

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 711 080**

51 Int. Cl.:

H04W 74/08 (2009.01)

H04W 88/00 (2009.01)

H04W 72/04 (2009.01)

H04W 76/10 (2008.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **03.07.2008** **E 15190589 (0)**

97 Fecha y número de publicación de la concesión europea: **28.11.2018** **EP 2991430**

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

30 Prioridad:

08.08.2007 US 835782

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

30.04.2019

73 Titular/es:

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

72 Inventor/es:

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

74 Agente/Representante:

MARTÍN BADAJOZ, Irene

ES 2 711 080 T3

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

DESCRIPCIÓN

Cifrado de enlace ascendente durante acceso aleatorio

5 **Campo técnico**

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

10 **Antecedentes**

El sistema universal de telecomunicaciones móviles (UMTS) es un sistema de comunicaciones móviles asíncrono de tercera generación (3G) que funciona en acceso múltiple por división de código de banda ancha (WCDMA) basándose en sistemas europeos, el sistema global para comunicaciones móviles (GSM) y el servicio general de radio por paquetes (GPRS). La evolución a largo plazo (LTE) de UMTS está en fase de desarrollo por el proyecto de asociación de tercera generación (3GPP) que normalizó UMTS. Existen muchas especificaciones técnicas alojadas en el sitio web de 3GPP relacionadas con el acceso de radio terrestre universal evolucionado (E-UTRA) y la red de acceso de radio terrestre universal evolucionado (E-UTRAN), por ejemplo, 3GPP TS 36.300. El objetivo del trabajo de LTE es desarrollar un entorno de trabajo para la evolución de la tecnología de acceso de radio 3GPP hacia una tecnología de acceso de radio de alta velocidad de datos, baja latencia y optimizada por paquetes. En particular, LTE tiene por objetivo soportar servicios proporcionados desde el dominio conmutado por paquetes (PS). Una meta clave de la tecnología LTE de 3GPP es permitir comunicaciones por paquetes a alta velocidad a o por encima de aproximadamente 100 Mbps.

La figura 1 ilustra un ejemplo de un sistema de comunicaciones móviles 10 de tipo LTE. Una E-UTRAN 12 incluye NodosB (eNodosB o eNB) de E-UTRAN 18 que proporcionan terminaciones de protocolo de plano de control y plano de usuario de E-UTRA hacia el equipo de usuario (UE) 20 a través de una interfaz de radio. Aunque un eNB es un nodo lógico, implementado a menudo aunque no necesariamente por una estación base física, el término estación base se usa aquí para cubrir generalmente tanto nodos lógicos como físicos. Un UE se denomina a veces terminal de radio móvil y, en un estado de inactividad, supervisa la información de sistema difundida por radio por los eNB dentro de su 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 de radio, envía una solicitud a través de un canal de acceso aleatorio (RACH) a un eNB adecuado, normalmente un eNB con las condiciones de radio más favorables. Los eNB están interconectados entre sí mediante una interfaz X2. Los eNB también están conectados mediante la interfaz S1 a un núcleo de paquetes evolucionado (EPC) 14 que incluye una entidad de gestión de movilidad (MME) por una S1-MME y a una pasarela de evolución de arquitectura de sistema (SAE) por una S1-U. En este ejemplo, se hace referencia a la pasarela de MME/SAE como un solo nodo 22. La interfaz S1 soporta una relación muchos a muchos entre pasarelas de MME/SAE y eNB. La E-UTRAN 12 y el EPC 14 forman conjuntamente una red móvil terrestre pública (PLMN). Las pasarelas de MME/SAE 22 están conectadas directa o indirectamente a Internet 16 y a otras redes.

Con el fin de permitir el funcionamiento en asignaciones de espectro diferentes, por ejemplo para tener una migración sin problemas desde 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, por ejemplo, anchos de banda que oscilan entre 1,25 MHz y 20 MHz para transmisiones de enlace descendente desde la red hasta el UE. Deben soportarse tanto servicios de datos de alta velocidad como servicios de baja velocidad como la voz, y dado que la LTE de 3G está diseñada para TCP/IP, VoIP posiblemente sea el servicio que transmite el habla.

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

El procesamiento de canal de transporte de enlace ascendente de LTE se describe resumidamente en la figura 2. Un bloque de transporte de tamaño dinámico se emite desde la capa de control de acceso al medio (MAC). Se calcula un código de redundancia cíclica (CRC) que va a usarse para la detección de errores en el receptor de estación base para el bloque y se adjunta al mismo. Entonces se realiza una codificación de canal de enlace ascendente por un codificador de canal que puede usar cualquier técnica de codificación adecuada. En LTE, el código puede ser un turbocódigo que incluye un intercalador interno basado en polinomios cuadráticos de permutación (QPP) para realizar un intercalado de bloque como parte del turbocodificador. La solicitud de repetición automática (ARQ) híbrida de enlace ascendente de LTE extrae, del bloque de bits codificados emitido por el codificador de canal, el conjunto exacto de bits que van a transmitirse en cada instante de transmisión/retransmisión. Un dispositivo de cifrado cifra los bits codificados en el enlace ascendente de LTE (por ejemplo, cifrado a nivel de bit) con el fin de aleatorizar la interferencia y garantizar de ese modo que la ganancia de procesamiento

proporcionada por el código de canal puede utilizarse completamente.

Para lograr esta aleatorización de la interferencia, el cifrado de enlace ascendente es específico de terminal móvil, es decir, terminales móviles diferentes (UE) usan secuencias de cifrado diferentes. El cifrado específico de terminal también proporciona al planificador la libertad de planificar múltiples usuarios en el mismo recurso de tiempo-frecuencia y recurrir al procesamiento del receptor de estación base para separar las transmisiones de los múltiples usuarios. El cifrado específico de terminal aleatoriza la interferencia de otros terminales móviles en la misma célula que se han planificado en el mismo recurso y mejora el rendimiento.

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

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

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

Pero durante el procedimiento de acceso aleatorio (inicial), las transmisiones de enlace ascendente desde el terminal de usuario no pueden emplear números de referencia o secuencias de cifrado específicas de terminal para aleatorizar la interferencia ya que el mensaje de solicitud de acceso aleatorio inicial desde el terminal de usuario acaba de iniciar la comunicación con la red y no se ha asignado ni un código de cifrado específico de terminal ni un número de referencia específico de terminal a ese terminal de usuario. Lo que se necesita es un mecanismo que permita mensajes de acceso aleatorio enviados a través de un canal de enlace ascendente compartido que va a cifrarse hasta que pueda asignarse un código de cifrado específico de terminal al terminal de usuario. Un motivo para cifrar los mensajes de acceso aleatorio es aleatorizar interferencias entre células, que es también el caso para el cifrado durante una transmisión de datos de enlace ascendente "normal". En el último caso, el cifrado también puede usarse para suprimir la interferencia dentro de células en caso de múltiples UE que se han planificado en el mismo recurso de tiempo-frecuencia. De manera similar, también será deseable poder tener terminales de usuario que transmitan señales de referencia conocidas durante el acceso aleatorio para permitir al receptor de estación base estimar el canal de enlace ascendente. Las señales de referencia tienen que incluirse en los mensajes de acceso aleatorio así como en las transmisiones de datos de enlace ascendente "normales" para permitir la estimación de canal en el eNodoB y su demodulación coherente correspondiente.

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

Sumario

La tecnología descrita a continuación facilita el acceso aleatorio por un terminal de usuario con una estación base de radio. Un terminal de usuario determina uno de un primer tipo de secuencias de cifrado de enlace ascendente y genera un mensaje de acceso aleatorio usando el determinado del primer tipo de secuencias de cifrado de enlace ascendente. Su transmisor transmite el mensaje de acceso aleatorio a la estación base de radio. El receptor de terminal de usuario recibe entonces desde la estación base un segundo tipo diferente de secuencia de cifrado de enlace ascendente. El terminal usa ese segundo tipo diferente de secuencia de cifrado de enlace ascendente para la comunicación posterior con la estación base de radio. En una realización de ejemplo no limitativa, el primer tipo de secuencias de cifrado de enlace ascendente puede estar asociado específicamente con el área de células de estación base de radio o un canal de radio de acceso aleatorio asociado con la estación base de radio, pero no se

asigna específicamente a ningún terminal de usuario, y el segundo tipo diferente de secuencia de cifrado de enlace ascendente puede seleccionarse a partir de un segundo conjunto de secuencias de cifrado de enlace ascendente que pueden asignarse específicamente a terminales de usuario. Usar estos dos tipos diferentes de secuencias de cifrado permite a los terminales de usuario cifrar sus transmisiones de señal de enlace ascendente aun cuando los

5 códigos de cifrado específicos de terminal no pueden usarse 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 a la estación base de radio usando un recurso de radio de canal de acceso aleatorio. Un segundo

10 mensaje de respuesta de acceso aleatorio se recibe entonces desde la estación base de radio indicando un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario temporal. El terminal ajusta una temporización en el terminal de usuario para transmitir señales a la estación base de radio basándose en información recibida en el mensaje de respuesta de acceso aleatorio y, basándose en la temporización ajustada,

15 transmite un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad completa del terminal de usuario a la estación base de radio a través del recurso de radio identificado. El tercer mensaje se cifra usando el determinado del primer tipo de secuencia de cifrado de enlace ascendente, se modula y se mapea a un recurso de canal de radio. El terminal recibe un cuarto mensaje de resolución de contienda desde la estación base de radio para completar los procedimientos de acceso aleatorio y siguen comunicaciones normales.

Diversas realizaciones no limitativas mapean el primer conjunto de secuencias de cifrado de enlace ascendente a algún otro parámetro conocido por el terminal de usuario y la estación base. Por ejemplo, el primer conjunto de secuencias de cifrado de enlace ascendente puede mapearse a las secuencias de preámbulo de acceso aleatorio correspondientes. Una del primer conjunto de secuencias de cifrado de enlace ascendente puede seleccionarse entonces basándose en el preámbulo de acceso aleatorio incluido en el primer mensaje de solicitud de acceso

20 aleatorio y el mapeo. Otro ejemplo mapea el primer conjunto de secuencias de cifrado de enlace ascendente a los identificadores de terminal de usuario correspondientes y selecciona una del primer conjunto de secuencias de cifrado de enlace ascendente en función del identificador de terminal de usuario incluido en el segundo mensaje de respuesta de acceso aleatorio y el mapeo. Un tercer ejemplo mapea el primer conjunto de secuencias de cifrado de enlace ascendente a los recursos de radio correspondientes usados para transmitir el mensaje de solicitud de acceso aleatorio y selecciona una del primer conjunto de secuencias de cifrado de enlace ascendente en función del

25 recurso de radio de canal de acceso aleatorio usado para enviar un primer mensaje de solicitud de acceso aleatorio que incluye un preámbulo de acceso aleatorio a la estación base de radio y el mapeo.

Los dos tipos de enfoques de secuencia de cifrado también pueden usarse para señales de referencia integradas en mensajes de acceso aleatorio de enlace ascendente enviados a la estación base que son usados por la estación

35 base para estimar el canal de enlace ascendente, por ejemplo, para fines de ecualización, etc. Se selecciona una de un primer conjunto de secuencias de referencia de enlace ascendente, por ejemplo, secuencias de referencia de enlace ascendente asociadas específicamente con un área de células de estación base de radio o canal de acceso aleatorio pero que no están asignadas específicamente a ningún terminal de usuario. Se genera un mensaje de acceso aleatorio usando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente y la seleccionada del primer conjunto de secuencias de referencia de enlace ascendente. El terminal de usuario transmite el mensaje de acceso aleatorio a la estación base de radio. Después de eso, la estación base informa al terminal de usuario de un segundo tipo diferente de secuencia de referencia para usar en comunicaciones de enlace ascendente posteriores, por ejemplo, un número de referencia asignado específicamente a ese terminal de usuario.

En una implementación de ejemplo no limitativa, el terminal de usuario y la estación base están configurados para comunicarse con una red de comunicaciones por radio de evolución a largo plazo (LTE), transmitiendo el terminal de

40 usuario el primer mensaje de solicitud de acceso aleatorio a través de un canal de acceso aleatorio (RACH) y el tercer mensaje a través de un canal compartido de enlace ascendente (UL-SCH). El identificador de terminal de usuario enviado por la estación base en el segundo mensaje puede ser un identificador de terminal de usuario temporal usado hasta que un identificador de terminal de red de radio (RNTI) se asigna al terminal de usuario.

Breve descripción de los dibujos

55 La figura 1 es un sistema de comunicaciones móviles por radio de LTE de ejemplo;

la figura 2 es un diagrama de flujo que ilustra procedimientos de ejemplo no limitativos para preparar un bloque de transporte emitido desde la capa de acceso al medio de un terminal de usuario para su transmisión a través de la

60 interfaz de radio a la red en un sistema de comunicaciones móviles por radio de LTE;

la figura 3 es un diagrama de flujo que ilustra procedimientos de ejemplo no limitativos 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 de ejemplo no limitativos para que una estación base reciba y procese un acceso aleatorio de terminal de usuario a la red de radio;

65

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

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

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

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

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

Descripción detallada

En la siguiente descripción, con fines explicativos y no limitativos, se exponen detalles específicos, tales como nodos, entidades funcionales, técnicas, protocolos, normas, etc. particulares con el fin de proporcionar un entendimiento de la tecnología descrita. En otros casos, se omiten descripciones detalladas de procedimientos, dispositivos, técnicas, etc. bien conocidos para no complicar la descripción con detalles innecesarios. Los bloques funcionales individuales se muestran en las figuras. Los expertos en la técnica apreciarán que las funciones de estos bloques pueden implementarse usando circuitos de hardware individuales, usando programas de software y datos conjuntamente con un microprocesador programado de manera adecuada o un ordenador de propósito general, usando circuitos integrados de aplicación específica (ASIC), matrices lógicas programables y/o usando uno o más procesadores de señales digitales (DSP).

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

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

La figura 4 es un diagrama de flujo que ilustra procedimientos homólogos de ejemplo no limitativos para que una estación base reciba y procese un acceso aleatorio del terminal de usuario para 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 de terminal. La estación base difunde por radio, implícita o explícitamente, a través de un canal de radiodifusión, por ejemplo, BCH, su conjunto de preámbulos y secuencias de cifrado de enlace ascendente (etapa S10). Si la estación base no difunde por radio explícitamente la secuencia de cifrado que va a usarse, la identidad de la célula a partir la cual puede usarse la secuencia de cifrado puede derivarse por ejemplo a través de un mapeo entre secuencia e identificador de célula. Las secuencias de cifrado de enlace ascendente pueden estar, por ejemplo, asociadas específicamente con un área de células de estación base de radio o un canal de acceso aleatorio y no se asignan específicamente a ningún terminal de usuario. Entonces, la estación base espera a recibir un primer mensaje de solicitud de acceso aleatorio desde un terminal de usuario que incluye uno de los preámbulos de estación base. En respuesta, la estación base transmite un segundo mensaje de respuesta de acceso aleatorio al

un terminal de usuario indicando un cambio de temporización, un recurso de radio identificado y un identificador de terminal de usuario. Un tercer mensaje correspondiente al mensaje de acceso aleatorio generado que incluye la identidad de terminal de usuario se descifra usando la seleccionada del primer conjunto de secuencias de cifrado de enlace ascendente (etapa S11). Después de eso, la estación base transmite al terminal de usuario un cuarto mensaje que incluye un segundo tipo diferente de secuencia de cifrado de enlace ascendente seleccionada de un segundo conjunto de secuencias de cifrado de enlace ascendente, por ejemplo, secuencias de cifrado de enlace ascendente que pueden asignarse específicamente a terminales de usuario (etapa S12). El terminal de usuario usa la segunda secuencia de cifrado de enlace ascendente para la comunicación posterior con la estación base de radio. Procedimientos similares pueden aplicarse a señales de referencia de enlace ascendente conocidas.

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

En LTE, como en otros sistemas de comunicación móvil por radio, un terminal móvil puede estar en diferentes estados de funcionamiento. La figura 6 ilustra estos estados para LTE. En el encendido, el terminal móvil entra en el estado de LTE_DETACHED. En este estado, la red no conoce el terminal móvil. Antes de que cualquier comunicación adicional pueda tener lugar entre el terminal móvil y la red, el terminal móvil tiene que registrarse con la red usando el procedimiento de acceso aleatorio para entrar en el estado LTE_ACTIVE. El estado LTE_DETACHED es principalmente un estado usado en el encendido. Una vez que el terminal móvil se registra con la red, está normalmente en uno de los otros estados: LTE_ACTIVE o LTE_IDLE.

LTE_ACTIVE es el estado usado cuando el terminal móvil está activo en la transmisión y recepción de datos. En este estado, el terminal móvil está conectado a una célula específica dentro de la red. Uno o varios protocolos de internet (IP) u otro tipo de direcciones de paquetes de datos se han asignado al terminal móvil, así como una identidad del terminal, un identificador temporal de red de radio celular (C-RNTI), usado para fines de señalización entre el terminal móvil y la red. El estado LTE_ACTIVE incluye dos subestados, 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 de enlace ascendente de datos de usuario y la señalización de control de capa inferior. Si no ha tenido lugar la transmisión de enlace ascendente dentro de un intervalo de tiempo dado, se indica que el enlace ascendente está fuera de sincronización, en cuyo caso, el terminal móvil debe realizar un procedimiento de acceso aleatorio para restaurar la sincronización de enlace ascendente.

LTE_IDLE es un estado de baja actividad en el que el terminal móvil reposa la mayoría del tiempo con el fin de reducir el consumo de batería. La sincronización de enlace ascendente no se mantiene y, por eso, la única actividad de transmisión de enlace ascendente que puede tener lugar es el acceso aleatorio para pasar a LTE_ACTIVE. El terminal móvil mantiene su(s) dirección/direcciones IP y otra información interna con el fin de pasar rápidamente a LTE_ACTIVE cuando sea necesario. La red conoce parcialmente la posición del terminal móvil de tal manera que la red conoce al menos el grupo de células en el que tiene que hacerse la búsqueda del terminal móvil.

Un procedimiento de acceso aleatorio de ejemplo no limitativo se ilustra en la figura 7 e incluye cuatro etapas denominadas etapas 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 de RACH y otra información en un mensaje de radiodifusión enviado de manera regular a través de un canal de radiodifusión explorado de manera regular por terminales móviles activos. En la etapa uno, después de que el terminal de usuario reciba y decodifique la información difundida por radio por la estación base (eNodoB), selecciona uno de los preámbulos de acceso aleatorio de estación base y lo transmite a través del RACH. La estación base supervisa el RACH y detecta el preámbulo que permite a la estación base estimar el tiempo de transmisión del terminal de usuario. Es necesaria la sincronización de enlace ascendente con el fin de permitir que el terminal transmita datos de enlace ascendente a la estación base.

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

La figura 8 ilustra de manera conceptual una transmisión de preámbulo de acceso aleatorio según la especificación de LTE a partir de este documento. Un ejemplo no limitativo para generar preámbulos adecuados se basa en secuencias de Zadoff-Chu (ZC) y secuencias cíclicamente desplazadas de las mismas. Las secuencias de Zadoff-Chu también pueden usarse, por ejemplo, para crear las señales de referencia de enlace ascendente incluidas en cada trama de datos para fines de estimación de canal.

Un terminal de usuario que lleva a cabo un intento de acceso aleatorio ha obtenido, previamente a la transmisión del preámbulo, sincronización de enlace descendente mediante un procedimiento de búsqueda de célula que usa información de temporización difundida por radio por la estación base. Pero tal como se explicó anteriormente, la temporización de enlace ascendente aún no se ha establecido. El inicio de una trama de transmisión de enlace ascendente en el terminal se define en relación con el inicio de la trama de transmisión de enlace descendente en el terminal. Debido al retardo de propagación entre la estación base y el terminal, la transmisión de enlace ascendente tendrá un retardo en relación con la temporización de transmisión de enlace descendente en la estación base. Dado que la distancia entre la estación base y el terminal no se conoce, existe incertidumbre en la temporización de enlace ascendente correspondiente a dos veces la distancia entre la estación base y el terminal. Para justificar esta incertidumbre y evitar la interferencia con subtramas posteriores que no se usan para acceso aleatorio, se usa un tiempo de guarda.

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

Si la estación base detecta múltiples intentos de acceso aleatorio (desde diferentes terminales de usuario), entonces los mensajes de respuesta de solicitud de acceso aleatorio 2 para múltiples terminales móviles pueden combinarse en una única transmisión. Por tanto, el mensaje de respuesta de solicitud de acceso aleatorio 2 se planifica en el DL-SCH y se indica en el canal físico de control de enlace descendente (PDCCH) usando una identidad común reservada para la respuesta de acceso aleatorio. El PDCCH es un canal de control usado 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 se encuentra el DL-SCH. Todos los terminales de usuario que transmitieron un preámbulo supervisan el PDCCH para una respuesta de acceso aleatorio transmitida usando la identidad común predefinida usada por la estación base para todas las respuestas de acceso aleatorio.

En la tercera etapa 3, el terminal de usuario transmite la información necesaria en el mensaje 3 a la red usando los recursos de enlace ascendente planificados asignados en el mensaje de respuesta de acceso aleatorio 2 y sincronizados en el enlace ascendente. Transmitir el mensaje de enlace ascendente en la etapa 3 de la misma manera que los datos de enlace ascendente planificados "normales", es decir, en el UL-SCH, en vez de vincularlos al preámbulo en la primera etapa, es beneficioso por diversos motivos. En primer lugar, la cantidad de información transmitida en ausencia de sincronización de enlace ascendente debe minimizarse ya que la necesidad de un tiempo de guarda largo hace que dichas transmisiones sean relativamente costosas. En segundo lugar, el uso de un esquema de transmisión de enlace ascendente "normal" para la transmisión de mensajes permite que el tamaño de concesión y el esquema de modulación se ajusten a, por ejemplo, diferentes condiciones de radio. En tercer lugar, permite una ARQ híbrida con combinación fácil para el mensaje de enlace ascendente que puede ser útil, especialmente en escenarios de cobertura limitada, ya que permite confiar en una o varias retransmisiones para recoger suficiente energía para la señalización de enlace ascendente para garantizar una probabilidad suficientemente alta de transmisión satisfactoria. El terminal móvil transmite su identidad de terminal móvil temporal, por ejemplo, un C-RNTI temporal, en la tercera etapa a la red usando el UL-SCH. El contenido exacto de esta señalización depende del estado del terminal, por ejemplo, si la red la conoce previamente o no.

Siempre que los terminales que realizaron acceso aleatorio al mismo tiempo usen secuencias de preámbulo diferentes, no se produce colisión. Pero hay una cierta probabilidad de contienda en la que múltiples terminales usan el mismo preámbulo de acceso aleatorio al mismo tiempo. En este caso, múltiples terminales reaccionan al mismo mensaje de respuesta de enlace descendente en la etapa 2 y se produce una colisión en la etapa 3. La resolución de colisión o contienda se realizan en la etapa 4.

En la etapa 4 se transmite un mensaje de resolución de contienda desde la estación base al terminal en el DL-SCH. Esta etapa resuelve la contienda en caso de que múltiples terminales intenten acceder al sistema en el mismo recurso, identificando qué terminal de usuario se detectó en la tercera etapa. Múltiples terminales que realizan intentos de acceso aleatorio simultáneos usando la misma secuencia de preámbulo en la etapa 1 atienden al mismo

mensaje de respuesta en la etapa 2 y, por tanto, tienen el mismo identificador de terminal de usuario temporal. Por tanto, en la etapa 4, cada terminal que recibe el mensaje de enlace descendente compara la identidad de terminal de usuario en el mensaje con la identidad de terminal de usuario que transmitieron en la tercera etapa. Solo un terminal de usuario que observa una coincidencia entre la identidad recibida en la cuarta etapa y la identidad transmitida como parte de la tercera etapa determina el procedimiento de acceso aleatorio como satisfactorio. Si aún no se ha asignado un C-RNTI al terminal, se promueve la identidad temporal de la segunda etapa al C-RNTI; en caso contrario, el terminal de usuario mantiene su C-RNTI ya asignado. Los terminales que no encuentran una coincidencia con la identidad recibida en la cuarta etapa deben reiniciar el procedimiento de acceso aleatorio desde la primera etapa.

Tal como se explicó anteriormente, la identidad de terminal de usuario incluida en el mensaje 3 se usa como parte del mecanismo de resolución de contienda en la cuarta etapa. Continuando el ejemplo no limitativo de LTE, si el terminal de usuario está en el estado de LTE_ACTIVE, es decir, está conectado a una célula conocida y por tanto tiene un C-RNTI asignado, este C-RNTI se usa como la identidad de terminal en el mensaje de enlace ascendente. De lo contrario, se usa un identificador de terminal de red central, y la estación base tiene que implicar a la red central antes de responder al mensaje de enlace ascendente en la etapa tres.

En este ejemplo de LTE no limitativo, solo la primera etapa usa procesamiento de capa física diseñado específicamente para acceso aleatorio. Las últimas tres etapas usan el mismo procesamiento de capa física como para la transmisión de datos de enlace ascendente y enlace descendente "normal", lo que simplifica la implementación tanto del terminal como de la estación base. Dado que el esquema de transmisión usado 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 de LTE no limitativo de ejemplo, las etapas generales de procesamiento descritas en la figura 2, que incluyen CRC, codificación, HARQ, cifrado, modulación y modulación de DFTS-OFDM, se aplican por el terminal de usuario al mensaje 3 en la figura 7 y las transmisiones de enlace ascendente posteriores desde ese terminal de usuario a la estación base (no hay cifrado en el mensaje de acceso aleatorio de enlace ascendente inicial en la etapa 1). Las diferentes secuencias de cifrado de enlace ascendente en el terminal dependen del tipo de transmisión de enlace ascendente. En cuanto al mensaje de acceso aleatorio 3, se usa un primer tipo de secuencia de cifrado, por ejemplo, un código de cifrado específico de célula o específico de canal de acceso aleatorio. En cuanto a transmisiones de datos "normales" posteriores en el enlace ascendente, es decir, cuando la estación base ha asignado una identidad no temporal al terminal, se usa un segundo tipo de secuencia de cifrado, por ejemplo, un código de cifrado específico de terminal. Puede usarse un enfoque de dos tipos similar para señales de referencia de enlace ascendente usadas por la estación base para la estimación de canal: un primer tipo, por ejemplo, una señal de referencia específica de acceso aleatorio o célula para el mensaje de acceso aleatorio 3, seguido por un segundo tipo, por ejemplo, una secuencia de señal de referencia de enlace ascendente asociada o asignada a una estación base para seguir transmisiones de datos "normales".

Cuando la estación base asigna una secuencia de cifrado y/o secuencia de referencia al terminal móvil, esa secuencia de referencia y/o secuencia de cifrado específica de terminal se usa(n) para todas las transmisiones de datos de enlace ascendente posteriores para esa conexión de enlace ascendente particular. La secuencia de cifrado y/o secuencia de referencia que va a usarse puede estar o bien configurada explícitamente en el terminal móvil o ligada a la identidad de terminal (por ejemplo, un C-RNTI) que la estación base asigna a un terminal móvil.

En lo anterior, el terminal de usuario usa una secuencia de cifrado específica de célula para cifrar el mensaje 3 dado que antes de realizar el acceso aleatorio, el terminal de usuario ha decodificado la información de radiodifusión de la estación base/célula y, por tanto, conoce la identidad de la célula a la que está accediendo, los preámbulos de acceso aleatorio asociados con esa célula, y números de referencia y/o secuencias de cifrado específicos de célula. Siempre que a múltiples terminales que realizan acceso aleatorio al mismo tiempo se les asignen recursos de tiempo/frecuencia diferentes para su mensaje de acceso aleatorio de enlace ascendente 3 respectivo, no hay interferencia entre esos usuarios y la falta de aleatorización entre usuarios no supone un problema.

En una realización no limitativa, un mapeo uno a uno se introduce entre la secuencia de preámbulo de acceso aleatorio usada en el mensaje de solicitud de acceso aleatorio enviado en la etapa 1 de la figura 7 y la secuencia de cifrado usada para cifrar el mensaje de acceso aleatorio enviado en la etapa 3. Dado que tanto la estación base como el terminal de usuario conocen el preámbulo usado para el mensaje de solicitud de acceso aleatorio enviado en la etapa 1 por el mensaje de tiempo 3 que va a transmitirse, ambos conocen qué secuencia de cifrado usar.

En otra realización no limitativa, la estación base asigna la secuencia de cifrado para que el terminal de usuario la use para cifrar el mensaje 3 como una parte de la respuesta de solicitud de acceso aleatorio transmitida en la etapa 2 de la figura 7, (es decir, antes de la transmisión del mensaje 3). Como ejemplo, esto puede hacerse estableciendo un mapeo uno a uno entre el identificador de usuario temporal enviado en el mensaje 2, por ejemplo, un C-RNTI temporal, y la secuencia de cifrado que va a usarse.

Aún otra realización no limitativa vincula la secuencia de cifrado que va a usarse por el terminal de usuario para

cifrar el mensaje 3 al/a los recurso(s) de tiempo-frecuencia usados por el terminal de usuario para transmitir el preámbulo de acceso aleatorio (mensaje 1). En este caso, tanto la estación base como el terminal de usuario conocerán la secuencia de cifrado porque ambos conocen los recursos de tiempo-frecuencia usados 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 recursos de tiempo/frecuencia diferentes para su propio mensaje de acceso aleatorio 3, no habrá interferencia entre esos usuarios y la falta de aleatorización entre usuarios no supone un problema.

5
10 También pueden usarse 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 las cuatro realizaciones también pueden usarse para los números de referencia de enlace ascendente usados para la estimación de canal de enlace ascendente. En otras palabras, puede usarse un tipo general o compartido de número de referencia para el mensaje de acceso aleatorio de enlace ascendente 3, y puede usarse otro número de referencia de tipo específico de terminal para comunicaciones de enlace ascendente posteriores asociadas con la conexión.

15 Puede haber situaciones en las que al terminal de usuario ya se le ha asignado una identidad pero todavía tiene la necesidad de realizar un acceso aleatorio. Un ejemplo es cuando el terminal se registra en la red, pero pierde la sincronización en el enlace ascendente y, por consiguiente, necesita realizar un intento de acceso aleatorio para recuperar la sincronización de enlace ascendente. Aunque el terminal de usuario tiene una identidad asignada, el cifrado específico de terminal no puede usarse 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, tiene que usarse una secuencia de cifrado asociada a célula en vez de una secuencia de cifrado específica de terminal obsoleta.

20
25 Por consiguiente, los beneficios del cifrado específico de terminal para la transmisión de datos normal se mantienen sin afectar a la funcionalidad del procedimiento de acceso aleatorio. Tal como se describió anteriormente, el cifrado específico de terminal aleatoriza la interferencia, lo que mejora el rendimiento de transmisión de enlace ascendente y proporciona flexibilidad adicional en el diseño de planificación.

30 Aunque se han mostrado y descrito en detalle diversas realizaciones, las reivindicaciones no se limitan a ninguna realización o ejemplo particular. Por ejemplo, aunque se han descrito principalmente en cuanto a secuencias de cifrado, los dos tipos de enfoque descritos para secuencias de cifrado de acceso aleatorio también pueden usarse para determinar las secuencias de señales de referencia enviadas en cada trama de enlace ascendente que se usan por el receptor de estación base para fines de estimación de canal de enlace ascendente. Ninguna de las descripciones anteriores debe entenderse como que implica que cualquier elemento, etapa, intervalo o función particular es esencial de tal manera que debe incluirse en el alcance de las reivindicaciones. El alcance del contenido patentado se define solo por las reivindicaciones.

40

REIVINDICACIONES

1. Procedimiento implementado en un terminal de usuario para acceder a un canal de radio, que comprende:
 - 5 transmitir un preámbulo de acceso aleatorio que usa un recurso de radio de canal de acceso aleatorio a una estación base de radio;
 - 10 recibir un mensaje de respuesta de acceso aleatorio desde la estación base de radio, en el que el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador de terminal de usuario que indica una secuencia de cifrado que no está asignada específicamente a ningún terminal de usuario;
 - 15 determinar una secuencia de cifrado de enlace ascendente en función del identificador de terminal de usuario incluido en el mensaje de respuesta de acceso aleatorio;
 - 20 transmitir un mensaje 3 a la estación base de radio, en el que el mensaje 3 incluye una identidad de terminal de usuario, y en el que el mensaje 3 se transmite a través del recurso de radio identificado, y en el que el mensaje 3 se cifra usando la secuencia de cifrado de enlace ascendente determinada;
 - 25 recibir un mensaje desde la estación base de radio, que incluye la identidad de terminal de usuario; y
 - 30 transmitir una transmisión de datos posterior cifrada con una secuencia de cifrado de enlace ascendente en función de la identidad de terminal de usuario.
2. Procedimiento según la reivindicación 1, en el que el terminal de usuario se comunica con una red de comunicaciones por radio de evolución a largo plazo, y en el que el preámbulo de acceso aleatorio se transmite a través de un canal de acceso aleatorio y en el que el mensaje 3 se transmite a través de un canal compartido de enlace ascendente.
3. Procedimiento según cualquiera de las reivindicaciones 1-2, en el que el mensaje de respuesta de acceso aleatorio indica adicionalmente un cambio de temporización y en el que el procedimiento comprende adicionalmente:
 - 35 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
 - 40 en el que el mensaje 3 se transmite en función de la temporización ajustada.
4. Procedimiento según cualquiera de las reivindicaciones 1-3, en el que determinar una secuencia de cifrado de enlace ascendente en función del identificador de terminal de usuario incluido en el mensaje de respuesta de acceso aleatorio comprende:
 - 45 establecer un mapeo uno a uno entre el identificador de terminal de usuario y la secuencia de cifrado de enlace ascendente.
5. Procedimiento implementado en una estación base de radio para responder a terminales de usuario que solicitan servicio de la estación base de radio a través de un canal de radio, que comprende:
 - 50 recibir un preámbulo de acceso aleatorio a través de un recurso de radio de canal de acceso aleatorio desde un terminal de usuario;
 - 55 transmitir un mensaje de respuesta de acceso aleatorio al terminal de usuario, en el que el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador de terminal de usuario, en el que el identificador de terminal de usuario indica una secuencia de cifrado de enlace ascendente que no está asignada específicamente a ningún terminal de usuario;
 - 60 recibir a través del recurso de radio identificado un mensaje 3 desde el terminal de usuario que incluye una identidad de terminal de usuario, en el que el mensaje 3 se cifra con una secuencia de cifrado de enlace ascendente tal como se indica en el mensaje de respuesta de acceso aleatorio;
 - 65 transmitir un mensaje al terminal de usuario que incluye la identidad de terminal de usuario; y
 - recibir una transmisión de datos posterior desde el terminal de usuario cifrado con una secuencia de cifrado de enlace ascendente en función de la identidad de terminal de usuario.
6. Procedimiento según la reivindicación 5, en el que la estación base de radio es parte de una red de

comunicaciones por radio de evolución a largo plazo, y en el que el preámbulo de acceso aleatorio se recibe a través de un canal de acceso aleatorio y en el que el mensaje 3 se recibe a través de un canal compartido de enlace ascendente.

- 5 7. Procedimiento según cualquiera de las reivindicaciones 5-6, en el que el mensaje de respuesta de acceso aleatorio indica adicionalmente un cambio de temporización.
8. Terminal de usuario para solicitar servicio de una estación base de radio que tiene un área de células donde la estación base de radio ofrece servicios de comunicaciones por radio, comprendiendo el terminal de usuario:
- 10 un transmisor de radio configurado para transmitir un preámbulo de acceso aleatorio usando un recurso de radio de canal de acceso aleatorio a la estación base de radio;
- 15 un receptor de radio configurado para recibir un mensaje de respuesta de acceso aleatorio desde la estación base de radio, en el que el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador de terminal de usuario que indica una secuencia de cifrado que no está asignada específicamente a un terminal de usuario;
- 20 un conjunto de circuitos de procesamiento electrónico configurado para determinar una secuencia de cifrado de enlace ascendente basándose en el identificador de terminal de usuario incluido en el mensaje de respuesta de acceso aleatorio;
- 25 en el que el transmisor de radio está configurado para transmitir un mensaje 3 a la estación base de radio, en el que el mensaje 3 incluye una identidad de terminal de usuario, el mensaje 3 se transmite a través del recurso de radio identificado, y el mensaje 3 se cifra usando la secuencia de cifrado de enlace ascendente determinada;
- 30 en el que el receptor de radio está configurado para recibir un mensaje desde la estación base de radio, que incluye la identidad de terminal de usuario; y
- 35 en el que el transmisor de radio está configurado para transmitir una transmisión de datos posterior en el enlace ascendente cifrado con una secuencia de cifrado de enlace ascendente basándose en la identidad de terminal de usuario.
9. Terminal de usuario según la reivindicación 8, en el que el terminal de usuario está configurado para comunicarse con una red de comunicaciones por radio de evolución a largo plazo, y
- 40 en el que el transmisor de radio está configurado para transmitir el preámbulo de acceso aleatorio a través de un canal de acceso aleatorio y el mensaje 3 a través de un canal compartido de enlace ascendente.
10. Terminal de usuario según cualquiera de las reivindicaciones 8-9, en el que el mensaje de respuesta de acceso aleatorio indica adicionalmente un cambio de temporización, y en el que el conjunto de circuitos de procesamiento electrónico está configurado para ajustar una temporización en el terminal de usuario para transmitir señales a la estación base de radio basándose en el cambio de temporización recibido en el mensaje de respuesta de acceso aleatorio de radio, y en el que el transmisor de radio está configurado para transmitir el mensaje 3 basándose en la temporización ajustada.
- 45 11. Terminal de usuario según cualquiera de las reivindicaciones 8-10, en el que el conjunto de circuitos de procesamiento electrónico está configurado para determinar la secuencia de cifrado de enlace ascendente estableciendo un mapeo uno a uno entre el identificador de terminal de usuario y la secuencia de cifrado de enlace ascendente.
- 50 12. Estación base de radio configurada para asociarse con una célula para responder a terminales de usuario que solicitan servicio de la estación base de radio a través de un canal de radio, que comprende un conjunto de circuitos configurado para:
- 55 recibir un preámbulo de acceso aleatorio a través de un recurso de radio de canal de acceso aleatorio desde un terminal de usuario;
- 60 transmitir un mensaje de respuesta de acceso aleatorio al terminal de usuario, en el que el mensaje de respuesta de acceso aleatorio indica un recurso de radio identificado y un identificador de terminal de usuario, y en el que el identificador de terminal de usuario indica una secuencia de cifrado de enlace ascendente que no está asignada específicamente al terminal de usuario;
- 65 recibir desde el terminal de usuario a través del recurso de radio identificado un mensaje 3 cifrado con la

secuencia de cifrado de enlace ascendente, en el que el mensaje 3 incluye una identidad de terminal de usuario;

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

recibir una transmisión de datos posterior desde el terminal de usuario cifrada con una secuencia de cifrado de enlace ascendente en función de la identidad de terminal de usuario.

10 13. Estación base de radio según la reivindicación 12, en la que la estación base de radio es parte de una red de comunicaciones por radio de evolución a largo plazo, y en la que el conjunto de circuitos está configurado para recibir el preámbulo de acceso aleatorio a través de un canal de acceso aleatorio y el mensaje 3 a través de un canal compartido de enlace ascendente.

15 14. Estación base de radio según cualquiera de las reivindicaciones 12-13, en la que el mensaje de respuesta de acceso aleatorio indica adicionalmente un cambio de temporización.

20 15. Procedimiento o dispositivo según cualquiera de las reivindicaciones anteriores, en el que el identificador de terminal de usuario es un identificador temporal de red de radio celular temporal y/o en el que la identidad de terminal de usuario es un identificador temporal de red de radio celular.

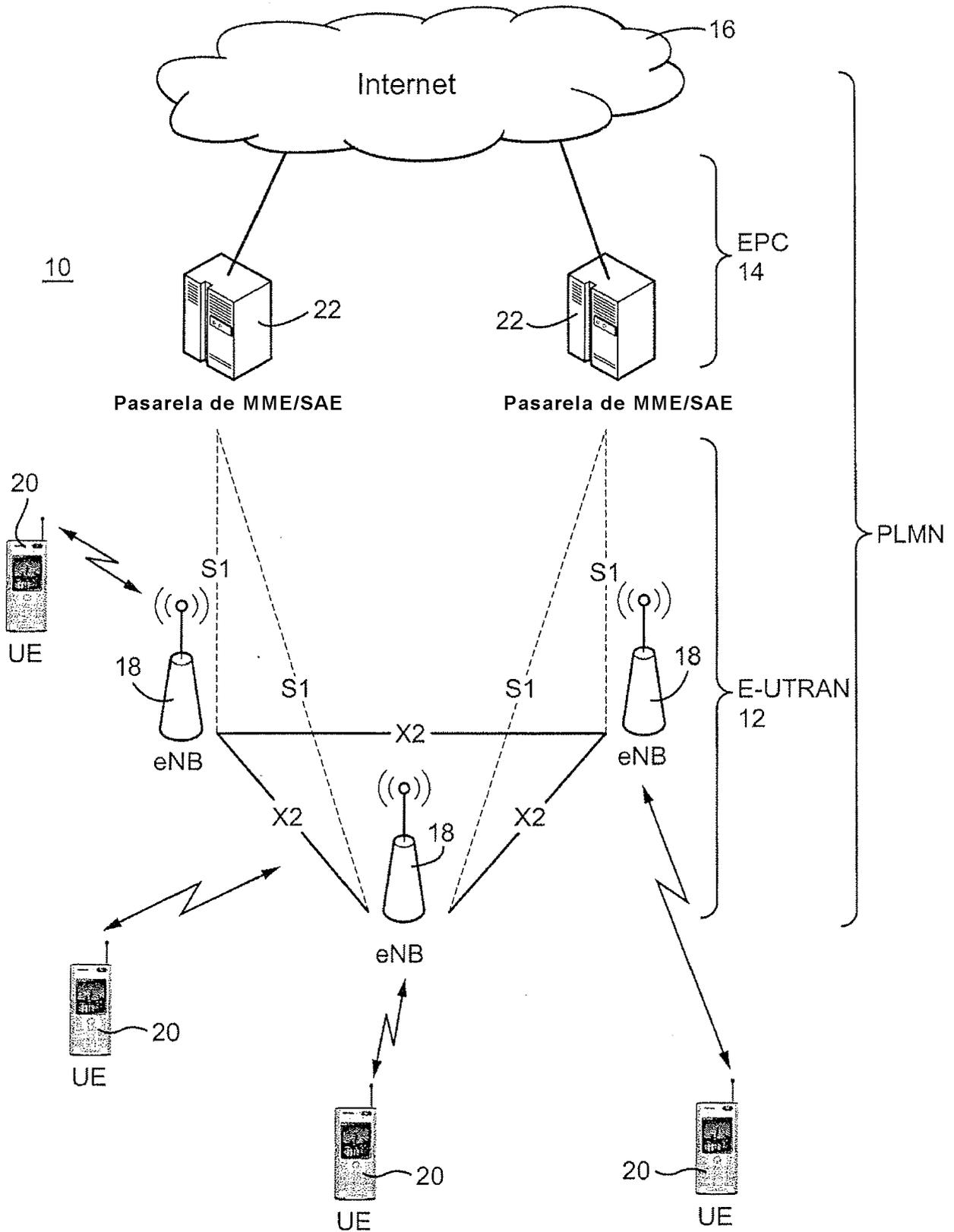
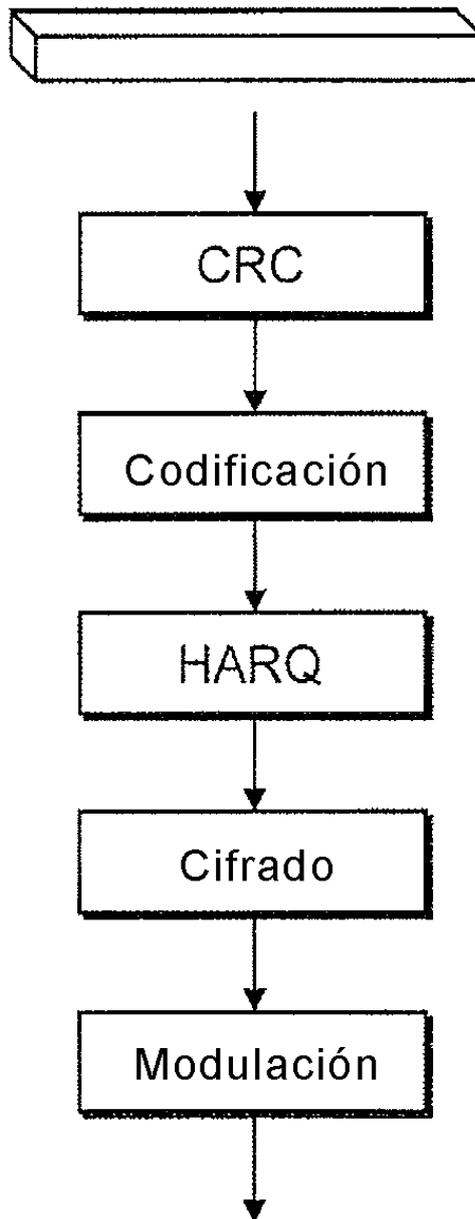


Figura 1

*Bloque de transporte de tamaño dinámico
emitido desde la capa de MAC*



*A modulación de DFT-S-OFDM que incluye
mapeo al recurso de frecuencia asignado*

Figura 2

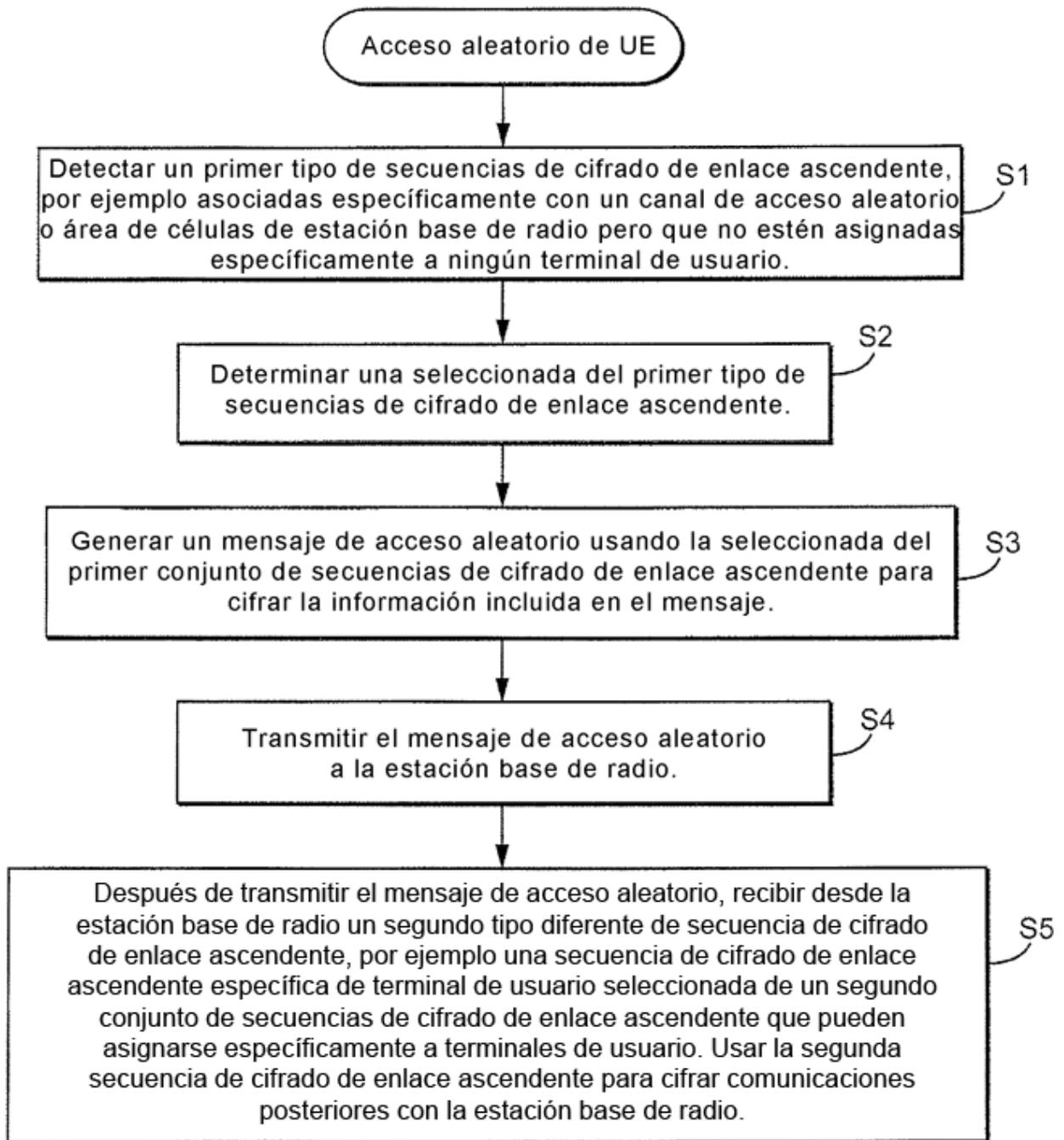


Figura 3

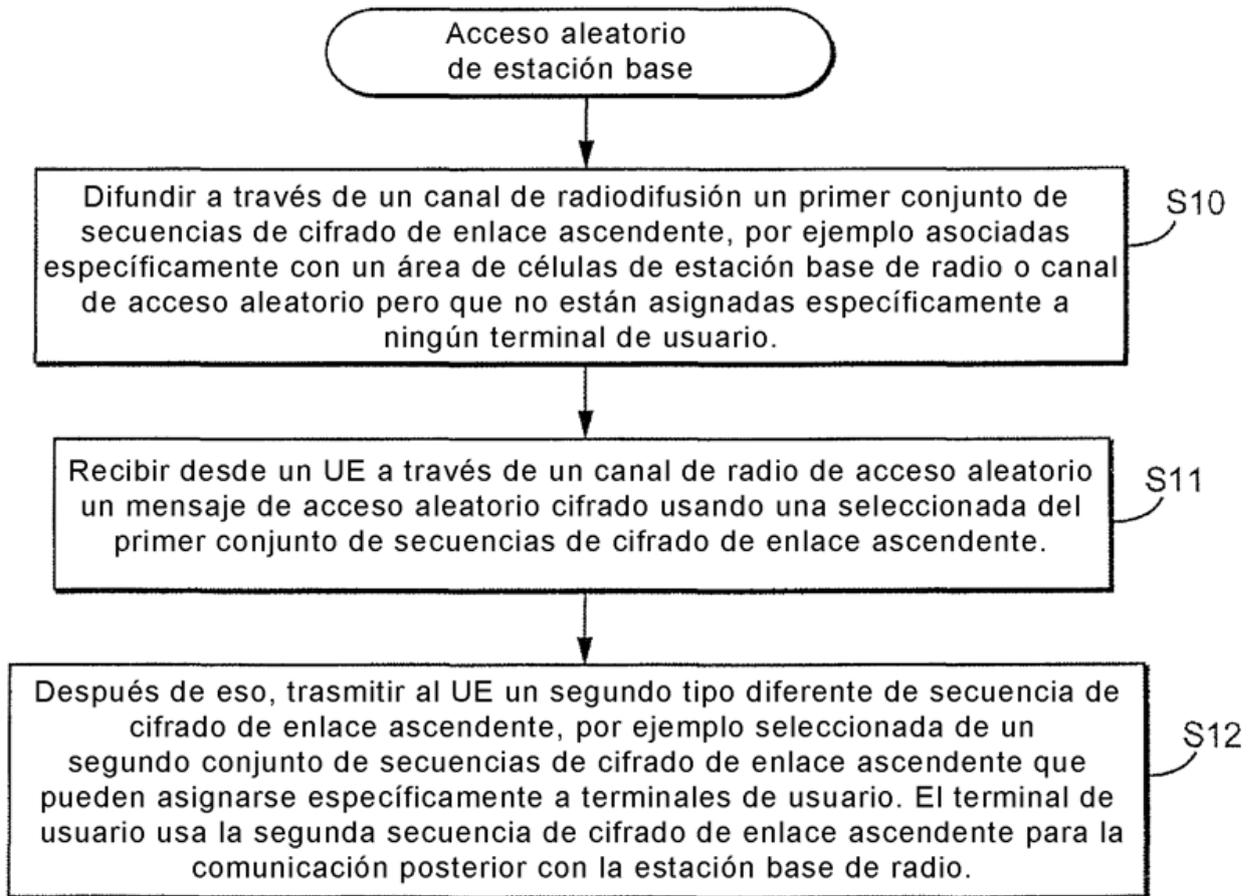


Figura 4

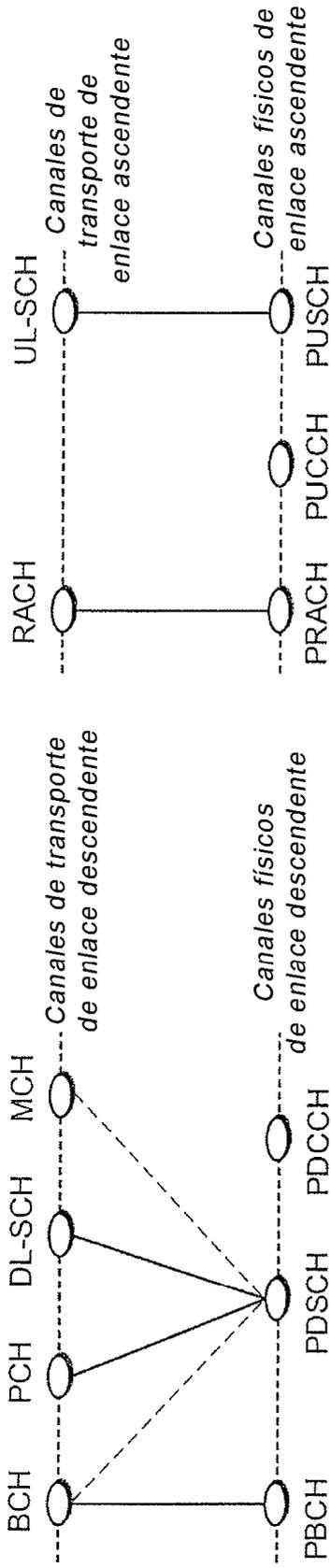


Figura 5B

Figura 5A

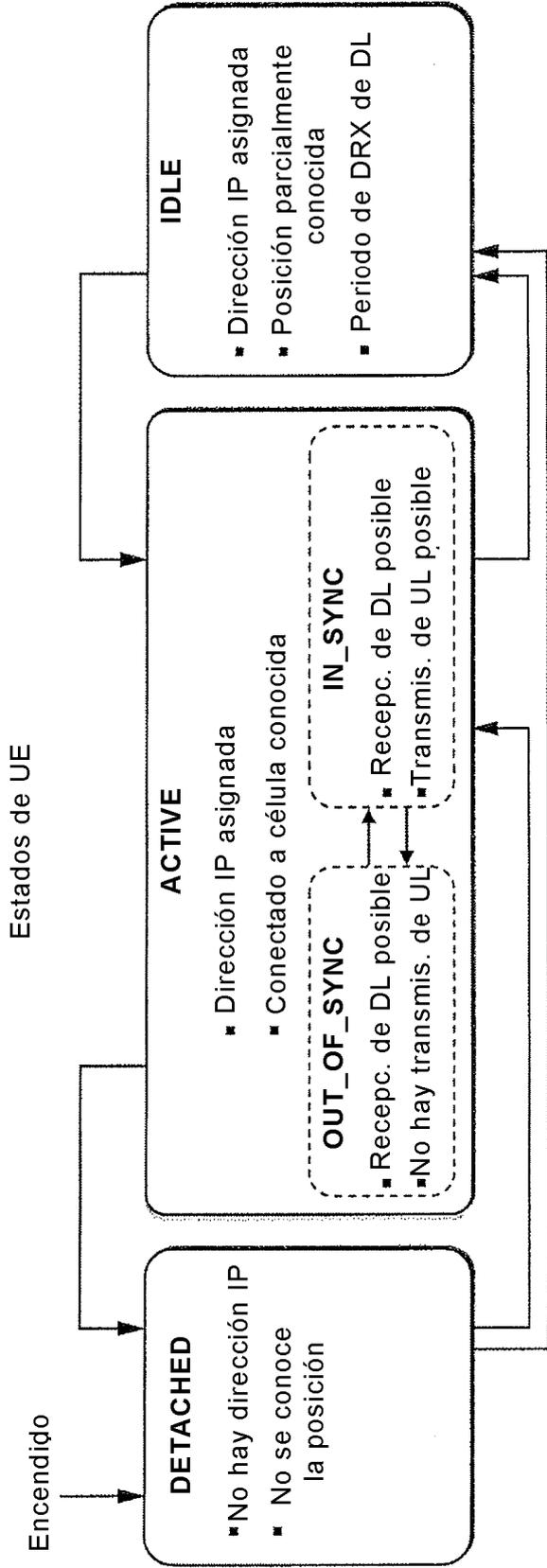


Figura 6

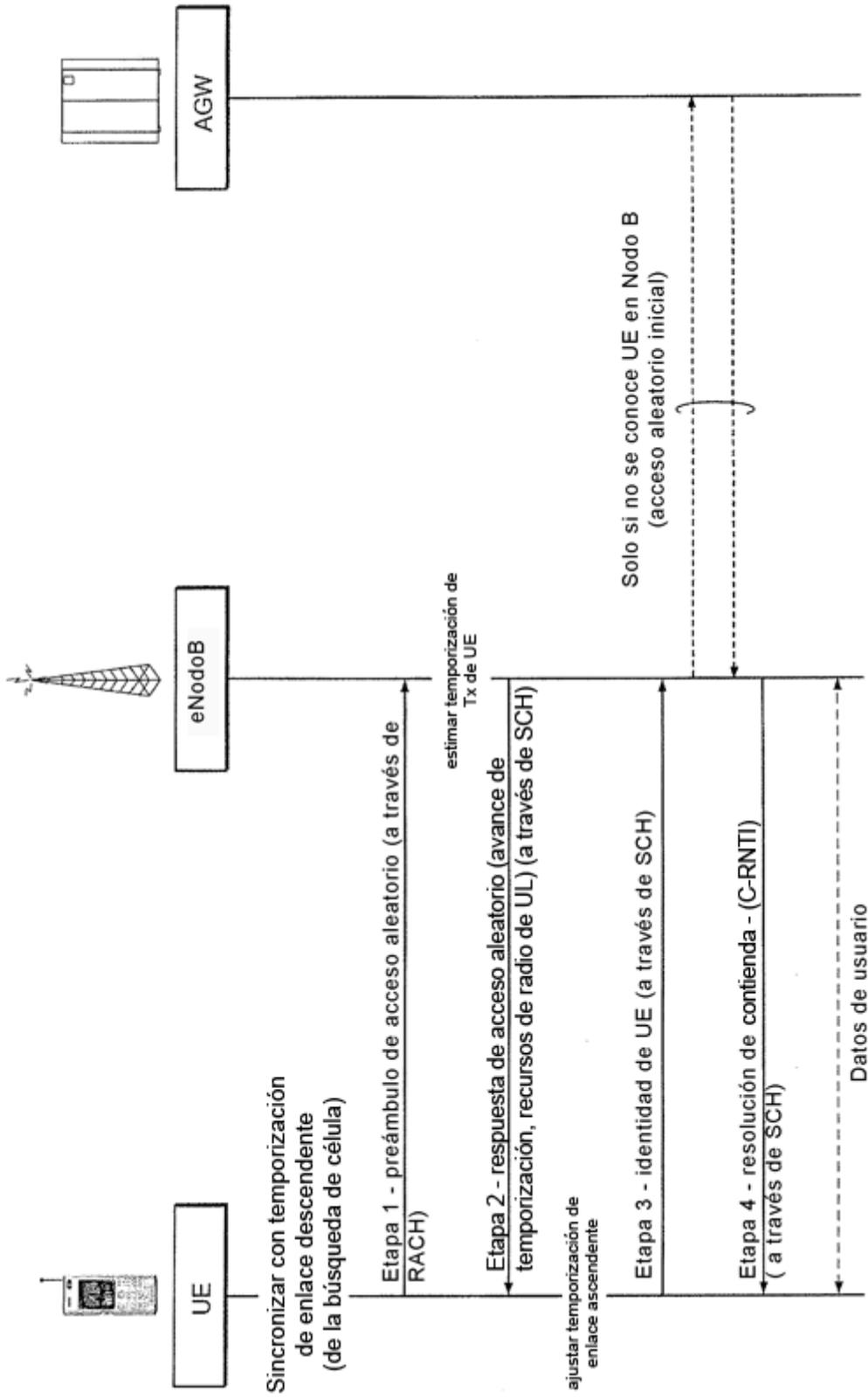


Figura 7

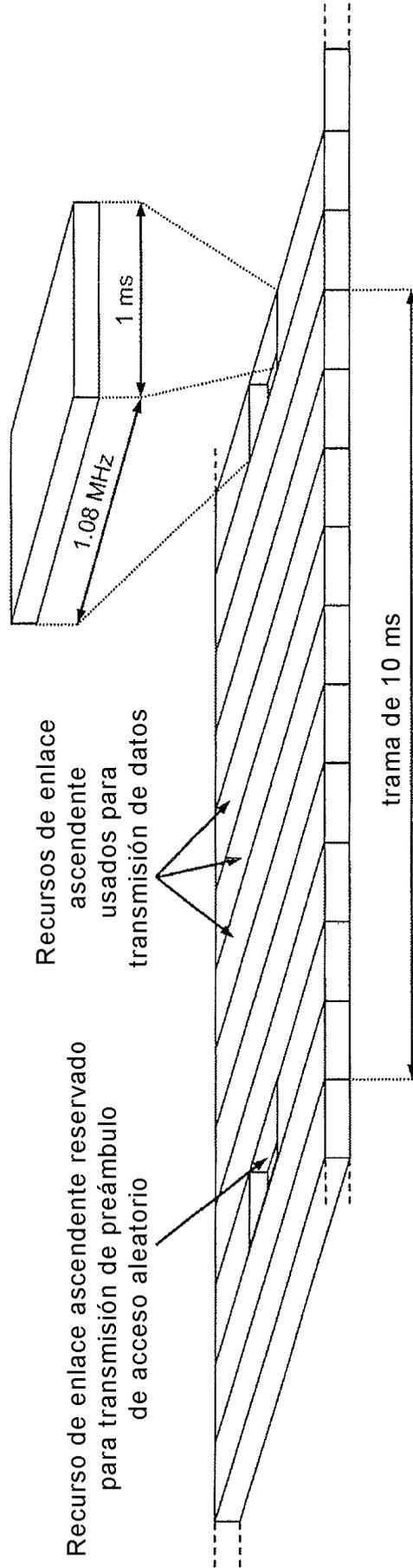


Figura 8

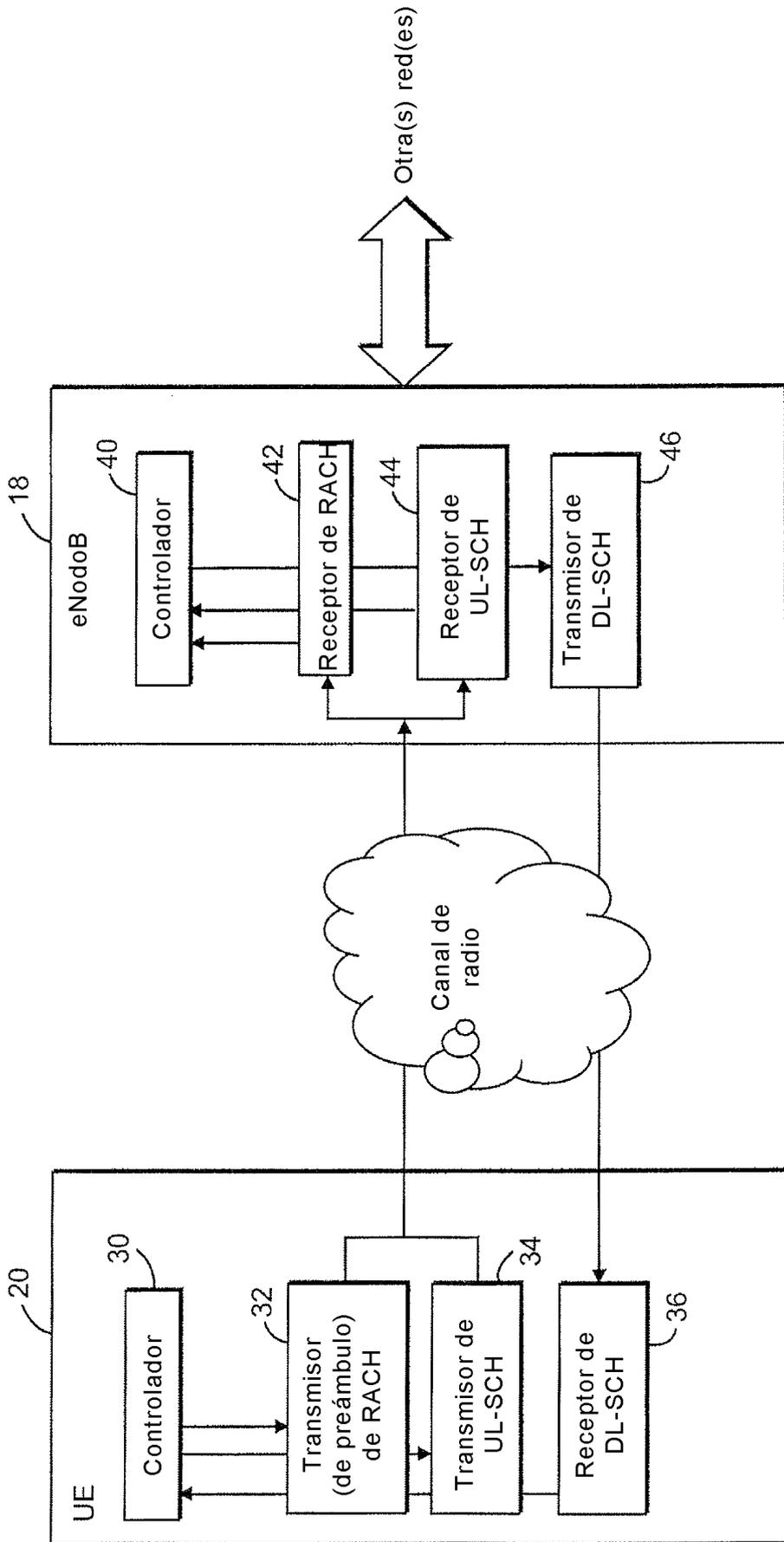


Figura 9