada del primer conjunto de secuencias de cifrado del enlace ascendente.
S11
Por lo tanto, transmitir al UE una segunda secuencia de cifrado, de diferente tipo de la secuencia de cifrado del enlace ascendente, p. ej., seleccionada de un segundo conjunto de secuencias de cifrado del enlace ascendente, asignables específicamente a terminales de usuario. Los terminales de usuario utilizan la segunda secuencia de cifrado del enlace ascendente para la comunicación posterior con la estación base de radio.
S12

Figura 4

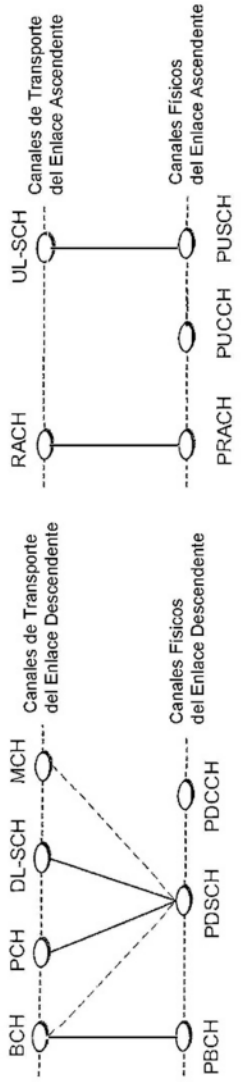

Figura 5A

Figura 5B

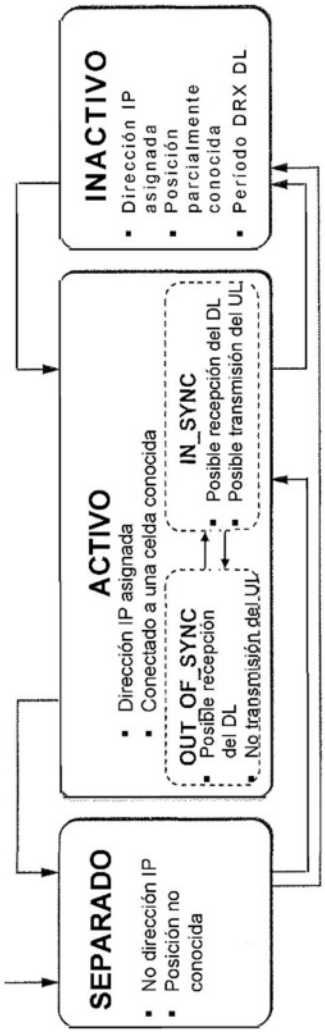

Figura 6

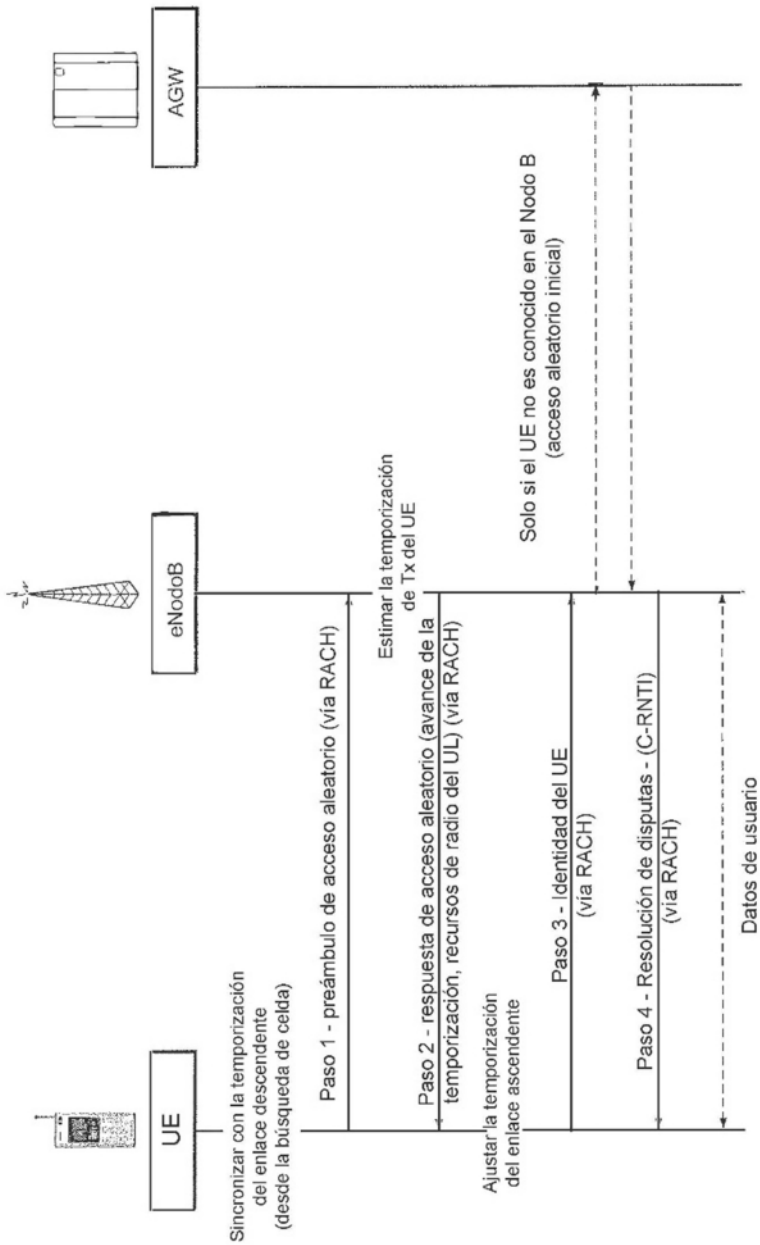
UE
eNodoB
AGW
Sincronizar con la temporización del enlace descendente (desde la búsqueda de celda)
Paso 1 - preámbulo de acceso aleatorio (vía RACH)
Estimar la temporización de Tx del UE
Paso 2 - respuesta de acceso aleatorio (avance de la temporización, recursos de radio del UL) (vía RACH)
Ajustar la temporización del enlace ascendente
Solo si el UE no es conocido en el Nodo B (acceso aleatorio inicial)
Paso 3 - Identidad del UE (vía RACH)
Paso 4 - Resolución de disputas - (C-RNTI) (vía RACH)
Datos de usuario

Figura 7

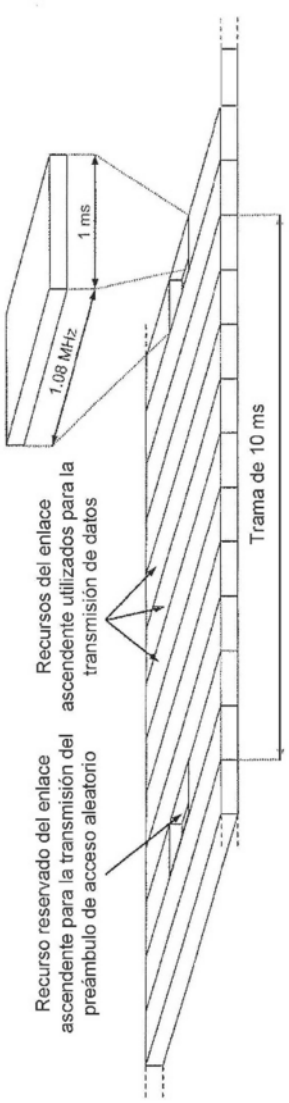
1.08 MHz
1 ms
Trama de 10 ms
Recursos del enlace ascendente utilizados para la transmisión de datos
Recurso reservado del enlace ascendente para la transmisión del preámbulo de acceso aleatorio

Figura 8

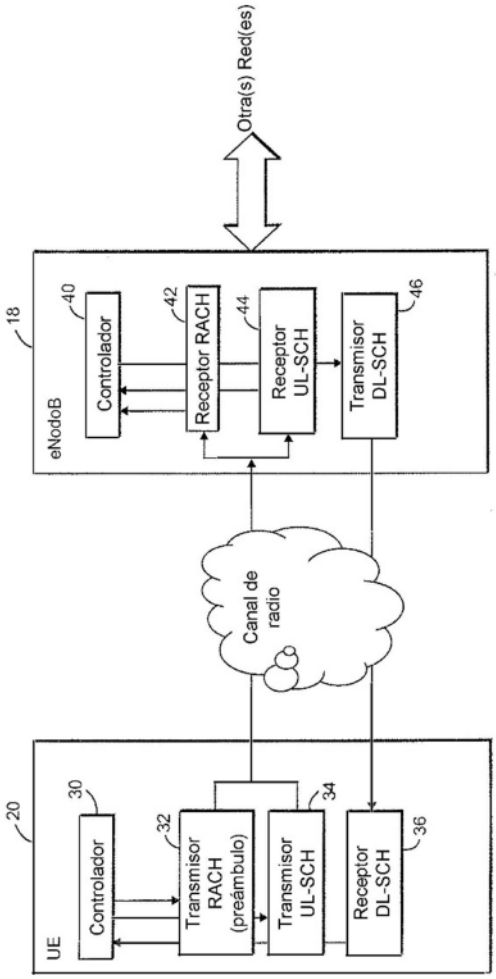
Otra(s) Red(es)
18
eNodoB
40
Controlador
42
Receptor RACH
44
Receptor UL-SCH
46
Transmisor DL-SCH
Canal de radio
20
UE
30
Controlador
32
Transmisor RACH (preámbulo)
34
Transmisor UL-SCH
36
Receptor DL-SCH

Figura 9