

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 000 285**

51 Int. Cl.:

H04W 74/0833 (2014.01)

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 23199938 (4)**

97 Fecha y número de publicación de la concesión europea: **11.12.2024** **EP 4277422**

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:

28.02.2025

73 Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON
(PUBL) (100.00%)
164 83 Stockholm, SE**

72 Inventor/es:

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

74 Agente/Representante:

ELZABURU, S.L.P

ES 3 000 285 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 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 de comunicaciones móvil de tipo LTE. Una E-UTRAN incluye un NodoB E-UTRAN (eNodoBs o eNBs) que proporciona terminaciones del protocolo del plano de usuario y del plano de control E-UTRA hacia el equipo 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 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. La interfaz S1 soporta una relación de varios a varios entre las Pasarelas MMEs / SAE y los eNBs. La E-UTRAN y el EPC juntos forman una Red Móvil Terrestre Pública (PLMN). Las pasarelas MMEs / SAE están conectadas, directa o indirectamente, a Internet 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 (eNodeB) 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 eNodeB 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 eNodeB 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 eNodeB y la correspondiente demodulación coherente.

La técnica anterior se conoce a partir de "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), 3GPP Technical Specification Group Radio Access Network", 3GPP TS 36.300 V8.1.0, 1 de junio de 2007 (2007-06-01), páginas 1-106.

45 **Compendio**

La presente invención proporciona métodos según las reivindicaciones independientes 1 y 10 en un terminal de usuario para realizar un procedimiento de acceso aleatorio. También se proporcionan un terminal de usuario según la reivindicación 13 y configurado para realizar cualquiera de los métodos y un producto de programa informático según la reivindicación 14 y que comprende partes de código de programa para realizar cualquiera de los métodos.

50 **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;

5 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

10 la Figura 9 es un diagrama de bloques de función no limitante, de ejemplo, de un terminal de usuario y de una estación base eNode 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 eNodeB 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 (PDSCH). 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_ACTIVE 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 (eNodeB), 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 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.

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.

REIVINDICACIONES

1. Un método implementado en un terminal de usuario (20) para realizar un procedimiento de acceso aleatorio, el método comprende:

5 transmitir un primer mensaje con un preámbulo de acceso aleatorio a una estación base de radio (18) utilizando un recurso de radio canal de acceso aleatorio, RACH;

recibir un segundo mensaje de respuesta de acceso aleatorio de la estación base de radio (18), el mensaje de respuesta de acceso aleatorio indica un cambio de temporización, un recurso de radio identificado de un canal compartido de enlace ascendente, UL-SCH, y una identidad temporal de terminal de usuario;

10 ajustar una temporización en el terminal de usuario (20) para transmitir señales a la estación base de radio (18) basándose en el cambio de temporización indicado en el segundo mensaje;

basándose en la temporización ajustada, transmitir un tercer mensaje a la estación base de radio (18) sobre el recurso de radio identificado del canal compartido de enlace ascendente, en el que el mensaje incluye una identidad de terminal de usuario que fue recibida por el terminal de usuario antes del procedimiento de acceso aleatorio, y en el que el tercer mensaje se cifra utilizando una secuencia de cifrado asociada a la célula que no es específica del terminal, en el que
15 la secuencia de cifrado asociada a la célula no específica del terminal se basa en la identidad de terminal de usuario temporal;

recibir un cuarto mensaje de resolución de contención de la estación base de radio (18) para completar el procedimiento de acceso aleatorio; y

20 realizar transmisiones de datos posteriores tras la finalización del procedimiento de acceso aleatorio utilizando una secuencia de cifrado específica del terminal.
2. El método de la reivindicación 1, en el que la identidad de terminal de usuario recibida por el terminal de usuario antes del procedimiento de acceso aleatorio se recibió como una identidad de terminal de usuario temporal en un procedimiento de acceso aleatorio precedente.
3. El método de cualquiera de las reivindicaciones anteriores, en el que la identidad de terminal de usuario recibida por el terminal de usuario antes del procedimiento de acceso aleatorio es un identificador temporal de red de radio celular, C-RNTI.
25
4. El método de cualquiera de las reivindicaciones anteriores, en el que la identidad de terminal de usuario temporal es un C-RNTI temporal, Identificador Temporal de Red de Radio Celular temporal.
5. El método de cualquiera de las reivindicaciones anteriores, en el que el preámbulo de acceso aleatorio es generado por el terminal de usuario (20).
30
6. El método de la reivindicación 5, en el que el preámbulo de acceso aleatorio se genera basándose en secuencias ZC, Zadoff-Chu.
7. El método de cualquiera de las reivindicaciones anteriores, en el que el mensaje de respuesta de acceso aleatorio se dirige a múltiples terminales de usuario en una única transmisión.
8. El método de cualquiera de las reivindicaciones anteriores, en el que el mensaje de respuesta de acceso aleatorio se recibe en un canal compartido de enlace descendente, DL-SCH, y se indica en un canal físico de control de enlace descendente, PDCCH, utilizando una identidad común reservada para la respuesta de acceso aleatorio.
35
9. El método de cualquiera de las reivindicaciones precedentes, en el que el cambio de temporización indicado en el mensaje de respuesta de acceso aleatorio es un comando de avance de temporización.
10. Un método implementado en un terminal de usuario (20) para realizar un procedimiento de acceso aleatorio, el método comprende:

40 transmitir un primer mensaje con un preámbulo de acceso aleatorio a una estación base de radio (18) utilizando un recurso de radio, canal de acceso aleatorio, RACH;

recibir un segundo mensaje de respuesta de acceso aleatorio de la estación base de radio (18), el mensaje de respuesta de acceso aleatorio indica un cambio de temporización, un recurso de radio identificado de un canal compartido de enlace ascendente, UL-SCH, y una identidad temporal de terminal de usuario;
45

ajustar una temporización en el terminal de usuario (20) para transmitir señales a la estación base de radio (18) basándose en el cambio de temporización indicado en el segundo mensaje de respuesta de acceso aleatorio;

- 5 basándose en la temporización ajustada, transmitir un tercer mensaje a la estación base de radio (18) a través del recurso de radio identificado del canal compartido de enlace ascendente, en el que el mensaje incluye un identificador de terminal de red central del terminal de usuario, y en el que el mensaje se cifra utilizando una secuencia de cifrado asociada a la célula que no es específica del terminal, en el que la secuencia de cifrado asociada a la célula no específica del terminal se basa en la identidad temporal del terminal de usuario;

recibir un cuarto mensaje de resolución de contención de la estación base de radio (18) para completar el procedimiento de acceso aleatorio; y

- 10 realizar transmisiones de datos posteriores tras la finalización del procedimiento de acceso aleatorio utilizando una secuencia de cifrado específica del terminal.

11. El método de la reivindicación 10, en el que la identidad de terminal de usuario temporal es un C-RNTI temporal, Identificador Temporal de Red de Radio Celular temporal.

12. El método de la reivindicación 10 u 11, que comprende promover la identidad de terminal de usuario temporal a un Identificador Temporal de Red de Radio Celular, C-RNTI.
- 15

13. Un terminal de usuario configurado para realizar el método de cualquiera de las reivindicaciones 1 a 12.

14. Un producto de programa informático que comprende partes de código de programa para realizar el método de cualquiera de las reivindicaciones 1 a 12 cuando el producto de programa informático es ejecutado por un procesador de un terminal de usuario.

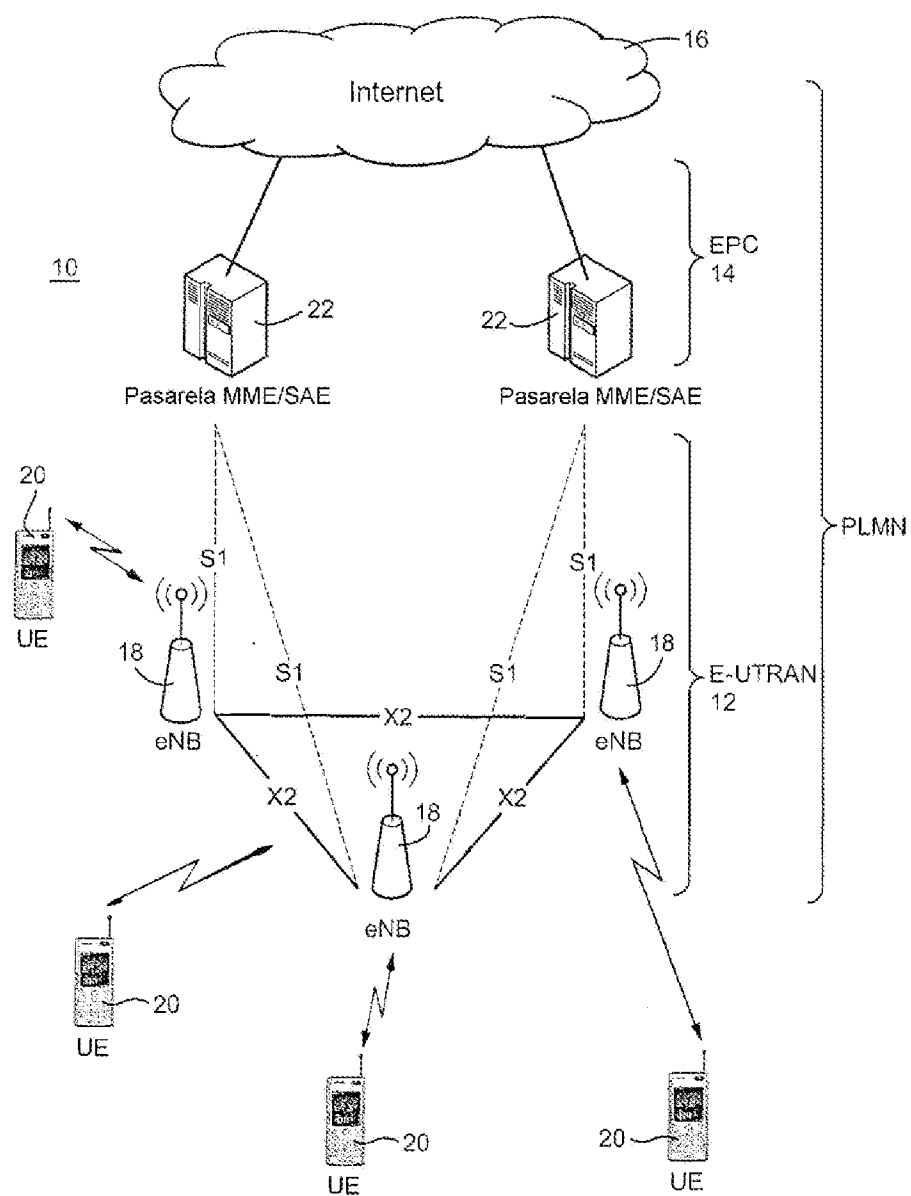


Figura 1

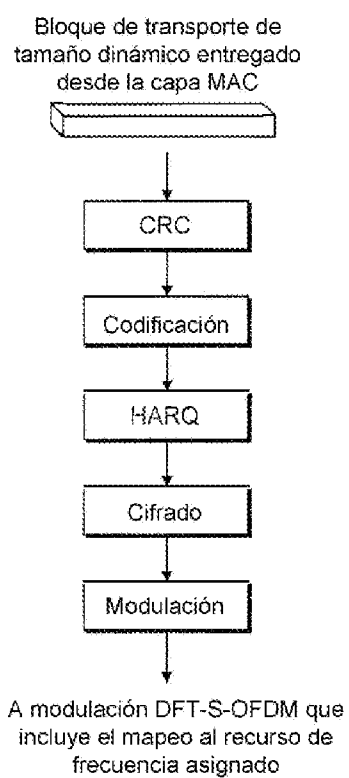


Figura 2

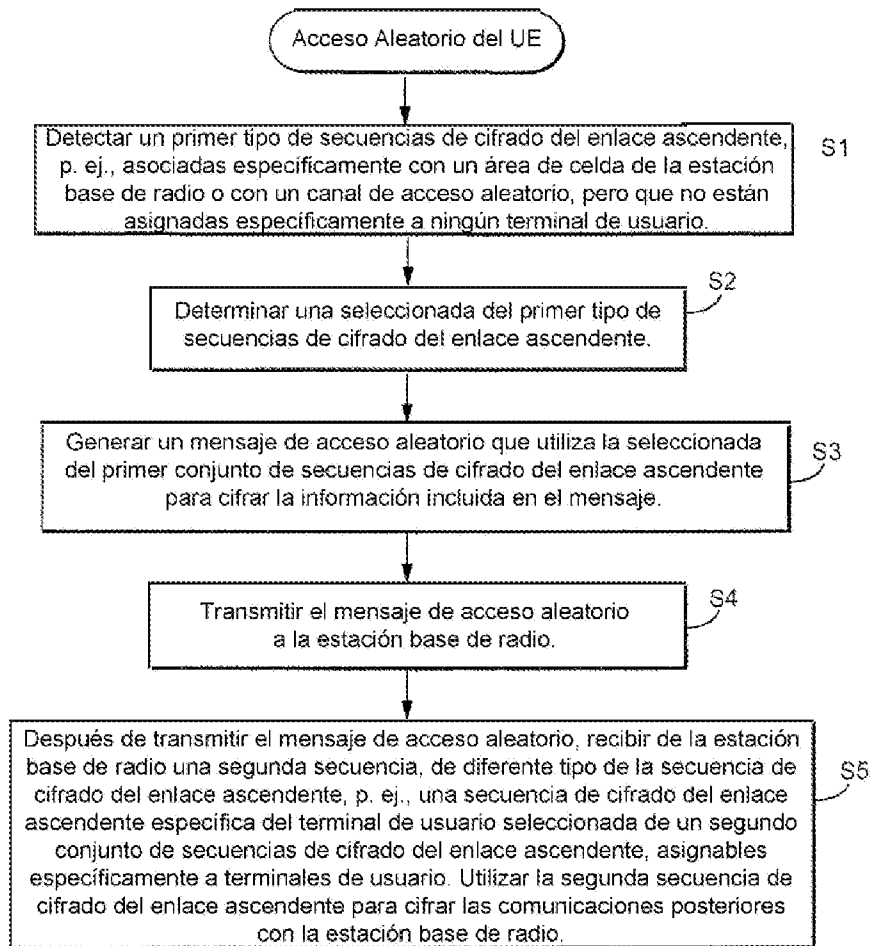


Figura 3

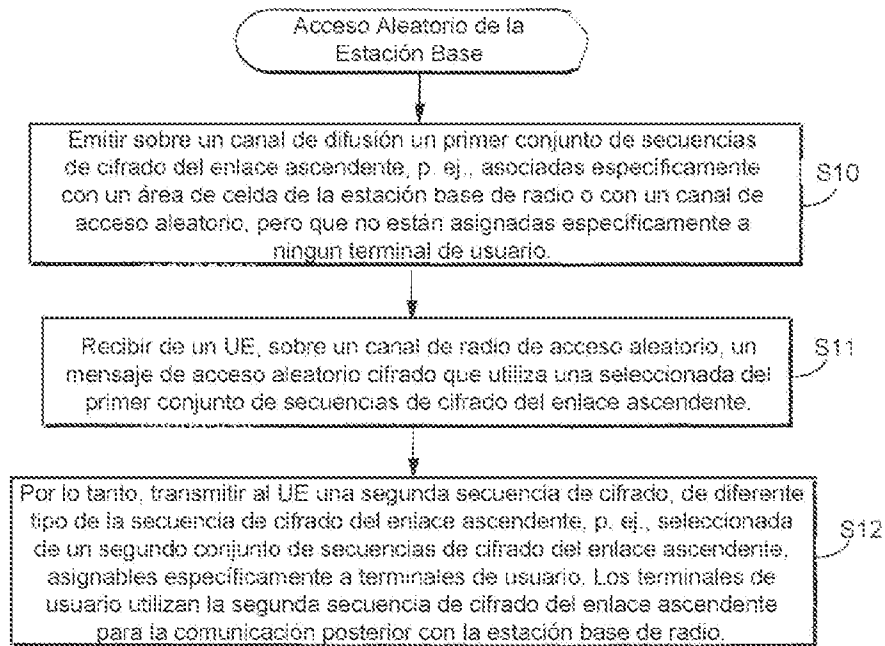


Figura 4

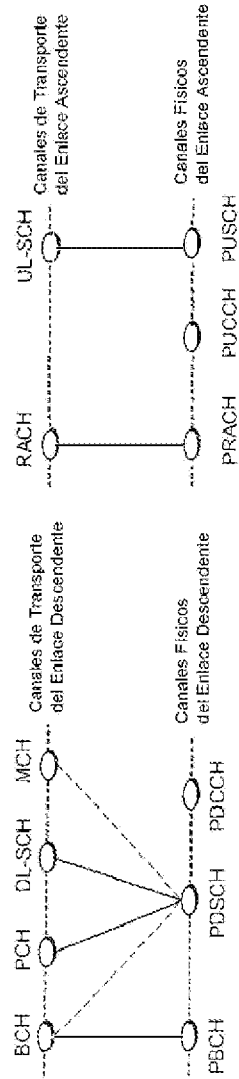


Figura 5A

Figura 5B

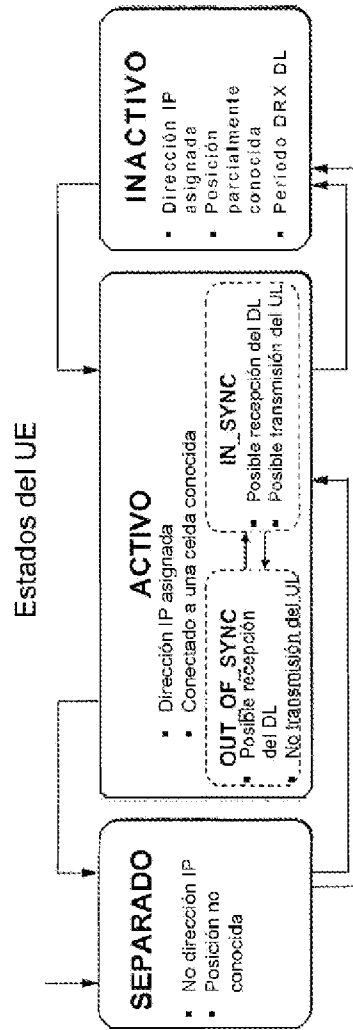


Figura 6

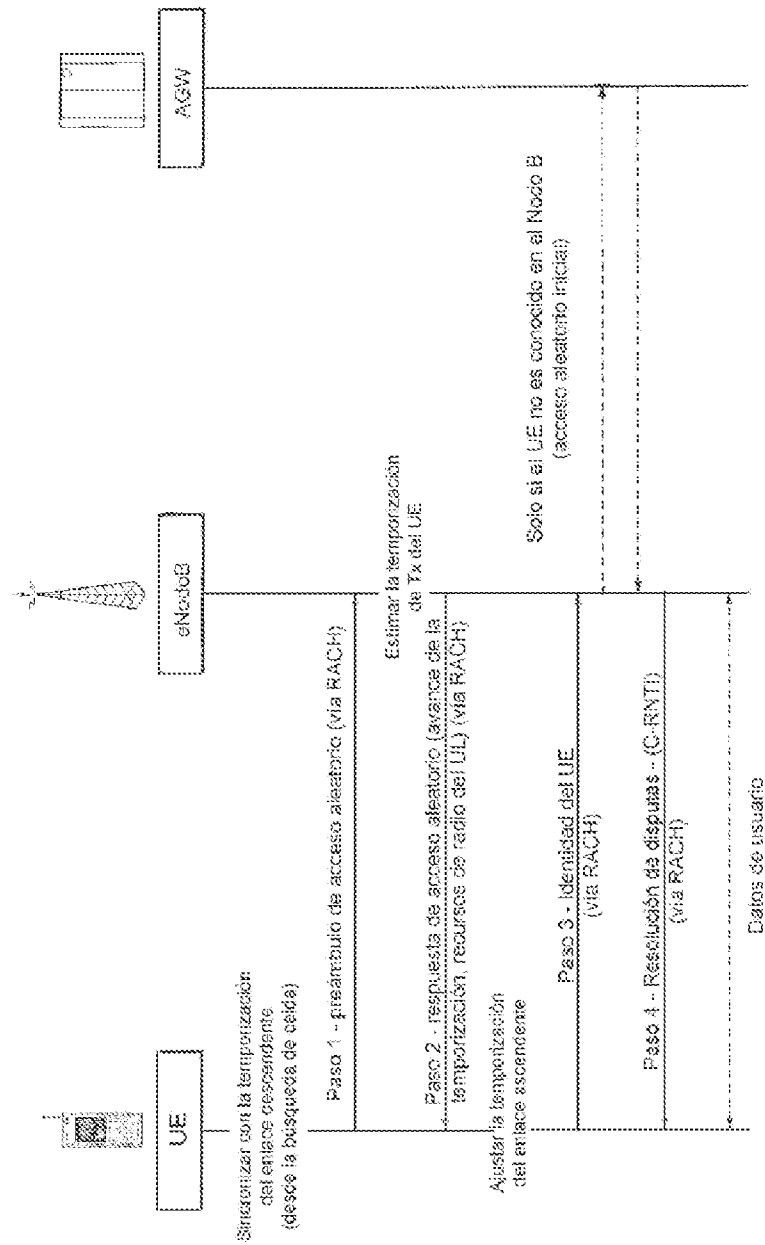


Figura 7

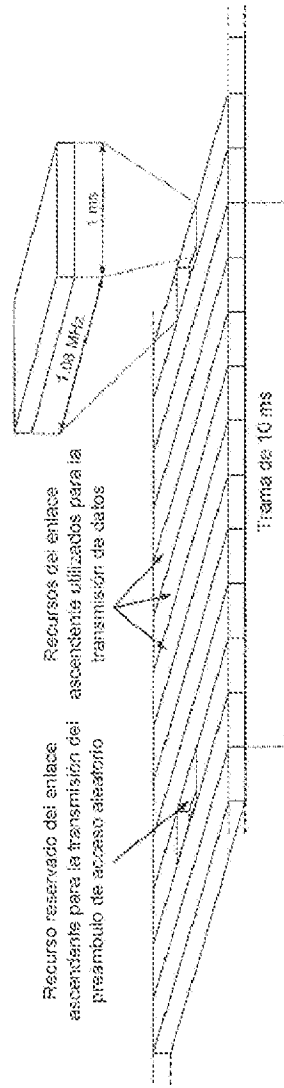


Figura 8

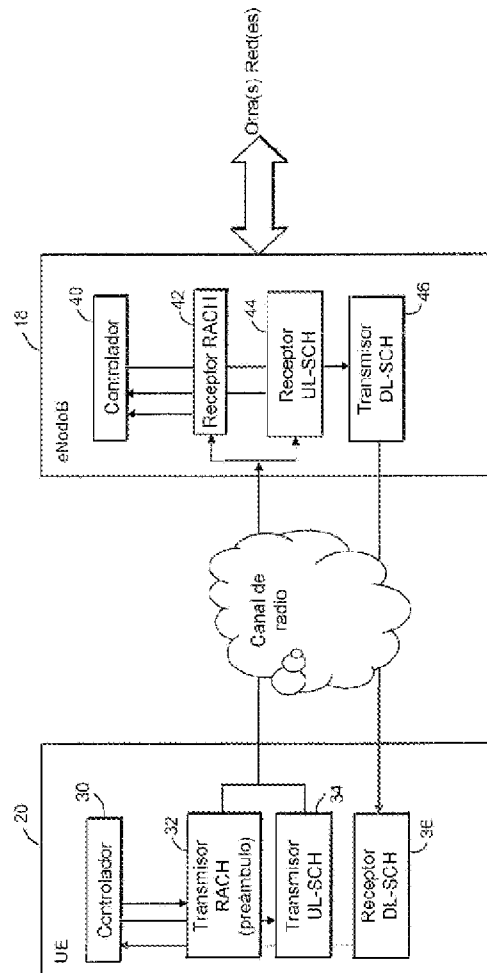


Figura 9