(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 823**

(51) Int. CI.:
H04W 74/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09155078 .0**
(96) Fecha de presentación: **13.03.2009**
(97) Número de publicación de la solicitud: **2101539**
(97) Fecha de publicación de la solicitud: **16.09.2009**

(54) Título: **Método de acceso aleatorio y terminal para mejorar la eficacia de encriptación**

(30) Prioridad:
13.03.2008 US 36455 P
21.03.2008 US 38470 P
28.04.2008 US 48549 P
27.02.2009 KR 20090016820

(45) Fecha de publicación de la mención BOPI:
02.04.2012

(45) Fecha de la publicación del folleto de la patente:
02.04.2012

(73) Titular/es:
LG ELECTRONICS INC.
20, YEOUIDO-DONG YEONGDEUNGPO-GU
SEOUL 150-721, KR

(72) Inventor/es:
Park, Sung Jun;
Yi, Seung June;
Lee, Young Dae y
Chun, Sung Duck

(74) Agente/Representante:
Veiga Serrano, Mikel

DESCRIPCIÓN

Método de acceso aleatorio y terminal para mejorar la eficacia de encriptación

Sector de la técnica

La presente invención se refiere a un método de acceso aleatorio para mejorar la eficacia de encriptación y, más particularmente, a un aparato para mejorar el rendimiento de encriptación/desencriptación y método del mismo. Aunque la presente invención es adecuada para una amplia gama de aplicaciones, es particularmente adecuada para mejorar el rendimiento de encriptación/desencriptación realizadas en un procedimiento de acceso aleatorio dentro de un sistema de comunicación móvil.

Estado de la técnica

En primer lugar, el sistema de comunicación de evolución a largo plazo LTE de 3GPP (proyecto de asociación de tercera generación): a continuación en el presente documento denominado 'LTE') se describe esquemáticamente como un sistema de comunicación móvil al que la presente invención es aplicable.

La figura 1 es un diagrama esquemático de una estructura de red de E-UMTS como un ejemplo de un sistema de comunicación móvil.

En referencia a la figura 1, el E-UMTS (sistema universal de telecomunicaciones móviles evolucionado) es el sistema que ha evolucionado desde UMTS (sistema universal de telecomunicaciones móviles) y su normalización básica está en marcha por 3GPF. Generalmente, el E-UMTS puede denominarse sistema de LTE.

La red de E-UMTS puede dividirse principalmente en E-TRAN (101) y CN (102) (red central). La E-UTRAN (red de acceso radio terrestre de UMTS evolucionado) (101) consiste en un equipo de usuario (a continuación en el presente documento abreviado como UE) (103), una estación base (a continuación en el presente documento denominada eNodo B o eNB) (104), y una pasarela de acceso (a continuación en el presente documento abreviada como AG) (105) ubicada en un punto de extremo de la red para conectarse externamente a una red externa. La AG (105) puede dividirse en una parte responsable del procesamiento de tráfico de usuario y la otra parte para procesar tráfico de control. En este caso, la AG para procesamiento de nuevo tráfico de usuario y la AG para procesar tráfico de control pueden comunicarse entre sí usando una nueva interfaz.

Puede existir al menos una célula en un eNodo B. Entre eNodos B puede usarse una interfaz para la transmisión de tráfico de control o usuario. Asimismo, la CN (102) puede consistir en un nodo para registros de usuario de la AG (105) y otro UE (103). Además, está disponible una interfaz para discriminar la E-UTRAN (101) y la CN (102).

Las capas de un protocolo de interfaz de radio entre un equipo de usuario y una red pueden dividirse en L1 (primera capa), L2 (segunda capa) y L3 (tercera capa) basándose en tres capas inferiores del modelo de referencia de interconexión de sistemas abiertos (OSI) ampliamente conocido en el campo de los sistemas de comunicación. Una capa física que pertenece a la primera capa proporciona un servicio de transferencia de información usando un canal físico. Un control de recursos de radio (a continuación en el presente documento abreviado como RRC) ubicado en la tercera capa desempeña un papel en el control de recursos de radio entre el equipo de usuario y la red. Para esto, las capas de RRC intercambian mensajes de RRC entre el equipo de usuario y la red. Las capas de RRC pueden distribuirse a nodos de red incluyendo el eNodo B (104), la AG (105) y similares. Además, la capa de RRC puede proporcionarse sólo al eNodo B (104) o a la AG (105).

La figura 2 y la figura 3 son diagramas de estructuras de un protocolo de interfaz de radio entre un equipo de usuario y UTRAN basándose en las especificaciones de red de acceso de radio de 3GPP.

En referencia a la figura 2 y la figura 3, un protocolo de interfaz de radio horizontalmente consiste en una capa física, una capa de enlace de datos y una capa de red. Asimismo, el protocolo de interfaz de radio verticalmente consiste en un plano de usuario para transferencia de información de datos y un plano de control para la entrega de señales de control (señalización). En particular, la figura 2 muestra las capas respectivas del plano de control de protocolo de radio y la figura 3 muestra las capas respectivas del plano de usuario de protocolo de radio. Las capas de protocolo de radio mostradas en la figura 2 y la figura 3 pueden dividirse en L1 (primera capa), L2 (segunda capa) y L3 (tercera capa) basándose en tres capas inferiores del modelo de referencia de interconexión de sistemas abiertos (OSI) ampliamente conocido en el campo de los sistemas de comunicación.

Las capas respectivas del plano de control de protocolo de radio mostradas en la figura 2 y las capas respectivas del plano de usuario de protocolo de radio mostradas en la figura 3 se explican de la siguiente manera.

En primer lugar, una capa física (PHY) de una primera capa proporciona una capa superior con un servicio de transferencia de información usando un canal físico. La capa física (PHY) está conectada a una capa de control de acceso al medio (MAC) en una capa superior a través de un canal de transporte. Asimismo, los datos se transportan

entre la capa de control de acceso al medio (MAC) y la capa física (PHY) a través del canal de transporte. En este caso, el canal de transporte puede clasificarse en un canal de transporte dedicado o un canal de transporte común según si un canal se comparte o no. Además, los datos se transportan a través del canal físico entre diferentes capas físicas, es decir, entre una capa física de un lado de transmisión y una capa física de un lado de recepción.

Existen diversas capas en la segunda capa. En primer lugar, una capa de control de acceso al medio (a continuación en el presente documento abreviado como 'MAC') desempeña un papel en la correlación de diversos canales lógicos con diversos canales de transporte. Asimismo, la capa de MAC también desempeña un papel como una multiplexación de canal lógico en la correlación de varios canales lógicos con un canal de transporte. La capa de MAC se conecta a una capa de control de enlace radio (RLC) de una capa superior a través de un canal lógico. Asimismo, el canal lógico puede clasificarse principalmente en un canal de control para transferir información de un plano de control y un canal de tráfico para transferir información de un plano de usuario según el tipo de la información transferida.

Un control de enlace radio (a continuación en el presente documento abreviado como RLC) de la segunda capa realiza segmentación y concatenación en los datos recibidos desde una capa superior para desempeñar un papel en el ajuste de un tamaño de los datos para que sean adecuados para una capa inferior para transferir los datos a una sección de radio. Asimismo, la capa de RLC proporciona tres clases de modos de RLC que incluyen un modo transparente (a continuación en el presente documento abreviado como TM), un modo sin acuse de recibo (a continuación en el presente documento abreviado como UM) y un modo con acuse de recibo (a continuación en el presente documento abreviado como AM) para garantizar diversas clases de QoS demandada por cada portadora de radio (a continuación en el presente documento abreviada como RB). En particular, el AM RLC realiza una función de retransmisión mediante petición y repetición automática (ARQ) para la transferencia de datos fiable.

Una capa de protocolo de convergencia de datos en paquetes (a continuación en el presente documento abreviado como PDCP) de la segunda capa realiza una función de compresión de cabecera para reducir un tamaño de una cabecera de paquete IP que contiene información de control relativamente grande e innecesaria para transmitir de manera eficaz tal paquete de IP como IPv4 e IPv6 en una sección de radio que tiene un ancho de banda pequeño. Esto permite que una parte de cabecera de datos lleve información obligatoria sólo para desempeñar un papel en el aumento de la eficacia de transmisión de la sección de radio. Además, en el sistema de LTE, la capa de PDCP también realiza una función de seguridad. Consiste en un cifrado para impedir la intercepción de datos efectuada por una tercera parte y protección de integridad para impedir la manipulación de datos efectuada por una tercera parte.

Una capa de control de recursos de radio (a continuación en el presente documento abreviado como RRC) ubicada en la parte más superior de una tercera capa se define sólo en el plano de control y es responsable de controlar un canal lógico, un canal de transporte y canales físicos en asociación con la configuración, reconfiguración y liberación de portadoras de radio (a continuación en el presente documento abreviadas como RB). En este caso, la RB significa un trayecto lógico proporcionado por las capas primera y segunda del protocolo de radio para la entrega de datos entre el equipo de usuario y la UTRAN. Generalmente, la configuración de una RB significa estipular características de canales y capas de protocolo de radio requeridas para proporcionar un servicio específico y también significa configurar parámetros detallados y métodos operativos de los mismos. La RB puede clasificarse en una RB de señalización (SRB) o una RB de datos (DRB). La SRB se usa como un trayecto para enviar un mensaje de RRC en un plano de control (plano C) y la DRB se usa como un trayecto para transferir datos de usuario en un plano de usuario (plano U).

Como un canal de transporte de enlace descendente para transportar datos a un equipo de usuario desde una red, hay un canal de difusión (BCH) para transmitir información de sistema y un canal compartido de enlace descendente (SCH) para transmitir un tráfico de usuario o un mensaje de control. Multidifusión de enlace descendente, tráfico de un servicio de difusión o un mensaje de control pueden transmitirse en SCH de enlace descendente o un MCH (canal de multidifusión) de enlace descendente separado. Mientras tanto, como un canal de transporte de enlace ascendente para transmitir datos a una red desde un equipo de usuario, hay un canal de acceso aleatorio (RACH) para transmitir un mensaje de control inicial o un canal compartido de enlace ascendente (SCH) para transmitir tráfico de usuario o un mensaje de control.

Como un canal físico de enlace descendente para transmitir información transferida en un canal de transporte de enlace descendente a una sección de radio entre una red y un equipo de usuario, hay un canal de difusión físico para transmitir información de BCH, un canal de multidifusión físico (PMCH) para transmitir información de MCH, un canal compartido de enlace descendente físico para transmitir información de PCH y SCH de enlace descendente o un control de enlace descendente físico (o denominado canal de control L1/L2 de DL) para transmitir información de control proporcionada por las capas primera y segunda.

Como un canal físico de enlace ascendente para transmitir información reenviada en un canal de transporte de enlace ascendente a una sección de radio entre una red y un equipo de usuario, hay un canal compartido de enlace ascendente físico (PUSCH) para transmitir información de SCH de enlace ascendente, un canal de acceso aleatorio físico (PRACH) para transmitir información de RACH o un canal de control de enlace ascendente físico (PUCCH)

para transmitir tal información de control, que se proporciona por las capas primera y segunda, como HARQ ACK, HARQ NACK, petición de planificación (SR), informe de indicador de calidad de canal (CQI) y similares.

Basándose en la descripción anterior, un procedimiento de acceso aleatorio proporcionado por el sistema de LTE se explica esquemáticamente de la siguiente manera.

En primer lugar, un equipo de usuario realiza un procedimiento de acceso aleatorio si se produce uno de los siguientes casos.

- El equipo de usuario realiza un acceso inicial sin una conexión de RRC con una estación base.

- El equipo de usuario inicialmente accede a una célula objetivo en un proceso de traspaso.

- Se solicita un proceso de acceso aleatorio según una orden dada por una estación base.

- Los datos que van a transmitirse en enlace ascendente se generan cuando no coincide la sincronización de tiempo de enlace ascendente o no se asigna un recurso de radio asignado para solicitar un recurso de radio.

- El proceso de reconstrucción se realiza en caso de fallo de enlace de radio o fallo de traspaso.

Al seleccionar un preámbulo de acceso aleatorio, el sistema de LTE proporciona tanto un procedimiento de acceso aleatorio basado en contienda y un procedimiento de acceso aleatorio no basado en contienda. En el procedimiento de acceso aleatorio basado en contienda, un equipo de usuario selecciona de manera aleatoria un preámbulo de un grupo de secuencias específico y luego usa el preámbulo seleccionado de manera aleatoria en la transmisión del preámbulo de acceso aleatorio. En el procedimiento de acceso aleatorio no basado en contienda, sólo se usa un preámbulo de acceso aleatorio asignado a un equipo de usuario específico por una estación base. Sin embargo, el procedimiento de acceso aleatorio no basado en contienda está disponible sólo en el procedimiento de traspaso descrito anteriormente o si se solicita por la orden dada por la estación base.

Mientras tanto, un proceso para que un equipo de usuario realice un acceso aleatorio a una estación base específica puede incluir principalmente las etapas de: (1) transmitir un preámbulo de acceso aleatorio a una estación base desde un equipo de usuario (a continuación en el presente documento denominado etapa de transmisión de 'mensaje 1' si no se confunde); (2) recibir una respuesta de acceso aleatorio desde la estación base en correspondencia con el preámbulo de acceso aleatorio transmitido (a continuación en el presente documento denominado etapa de recepción de 'mensaje 2' si no se confunde); (3) transmitir un mensaje de enlace ascendente usando información contenida en el mensaje de respuesta de acceso aleatorio recibido (a continuación en el presente documento denominado etapa de transmisión de 'mensaje 3' si no se confunde); y (4) recibir un mensaje de enlace descendente que corresponde al mensaje de enlace ascendente desde la estación base (a continuación en el presente documento denominado etapa de recepción de 'mensaje 4' si no se confunde). En este proceso, el equipo de usuario facilita la identificación de la transmisión de enlace ascendente frente a otra transmisión de enlace ascendente de un equipo de usuario diferente mediante encriptación usando información de identificación prescrita atribuida a la transmisión de mensaje de mensaje 3.

La encriptación general del sistema de LTE se explica esquemáticamente en asociación con la descripción anterior de la siguiente manera.

En primer lugar, en un sistema de comunicación móvil, un lado de transmisión realiza una operación de encriptación con el fin de identificar un usuario y una estación base y aleatorizar los datos que van a transmitirse. Esta encriptación se realiza de manera que se realiza una operación en una secuencia generada por un método pseudoaleatorio usando la adición módulo 2 de datos de transmisión. Mediante esta encriptación, los datos de transmisión tienen más características aleatorias de modo que una señal de transmisión puede tener una característica de potencia de transmisión equilibrada. Asimismo, una secuencia pseudoaleatoria se genera de manera diferente según un usuario o una estación base de modo que el usuario o la estación base puedan identificarse.

Asimismo, puede generarse la secuencia pseudoaleatoria usando un identificador (RNTI) relacionado con la transmisión de datos correspondiente. Por ejemplo, si un equipo de usuario recibe una asignación de recurso de enlace ascendente (concesión de UL) a través del PDCCH (canal de control de enlace descendente físico) en el que está marcado un identificador de célula (C-RNTI) propio, el equipo de usuario transmite datos en enlace ascendente a través del recurso asignado por la concesión de UL. En este caso, se genera una secuencia pseudoaleatoria a partir de los datos usando el C-RNTI del equipo de usuario y la encriptación se realiza entonces actuando sobre la secuencia y los datos conjuntamente.

Sin embargo, en relación con el procedimiento de acceso aleatorio anteriormente descrito, es necesario comentar adicionalmente en detalle qué clase de información de identificación se usa para realizar la encriptación en cada proceso y cómo establecer los correspondientes procedimientos de acceso aleatorio y módulos de procesamiento.

Un documento 'E-UTRAN Random Access procedure C-RNTI assignment and HARQ on message 4 with RACH model' (3GPP draft, Ericsson, 22.1.2007) describe un método para realizar acceso aleatorio en el que se asigna un identificador temporal de red de radio celular temporal (C-RNTI). Un documento Ericsson 3GPP, R1-080898, 15.2.2008, describe canales físicos para UTRA evolucionado.

Objeto de la invención

Por consiguiente, la presente invención se refiere a un método de acceso aleatorio para mejorar la eficacia de encriptación que sustancialmente elimina uno o más problemas debidos a las limitaciones y desventajas de la técnica relacionada.

Un objeto de la presente invención es proporcionar un aparato para mejorar el rendimiento de encriptación/desencriptación y método del mismo, en el que la encriptación/desencriptación se realiza en un procedimiento de acceso aleatorio dentro de un sistema de comunicación móvil.

Ventajas, objetos y características adicionales de la invención se expondrán en parte en la descripción que sigue y en parte serán evidentes para los expertos en la técnica tras el examen de lo siguiente, o pueden aprenderse a partir de la práctica de la invención. Los objetivos y otras ventajas de la invención pueden realizarse y conseguirse mediante la estructura señalada particularmente en la descripción escrita y las reivindicaciones de la misma así como en los dibujos adjuntos.

Para lograr estos objetos y otras ventajas y según el propósito de la invención, tal como se realiza y se describe en términos generales en el presente documento, se propone un método según la reivindicación 1.

Preferiblemente, el acceso aleatorio a la red específica corresponde a un acceso aleatorio basado en contienda y el método incluye además establecer el valor de información de identificación de terminal recibido a través del mensaje de respuesta de acceso aleatorio antes de que se transmita la señal de transmisión de enlace ascendente encriptada.

Más preferiblemente, la encriptación de la señal de transmisión de enlace ascendente incluye entregar la información de concesión de enlace ascendente recibida a una capa física del terminal desde una capa de MAC (control de acceso al medio) del terminal, generar una secuencia de encriptación usando el valor de información de identificación de terminal en la capa física del terminal, y encriptar la señal de transmisión de enlace ascendente usando la secuencia de encriptación generada.

Preferiblemente, el método incluye además retransmitir la señal de transmisión de enlace ascendente después de encriptar la señal de transmisión de enlace ascendente usando el valor de información de identificación de terminal recibido a través del mensaje de respuesta de acceso aleatorio.

Preferiblemente, la señal de transmisión de enlace ascendente encriptada se transmite a través de un canal de compartición de enlace ascendente físico (PUSCH). Preferiblemente, la información de identificación de terminal recibida a través del mensaje de respuesta de acceso aleatorio incluye un RNTI celular temporal (identificador temporal de red de radio celular temporal).

En otro aspecto de la presente invención, se propone un terminal, según la reivindicación 6.

Preferiblemente, el módulo de recepción recibe adicionalmente información de concesión de enlace ascendente específica a través del mensaje de respuesta de acceso aleatorio y el módulo de transmisión transmite la señal de transmisión de enlace ascendente encriptada por el módulo de encriptación basándose en la información de concesión de enlace ascendente específica.

Más preferiblemente, el terminal incluye además un módulo de capa de MAC, y el módulo de recepción entrega el mensaje de respuesta de acceso aleatorio recibido al módulo de capa de MAC.

En este caso, si el acceso aleatorio corresponde a un acceso aleatorio basado en contienda, el módulo de capa de MAC establece la información de identificación de terminal específica recibida a través del mensaje de respuesta de acceso aleatorio antes de que el módulo de transmisión transmita la señal de transmisión de enlace ascendente basándose en la información de concesión de enlace ascendente específica.

Además, el módulo de capa de MAC entrega la información de concesión de enlace ascendente específica en el mensaje de respuesta de acceso aleatorio al módulo de transmisión, el módulo de encriptación genera una secuencia de encriptación usando el valor de información de identificación de terminal especifico establecido por el módulo de capa de MAC, y el módulo de encriptación encripta la señal de transmisión de enlace ascendente usando la secuencia de encriptación generada.

Preferiblemente, el módulo de transmisión transmite la señal de transmisión de enlace ascendente a través de un canal de compartición de enlace ascendente físico (PUSCH).

Preferiblemente, la información de identificación de terminal específica recibida a través del mensaje de respuesta de acceso aleatorio incluye un RNTI celular temporal (identificador temporal de red de radio celular temporal).

En un aspecto adicional de la presente invención, un método para controlar un acceso aleatorio del terminal incluye las etapas de recibir un mensaje de preámbulo de acceso aleatorio desde el terminal, transmitir información de identificación de terminal e información de concesión de enlace ascendente (UL) a través de un mensaje de respuesta de acceso aleatorio que corresponde al mensaje de preámbulo de acceso aleatorio, recibir un mensaje de transmisión de enlace ascendente desde el terminal para que corresponde con la información de concesión de enlace ascendente, y desencriptar el mensaje de transmisión de enlace ascendente usando la información de identificación de terminal transmitida a través del mensaje de respuesta de acceso aleatorio.

Preferiblemente, la información de identificación de terminal transmitida a través del mensaje de respuesta de acceso aleatorio incluye un RNTI celular temporal (identificador temporal de red de radio celular temporal).

Por consiguiente, la presente invención proporciona los siguientes efectos y/o ventajas.

En primer lugar, una estación base puede realizar normalmente una operación de desencriptación en un tercer mensaje encriptado con un identificador de un equipo de usuario. En particular, la estación base puede realizar la desencriptación del tercer mensaje usando un C-RNTI temporal transmitido a través de una transmisión de un segundo mensaje.

En segundo lugar, un equipo de usuario que no tenga un identificador de célula asignado al mismo puede realizar la encriptación con su identificador. Por tanto, aumenta el rendimiento de aleatorización y se minimiza la interferencia.

En tercer lugar, en caso de que se use un C-RNTI temporal, un intervalo de una secuencia pseudoaleatoria, que puede generarse por un equipo de usuario en un punto de sincronismo de transmisión de un tercer mensaje, se amplía considerablemente. Por tanto, aumenta el rendimiento de aleatorización y se minimiza la interferencia con una célula adyacente así como la interferencia dentro de una célula del equipo de usuario.

Debe entenderse que tanto la descripción general anterior como la siguiente descripción detallada de la presente invención son a modo de ejemplo y explicativas y pretenden proporcionar una mejor explicación de la invención según se reivindica.

Descripción de las figuras

Los dibujos adjuntos, que están incluidos para proporcionar un mejor entendimiento de la invención y están incorporados en y constituyen una parte de esta solicitud, ilustran una realización(es) de la invención y junto con la descripción sirven para explicar el principio de la invención. En los dibujos:

la figura 1 es un diagrama esquemático de una estructura de red de E-UMTS como un ejemplo de un sistema de comunicación móvil;

la figura 2 y la figura 3 son diagramas de estructuras de un protocolo de interfaz de radio entre un equipo de usuario y UTRAN basándose en las especificaciones de red de acceso de radio de 3GPP;

la figura 4 es un diagrama de un proceso operativo entre un equipo de usuario y una estación base en un procedimiento de acceso aleatorio no basado en contienda;

la figura 5 es un diagrama de un proceso operativo entre un equipo de usuario y una estación base en un procedimiento de acceso aleatorio basado en contienda;

la figura 6 es un diagrama de un método para realizar un acceso aleatorio basado en contienda entre un equipo de usuario y una estación base según una realización de la presente invención;

la figura 7 es un diagrama de un formato de un mensaje de respuesta de acceso aleatorio recibido a través de un segundo mensaje;

la figura 8 es un diagrama de bloques esquemático de un equipo de usuario para realizar un acceso aleatorio según una realización de la presente invención; y

la figura 9 es un diagrama para explicar un proceso de que un equipo de usuario realiza un acceso aleatorio a una estación base específica según una realización de la presente invención.

Descripción detallada de la invención

Ahora se hará referencia en detalle a las realizaciones preferidas de la presente invención, ejemplos de las cuales se ilustran en los dibujos adjuntos. Cuando sea posible, se usarán los mismos números de referencia en todos los dibujos para hacer referencia a partes iguales o similares. En la siguiente descripción detallada de la invención se incluyen detalles para ayudar el entendimiento completo de la presente invención. Sin embargo, es evidente para los expertos en la técnica que la presente invención puede implementarse sin estos detalles. Por ejemplo, aunque la siguiente descripción detallada se hace en detalle suponiendo que un sistema de comunicación móvil es el sistema de LTE de 3GPP, puede aplicarse para otros sistemas de comunicación móvil prescritos excluyendo los elementos únicos del LTE de 3GPP.

Ocasionalmente, se omiten las estructuras y dispositivos conocidos para el público para evitar una imprecisión conceptual de la presente invención o pueden ilustrarse como diagramas de bloques centrándose en sus funciones principales.

En la siguiente descripción, se supone que un terminal es un término genérico de un dispositivo de extremo de usuario fijo o móvil tal como un equipo de usuario (UE), una estación móvil (MS) y similares. Y, se supone que una estación base es una denominación genérica de cualquier nodo de un extremo de red, que se comunica con un terminal, tal como un Nodo B, un eNodo B y similares.

En relación con qué clase de identificación se usa para realizar la encriptación en cada proceso en asociación con un procedimiento de acceso aleatorio y cómo establecer procedimientos correspondientes y módulos de procesamiento, el procedimiento de acceso aleatorio, al que se aplicará la presente invención, se explica en detalle de la siguiente manera.

La figura 4 muestra un proceso operativo entre un terminal y una estación base en un procedimiento de acceso aleatorio no basado en contienda.

·1.- Asignación de preámbulo de acceso aleatorio

Tal como se mencionó en la descripción anterior, un procedimiento de acceso aleatorio no basado en contienda puede realizarse en caso de: (i) un proceso de traspaso; y (ii) una petición por una orden dada por una estación base. Naturalmente, en ambos casos anteriores, puede realizarse un procedimiento de acceso aleatorio basado en contienda.

En primer lugar, para un procedimiento de acceso aleatorio no basado en contienda, es importante recibir un preámbulo de acceso aleatorio especificado, que está libre de colisión, desde una estación base. Como un método de especificar el preámbulo de acceso aleatorio, hay un método a través de una orden de traspaso o un método a través de una orden de PDCCH. A través de esto, se asigna un preámbulo de acceso aleatorio a un terminal (5401).

·2.- Transmisión de primer mensaje (mensaje-1)

Tal como se mencionó en la descripción anterior, después de que el preámbulo de acceso aleatorio especificado al terminal se haya asignado sólo al terminal, el terminal transmite entonces el preámbulo a una estación base (S402).

·3.- Recepción de segundo mensaje (mensaje-2)

Después de que el terminal ha transmitido el preámbulo de acceso aleatorio en la etapa (S402), intenta una recepción de su respuesta de acceso aleatorio dentro de una ventana de recepción de respuesta de acceso aleatorio indicada a través de la información de sistema u orden de traspaso de la estación base (S403). En particular, la información de respuesta de acceso aleatorio puede transmitirse en un formato de PDU de MAC (unidad de datos de paquetes de MAC). En este caso, la PDU de MAC puede entregarse a través de PDSCH (canal compartido de enlace descendente físico).

Preferiblemente, con el fin de recibir apropiadamente la información llevada en el PDSCH, el terminal monitoriza el PDCCH (canal de control de enlace descendente físico). En particular, se prefiere que la información del terminal para recibir el PDSCH, una frecuencia de un recurso de radio del PDSCH, información de tiempo, un formato de transmisión del PDSCH y similar estén contenidos en el PDCCH.

Una vez que el terminal logra satisfactoriamente la recepción del PDCCH transmitido para sí mismo, puede recibir apropiadamente una respuesta de acceso aleatorio llevada en el PDSCH según informaciones del PDCCH. Y, la respuesta de acceso aleatorio puede incluir un identificador de preámbulo de acceso aleatorio (ID), una concesión de enlace ascendente (concesión de UL) que indica un recurso de radio de enlace ascendente, un identificador de célula temporal (C-RNTI temporal) y un valor de corrección de sincronización de tiempo (orden de avance de sincronismo: TAC).

Tal como se mencionó en la descripción anterior, es necesario un identificador de preámbulo de acceso aleatorio para una respuesta de acceso aleatorio. Puesto que puede incluirse información de respuesta de acceso aleatorio para al menos un terminal en una respuesta de acceso aleatorio, es necesario indicar la concesión de enlace ascendente (concesión de UL), el C-RNTI temporal y TAC son válidos para un terminal prescrito. En esta etapa, se supone que el terminal selecciona un identificador de preámbulo de acceso aleatorio que coincide con el preámbulo de acceso aleatorio anterior seleccionado por el terminal en la etapa (S402).

En el procedimiento de acceso aleatorio no basado en contienda, se determina que el acceso aleatorio se ha realizado satisfactoriamente si se recibe la información de respuesta de acceso aleatorio. Entonces puede finalizar el procedimiento de acceso aleatorio.

La figura 5 es un diagrama para un proceso operativo entre un terminal y una estación base en un procedimiento de acceso aleatorio basado en contienda.

·1.- Transmisión de primer mensaje

En primer lugar, un terminal selecciona de manera aleatoria un preámbulo de acceso aleatorio a partir de un conjunto de preámbulos de acceso aleatorio indicados por la información de sistema o una orden de traspaso. El terminal selecciona un recurso de PRACH (RACH físico) que puede llevar el preámbulo de acceso aleatorio y entonces puede transmitir el preámbulo de acceso aleatorio correspondiente (S501).

·2.- Recepción de segundo mensaje

Un método para recibir una respuesta de acceso aleatorio es similar al procedimiento de acceso aleatorio no basado en contienda mencionado anteriormente. En particular, después de que el terminal ha transmitido el preámbulo de acceso aleatorio, tal como se muestra en la etapa (S501), el terminal intenta una recepción de su respuesta de acceso aleatorio en el PDCCH dentro de una ventana de recepción de respuesta de acceso aleatorio indicada por la información de sistema o la orden de traspaso de una estación base. El terminal recibe entonces el PDSCH a través de una información de RA-RNTI correspondiente (S502). A través del PDSCH recibido, el terminal puede recibir una concesión de enlace ascendente (concesión de UL), un identificador de célula temporal (C-RNTI temporal), un valor de corrección de sincronización de tiempo (orden de avance de sincronismo: TAC) y similares.

·3.- Transmisión de tercer mensaje

Si el terminal recibe una respuesta de acceso aleatorio válida para sí mismo, el terminal procesa informaciones contenidas en la respuesta de acceso aleatorio. En particular, el terminal aplica la TAC y almacena el C-RNTI temporal. El terminal también transmite datos (es decir, un tercer mensaje) a la estación base usando la concesión de UL (S503). En este caso, se prefiere que el tercer mensaje contenga un identificador del terminal puesto que una estación base no puede determinar qué terminal realiza el procedimiento de acceso aleatorio en el procedimiento de acceso aleatorio basado en contienda cuando el tercer mensaje no contiene el identificador del terminal. Por tanto, se prefiere identificar un terminal para una futura resolución de contienda.

Se han comentado dos clases de métodos como un método para tener un identificador de terminal incluido. En un primer método, si un terminal tiene un identificador de célula válido asignado en una célula correspondiente antes del procedimiento de acceso aleatorio, el terminal transmite su identificador de célula a través de una señal de transmisión de enlace ascendente que corresponde a la concesión de UL. Si el identificador de célula válido no se asigna antes del procedimiento de acceso aleatorio, el terminal transmite su identificador único (por ejemplo, S-TMSI, un ID aleatorio, etc.). El identificador único es generalmente más largo que el identificador de célula. Si el terminal transmite datos que corresponden a la concesión de UL, el terminal inicia un temporizador para solución de colisión (temporizador de resolución de contienda).

·4.- Recepción de cuarto mensaje

Después de que el terminal ha transmitido los datos que contienen su identificador usando la concesión de UL contenida en la respuesta de acceso aleatorio, el terminal espera una indicación de la estación base para la resolución de contienda. En particular, el terminal intenta una recepción de PDCCH para recibir un mensaje específico (S504).

Se han comentado dos clases de métodos como un método para recibir el PDCCH. Tal como se mencionó en la descripción anterior, si el tercer mensaje transmitido basándose en la concesión de UL se transmite usando el identificador de célula, el terminal intenta la recepción del PDCCH usando su identificador de célula. Si el identificador es un identificador único, el terminal puede intentar la recepción del PDCCH usando el C-RNTI temporal contenido en la respuesta de acceso aleatorio.

A continuación, en el caso anterior, si el terminal recibió el PDCCH a través de su identificador de célula antes de que el temporizador de resolución de contienda expire, el terminal determina que el procedimiento de acceso

aleatorio se realiza satisfactoriamente. El terminal finaliza entonces el procedimiento de acceso aleatorio. En el último caso, si el terminal recibió el PDCCH a través del C-RNTI temporal antes de que el temporizador de resolución de contienda expire, el terminal comprueba los datos llevados en el PDSCH indicado por el PDCCH. Si el identificador único del terminal se incluye en el contenido de los datos, el terminal determina que el procedimiento de acceso aleatorio se realiza satisfactoriamente. El terminal finaliza entonces el procedimiento de acceso aleatorio.

Mientras tanto, tal como se mencionó en la descripción anterior, en el procedimiento de acceso aleatorio, y más particularmente, en el procedimiento de acceso aleatorio basado en contienda, si el identificador del terminal se incluye en el tercer mensaje y la encriptación para la transmisión de tercer mensaje se establece para usar el identificador de terminal, puede provocarse el siguiente problema. Concretamente, la estación base sólo puede confirmar el identificador del terminal si la estación base normalmente recibe el tercer mensaje y consigue decodificar el tercer mensaje. Sin embargo, puesto que el punto de sincronismo para que la estación base realice una operación de desencriptación después de recibir el tercer mensaje es un punto de sincronismo para comprobar el identificador del terminal, la estación base no puede conocer el identificador del terminal al realizar la operación de desencriptación. En particular, la estación base debe obtener el identificador de terminal a través de la desencriptación del tercer mensaje. Si se requiere el identificador de terminal para la desencriptación del tercer mensaje, es difícil para la estación base obtener el identificador de terminal.

En el punto de sincronismo de transmisión de tercer mensaje, el terminal puede o no tener el identificador de célula, que se asignó por la estación base, del terminal. En caso de que el terminal no logre tener el identificador de célula asignado por la estación base, el terminal no puede encriptar el tercer mensaje con el identificador del terminal. Por tanto, puede surgir una interferencia entre una célula correspondiente y una célula adyacente.

En un procedimiento de acceso aleatorio según una realización preferida de la presente invención, en caso de que un terminal transmite datos usando una concesión de UL incluida en una respuesta de acceso aleatorio, se establece un identificador usado para la encriptación de datos para usar información de identificación compartida entre el terminal y una estación base. Preferiblemente, una secuencia de encriptación se genera usando un C-RNTI temporal llevado por un segundo mensaje. Entonces se transmite un tercer mensaje usando la secuencia de encriptación generada basándose en el C-RNTI temporal. Por tanto, puede resolverse el problema mencionado anteriormente. Este esquema puede aplicarse para realizar la encriptación al transmitir una señal de transmisión de enlace ascendente que sigue a la recepción del segundo mensaje en un procedimiento de acceso aleatorio no basado en contienda. Sin embargo, en la siguiente descripción, se explica un ejemplo que se centra en un procedimiento de acceso aleatorio basado en contienda para transmitir un tercer mensaje en correspondencia con una concesión de UL llevada por un segundo mensaje.

La figura 6 es un diagrama para un método para realizar un acceso aleatorio basado en contienda entre un terminal y una estación base según una realización de la presente invención.

·1.- Transmisión de primer mensaje

Cuando se solicita un procedimiento de acceso aleatorio, un terminal selecciona de manera aleatoria un preámbulo de acceso aleatorio por una capa de MAC y entonces puede transmitir el preámbulo de acceso aleatorio seleccionado a una estación base (S601).

·2.- Recepción de segundo mensaje

El terminal recibe una respuesta de acceso aleatorio que incluye un identificador de preámbulo de acceso aleatorio que corresponde al preámbulo de acceso aleatorio transmitido por sí mismo (S602). La respuesta de acceso aleatorio puede incluir un identificador de preámbulo de acceso aleatorio (RA-RNTI), una concesión de UL, un C-RNTI temporal y TAC. Se muestra una estructura detallada de la respuesta de acceso aleatorio en la figura 7.

La figura 7 es un diagrama para un formato de un mensaje de respuesta de acceso aleatorio recibido a través de un segundo mensaje.

En referencia a la figura 7, 'R' indica un bit reservado y se supone que se establece a 0. Una concesión de enlace ascendente indica un recurso de enlace ascendente que se usará para la transmisión de enlace ascendente. Se usa un campo de TAC para controlar un tamaño de adaptación de sincronismo que debe aplicar un terminal. Y, un C-RNTI temporal indica un identificador temporal que usa un terminal para un procedimiento de acceso aleatorio. En este caso, el C-RNTI temporal tiene una longitud de 16 bits.

Mientras tanto, una capa de MAC de un terminal almacena un C-RNTI temporal recibido a través de una respuesta de acceso aleatorio. Y, la capa de MAC del terminal controla la capa física para generar una secuencia pseudoaleatoria usando el C-RNTI temporal establecido y encripta datos usando la secuencia pseudoaleatoria generada al transmitir el mensaje.

Preferiblemente, el terminal recibe una respuesta de acceso aleatorio mostrada en la figura 7, establece un C-RNTI temporal contenido en la respuesta no más tarde de la transmisión de un tercer mensaje, y entonces informa directamente a una capa física del ajuste. En la presente realización, puesto que se supone que se usa un C-RNTI temporal recibido a través del segundo mensaje en la transmisión del tercer mensaje, si un punto de sincronismo para permitir a una capa de MAC establecer un C-RNTI temporal está detrás de un punto de sincronismo de transmisión de tercer mensaje, es difícil para la capa física aplicar la encriptación a la transmisión del tercer mensaje.

·3.- Transmisión de tercer mensaje

El terminal transmite un tercer mensaje a la estación base usando la concesión de UL contenida en la respuesta de acceso aleatorio (S603). Preferiblemente, un C-RNTI (o, un elemento de control de MAC de C-RNTU) del terminal o una SDU de CCCH de enlace ascendente está contenido en el tercer mensaje. Y, se supone que el tercer mensaje se transmite a través de PUSCH. Además, la presente realización propone realizar una encriptación usando una secuencia pseudoaleatoria que se genera usando información de identificación de terminal que se garantiza que se comparte entre la estación base y el terminal en un punto de sincronismo de transmisión de tercer mensaje, y preferiblemente, usando un C-RNTI temporal recibido a través de la respuesta de acceso aleatorio que tiene la estructura mostrada en la figura 7.

La información de identificación, que se garantiza que se comparte entre la estación base y el terminal en el punto de sincronismo de transmisión de tercer mensaje, puede considerar usar RA-RNTI o C-RNTI=0 así como el C-RNTI temporal. Sin embargo, el RA-RNTI es un identificador asignado para identificar qué clase de recurso de tiempo-frecuencia se usa para que el terminal transmita un preámbulo de acceso aleatorio. Puesto que el número de identificadores disponibles es más pequeño que el de RNTI temporales, es difícil identificar un número suficiente de terminales en caso del RA-RNTI.

Además, 'realizar la encriptación usando el C-RNTI=0' tiene el mismo significado que 'no aplicar la encriptación', lo que provoca un problema de que no se obtiene una ganancia de aleatorización a partir de la encriptación.

Por tanto, según la presente realización, la encriptación se realiza usando el C-RNTI temporal recibido a través del segundo mensaje y sus detalles se explican de la siguiente manera.

En primer lugar, una capa física de un terminal genera una secuencia pseudoaleatoria como una secuencia de encriptación de una manera de ajustar un C-RNTI temporal establecido por una capa de MAC a un valor inicial de la secuencia pseudoaleatoria. En caso del sistema de LTE, se define una secuencia pseudoaleatoria usando la siguiente secuencia de oro que tiene una longitud de 31.

(Fórmula 1)

$$c(n)=(x_1(n+N_c)+x_2(n+N_c))\bmod 2$$
$$x_1(n+31)=(x_1(n+3)+x_1(n))\bmod 2$$
$$x_2(n+31)=(x_2(n+3)+x_2(n+2)+x_2(n+1)+x_2(n))\bmod 2$$

En la formula 1, se proporciona una secuencia pseudoaleatoria emitida c(n) por una primera secuencia m $x_1(n)$ y una segunda secuencia m $x_2(n)$ [donde n = 0, 1, 2, ..., M_{PN}-1]. Y, es N_c=1600. M_{PN} indica una longitud de secuencia. La primera secuencia m se inicia en $x_1(0)$ =1 y $x_1(n)$=0, donde n = 1, 2, ..., 30. Y, se inicia la segunda secuencia 2m mediante. En este caso, se determina un valor de C_{inic} según un uso de una secuencia para su uso. Y, la presente realización propone usar el siguiente valor inicial con el fin de realizar una transmisión de tercer mensaje a través de PSUCH.

(Fórmula 2)

$$c_{inic} = n_{RNTI} \cdot 2^{14} + \lfloor n_s / 2 \rfloor \cdot 2^9 + N_{ID}^{cel}$$

En la formula 2, n_s indica un número de ranura dentro de una célula de un marco de radio, indica un identificador de célula de capa física, y n_{PNIT} indica un valor de RNTI para una transmisión de PUSCH correspondiente. Además, $[n_s/2]$ significa un número entero máximo que no supera $n_s/2$. Por eso, en caso de aplicar la presente realización al sistema de LTE, la presente realización propone las siguientes etapas. En primer lugar, se genera un valor inicial C_{inic} para una transmisión de PUSCH estableciendo un valor de C-RNTI temporal a n_{RNTI}, se genera una secuencia pseudoaleatoria usando el valor inicial generado para la inicialización de la segunda secuencia m, y entonces se usa esta secuencia para la encriptación realizada para una transmisión de tercer mensaje.

En la siguiente descripción, se explica una estructura de un terminal que realiza la realización descrita anteriormente.

La figura 8 es un diagrama de bloques esquemático de un terminal para realizar un acceso aleatorio según una realización de la presente invención.

En referencia a la figura 8, un terminal según la presente realización incluye un módulo (801) de capa física y un módulo (802) de capa de MAC. Y, el módulo (801) de capa física puede incluir un módulo (803) de transmisión, un módulo (804) de recepción, un módulo (805) de encriptación y similares.

Basándose en la estructura anterior, operaciones según la presente realización se explican de la siguiente manera.

En primer lugar, en caso de un procedimiento de acceso aleatorio basado en contienda, un preámbulo de acceso aleatorio seleccionado por el módulo (802) de capa de MAC se entrega al módulo (803) de transmisión. El módulo (803) de transmisión puede entonces transmitir el preámbulo de acceso aleatorio a una estación base teniendo el preámbulo de acceso aleatorio contenido en el primer mensaje.

Posteriormente, el terminal monitoriza si una señal que indica un RA-RNTI que corresponde a un preámbulo de acceso aleatorio transmitido previamente se transmite a través de PDCCH dentro de una ventana que tiene un tamaño prescrito. Si la señal que indica el RA-RNTI que corresponde al preámbulo de acceso aleatorio transmitido previamente se transmite a través de PDCCH dentro de la ventana correspondiente, una capa física del terminal, y más particularmente, el módulo (804) de recepción, puede entregar un bloque de transporte (TB), que incluye una respuesta de acceso aleatorio (RAR), a una capa de MAC.

En este caso, la información de TAC, la información de concesión de UL y la información de C-RNTI temporal, tal como se muestra en la figura 7, están contenidas en el mensaje de respuesta de acceso aleatorio de MAC entregado (RAR de MAC).

Habiendo obtenido la capa (802) de MAC del terminal las informaciones anteriores, entrega la información de concesión de UL en el mensaje de RAR recibido a la capa (801) física.

La capa (802) de MAC de la presente realización configura un valor de C-RNTI temporal obtenido a través de la RAR recibida antes de una transmisión del tercer mensaje a través del módulo (803) de transmisión de la capa (801) física y entonces entrega el valor de configuración al módulo (805) de encriptación de la capa (801) física.

Habiendo recibido el módulo (805) de encriptación el valor de C-RNTI temporal desde la capa (802) de MAC, genera una secuencia de encriptación usando el valor de C-RNTI temporal como un valor inicial de la secuencia pseudoaleatoria y luego encripta una señal de transmisión de enlace ascendente que corresponde a una concesión de UL usando la secuencia de encriptación generada. En caso del sistema de LTE, el módulo (805) de encriptación realiza un proceso de añadir la señal de transmisión de enlace ascendente que corresponde a la concesión de UL y la secuencia de encriptación generada conjuntamente usando un sumador de módulo 2 (no mostrado en el dibujo).

La señal de transmisión encriptada por el módulo (805) de encriptación se entrega al módulo (803) de transmisión. El módulo (803) de transmisión puede transmitir entonces la señal de transmisión de enlace ascendente encriptada a través de la zona de recurso de tiempo-frecuencia.

Mientras tanto, ‘realizar la encriptación usando la información de identificación recibida a través del segundo mensaje’ en la descripción anterior puede aplicarse a una retransmisión de un tercer mensaje así como una transmisión inicial del tercer mensaje.

La figura 9 es a diagrama para explicar un proceso en el que un terminal realiza un acceso aleatorio para una estación base específica según una realización de la presente invención.

En referencia a la figura 9, una transmisión de primer mensaje (S901), una recepción de segundo mensaje (S902) y una transmisión de tercer mensaje (S903) son idénticas a la transmisión de primer mensaje anterior (S601), la recepción de segundo mensaje anterior (S602) y la transmisión de tercer mensaje anterior (S603) de la figura 6, respectivamente.

Tal como se mencionó en la descripción anterior, después de transmitir el tercer mensaje encriptado usando el C-RNTI temporal recibido a través del segundo mensaje, el terminal puede no recibir información de retroalimentación que indica la recepción satisfactoria de tercer mensaje desde la estación base. En particular, el terminal puede recibir NACK desde la estación base (S904). De ser así, el terminal puede realizar una transmisión del tercer mensaje.

Según la presente realización, en la retransmisión del tercer mensaje, el terminal realiza la encriptación usando la secuencia pseudoaleatoria generada usando el C-RNTI temporal contenido en la información de respuesta de acceso aleatorio.

Tal como se mencionó en las descripciones anteriores de las realizaciones de la presente invención, la encriptación del tercer mensaje se realiza en un procedimiento de acceso aleatorio usando un identificador contenido en un mensaje de respuesta de acceso aleatorio, por ejemplo, una secuencia pseudoaleatoria generada usando C-RNTI. Por tanto, la estación base puede desencriptar normalmente el tercer mensaje que se ha encriptado con el identificador del terminal. En particular, la estación base puede desencriptar el tercer mensaje usando el C-RNTI temporal transmitido en la transmisión de segundo mensaje.

Mientras tanto, según la presente realización, un terminal que no logra tener un identificador de célula asignado al mismo puede realizar una encriptación con su identificador de célula. Por tanto, se aumenta el rendimiento de aleatorización y se minimiza la interferencia.

Además, en caso de usar un C-RNTI temporal, puesto que se extiende considerablemente un intervalo de una secuencia pseudoaleatoria, que puede generarse mediante un terminal en un punto de sincronismo de transmisión de un tercer mensaje, se aumenta el rendimiento de aleatorización. Y, la interferencia con una célula adyacente puede minimizarse así como la interferencia dentro de una célula del terminal.

Por consiguiente, la tecnología de acceso aleatorio y la estructura de terminal para el mismo se describen con referencia al ejemplo aplicado al sistema de LTE de 3GPP y también pueden aplicarse a diversos sistemas de comunicación móvil que tienen los procedimientos de acceso aleatorio similares.

Será evidente para los expertos en la técnica que pueden realizarse diversas modificaciones y variaciones en la presente invención sin apartarse del alcance de las invenciones. Por tanto, se pretende que la presente invención cubra las modificaciones y variaciones de esta invención siempre que entren dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para realizar un acceso aleatorio a una red de comunicación inalámbrica mediante un terminal, caracterizado porque el método comprende:

transmitir un mensaje de preámbulo de acceso aleatorio que incluye un preámbulo prescrito como un primer mensaje del acceso aleatorio;

recibir un mensaje de respuesta de acceso aleatorio que corresponde al mensaje de preámbulo de acceso aleatorio como un segundo mensaje del acceso aleatorio, en el que el mensaje de respuesta de acceso aleatorio comprende información de concesión de enlace ascendente y un identificador temporal de red de radio celular temporal, a continuación en el presente documento denominado C-RNTI temporal;

encriptar una señal de transmisión de enlace ascendente usando el C-RNTI temporal recibido a través del mensaje de respuesta de acceso aleatorio; y

transmitir la señal de transmisión de enlace ascendente encriptada basándose en la información de concesión de enlace ascendente como un tercer mensaje del acceso aleatorio para un procedimiento de resolución de contienda.

2. Método según la reivindicación 1, caracterizado porque el acceso aleatorio a la red de comunicación inalámbrica es un acceso aleatorio basado en contienda, y

en el que el método comprende además:

establecer información de identificación de terminal del terminal para encriptar la señal de transmisión de enlace ascendente como el C-RNTI temporal recibido a través del mensaje de respuesta de acceso aleatorio antes de que se transmita la señal de transmisión de enlace ascendente encriptada.

3. Método según la reivindicación 2, caracterizado porque la encriptación de la señal de transmisión de enlace ascendente comprende:

entregar la información de concesión de enlace ascendente recibida a una capa física del terminal desde una capa de MAC (control de acceso al medio) del terminal;

generar una secuencia de encriptación usando la información de identificación de terminal en la capa física del terminal; y

encriptar la señal de transmisión de enlace ascendente usando la secuencia de encriptación generada.

4. Método según la reivindicación 1, caracterizado porque comprende además:

retransmitir la señal de transmisión de enlace ascendente después de encriptar la señal de transmisión de enlace ascendente usando el C-RNTI temporal recibido a través del mensaje de respuesta de acceso aleatorio.

5. Método según la reivindicación 1, caracterizado porque la señal de transmisión de enlace ascendente encriptada se transmite a través de un canal de compartición de enlace ascendente físico (PUSCH).

6. Terminal para realizar un acceso aleatorio a una red de comunicación inalámbrica, caracterizado porque comprende:

un módulo de transmisión adaptado para transmitir un mensaje de preámbulo de acceso aleatorio como un primer mensaje del acceso aleatorio y una señal de transmisión de enlace ascendente que corresponde a información de concesión de enlace ascendente;

un módulo de recepción adaptado para recibir un mensaje de respuesta de acceso aleatorio que corresponde al mensaje de preámbulo de acceso aleatorio como un segundo mensaje del acceso aleatorio; y

un módulo de encriptación adaptado para encriptar la señal de transmisión de enlace ascendente usando un valor de información de identificación de terminal,

en el que el módulo de transmisión, el módulo de recepción y el módulo de encriptación es un módulo de capa física, y

en el que el módulo de encriptación se adapta además para encriptar la señal de transmisión de enlace ascendente, que va a transmitirse como un tercer mensaje del acceso aleatorio para un procedimiento de resolución de contienda, usando un identificador temporal de red de radio celular temporal, a continuación en el presente documento denominado valor de C-RNTI temporal, recibido por el módulo de recepción a través del mensaje de respuesta de acceso aleatorio.

7. Terminal según la reivindicación 6, caracterizado porque el módulo de recepción está adaptado además para recibir información de concesión de enlace ascendente específica a través del mensaje de respuesta de acceso aleatorio, y

en el que el módulo de transmisión está adaptado para transmitir la señal de transmisión de enlace ascendente encriptada por el módulo de encriptación basándose en la información de concesión de enlace ascendente específica.

8. Terminal según la reivindicación 7, caracterizado porque comprende además un módulo de capa de MAC,

en el que el módulo de recepción está adaptado para entregar el mensaje de respuesta de acceso aleatorio recibido al módulo de capa de MAC.

9. Terminal según la reivindicación 8, caracterizado porque si el acceso aleatorio corresponde a un acceso aleatorio basado en contienda, el módulo de capa de MAC está adaptado para establecer un valor de información de identificación de terminal del terminal para encriptar la señal de transmisión de enlace ascendente como el valor de C-RNTI temporal recibido a través del mensaje de respuesta de acceso aleatorio antes de que el módulo de transmisión transmita la señal de transmisión de enlace ascendente basándose en la información de concesión de enlace ascendente específica.

10. Terminal según la reivindicación 9, caracterizado porque el módulo de capa de MAC está adaptado para entregar la información de concesión de enlace ascendente específica en el mensaje de respuesta de acceso aleatorio al módulo de transmisión, y

en el que el módulo de encriptación está adaptado para generar una secuencia de encriptación usando el valor de información de identificación de terminal establecido por el módulo de capa de MAC, y para encriptar la señal de transmisión de enlace ascendente usando la secuencia de encriptación generada.

11. Terminal según la reivindicación 6, caracterizado porque el módulo de transmisión está adaptado para transmitir la señal de transmisión de enlace ascendente a través de un canal de compartición de enlace ascendente físico (PUSCH).

FIG. 1

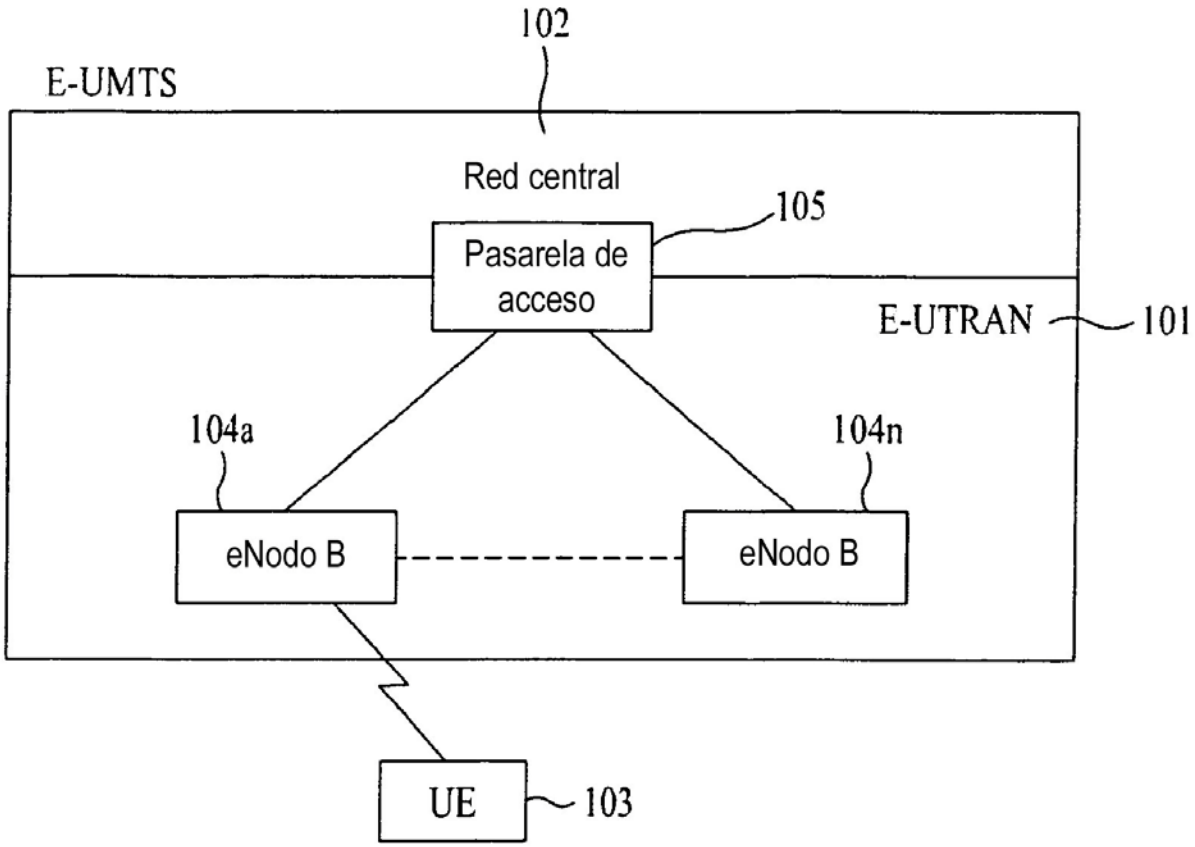

102
E-UMTS
Red central
105
Pasarela de acceso
E-UTRAN
101
104a
104n
eNodo B
eNodo B
UE
103

FIG. 2

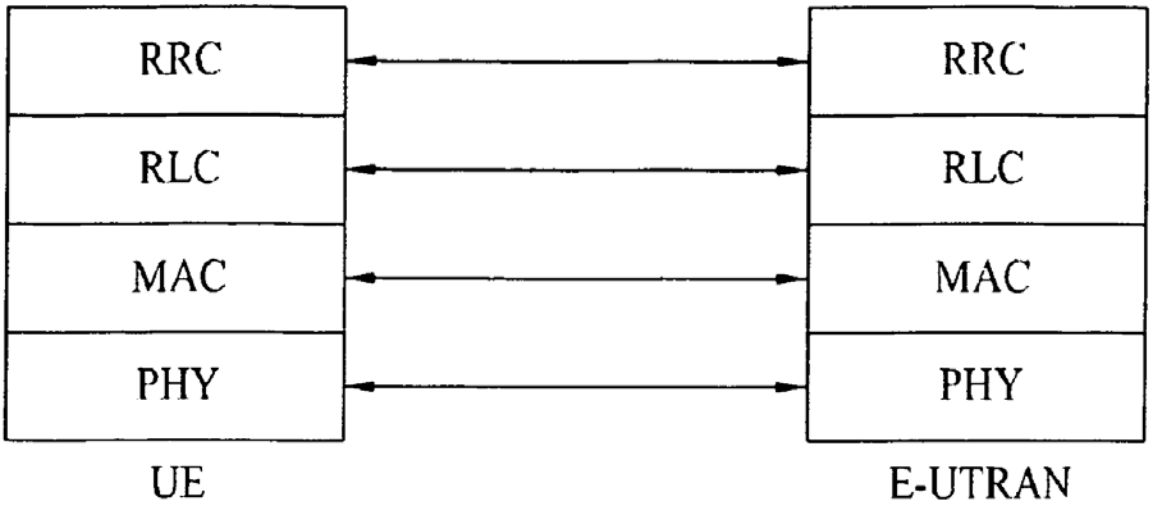

RRC
RLC
MAC
PHY
UE
RRC
RLC
MAC
PHY
E-UTRAN

FIG. 3

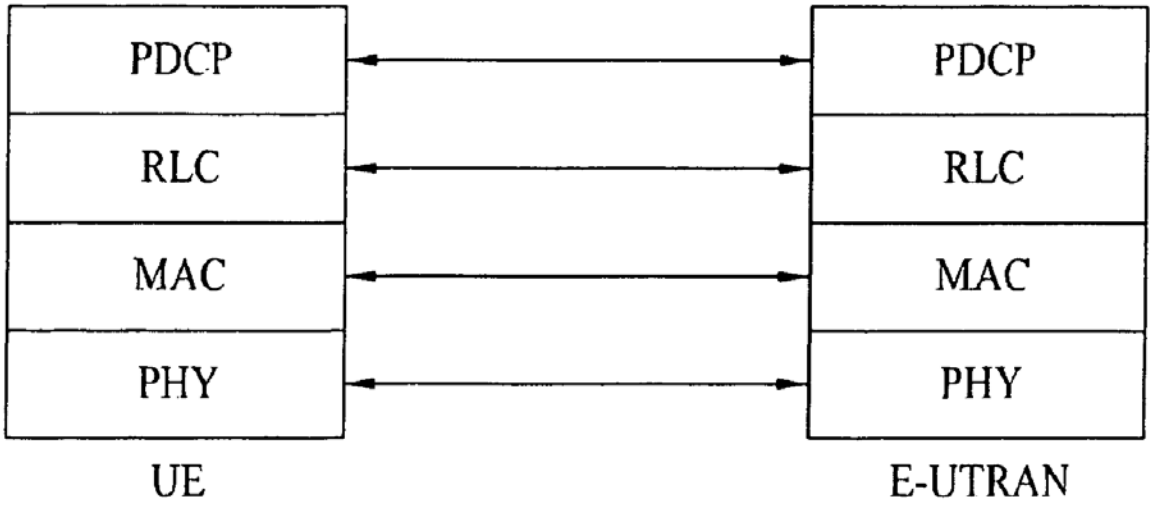

PDCP
RLC
MAC
PHY
UE
PDCP
RLC
MAC
PHY
E-UTRAN

FIG. 4

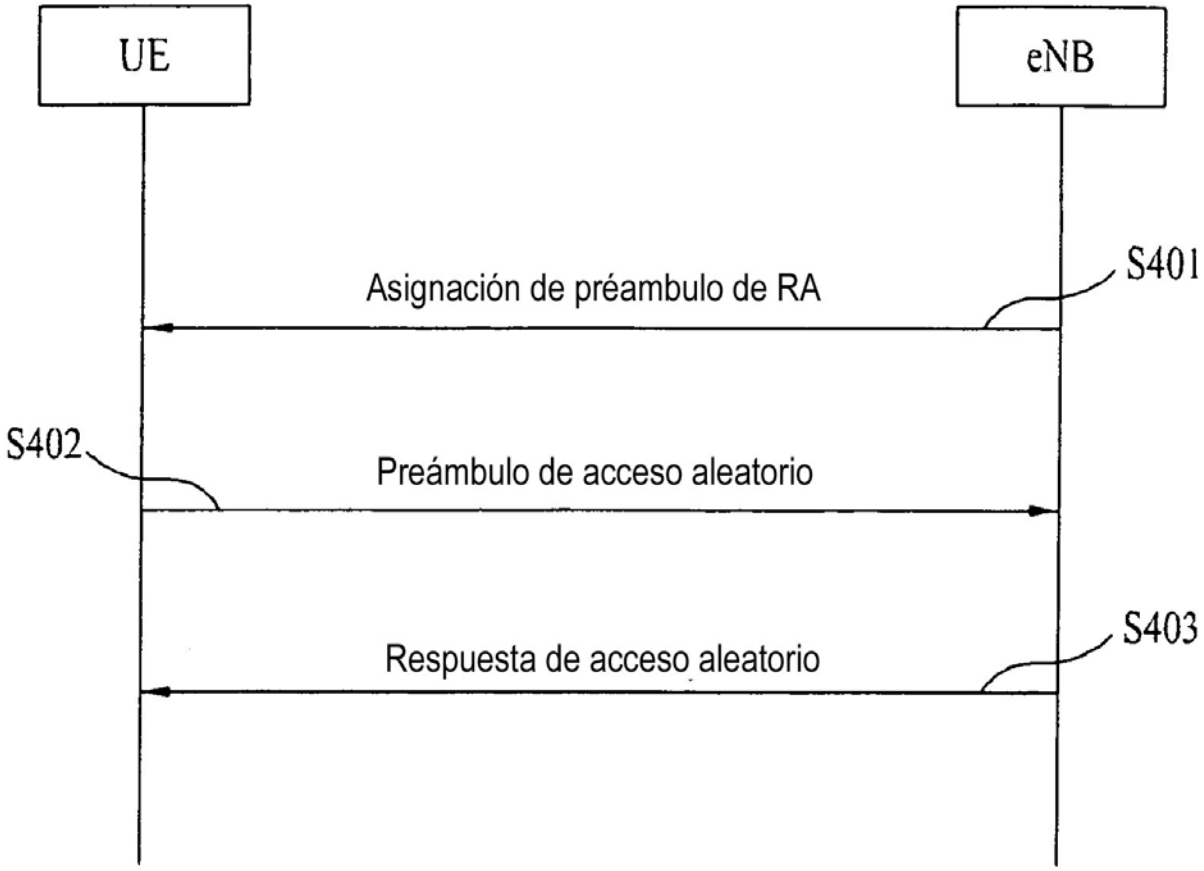

UE
eNB
S401
Asignación de préambulo de RA
S402
Preámbulo de acceso aleatorio
S403
Respuesta de acceso aleatorio

FIG. 5

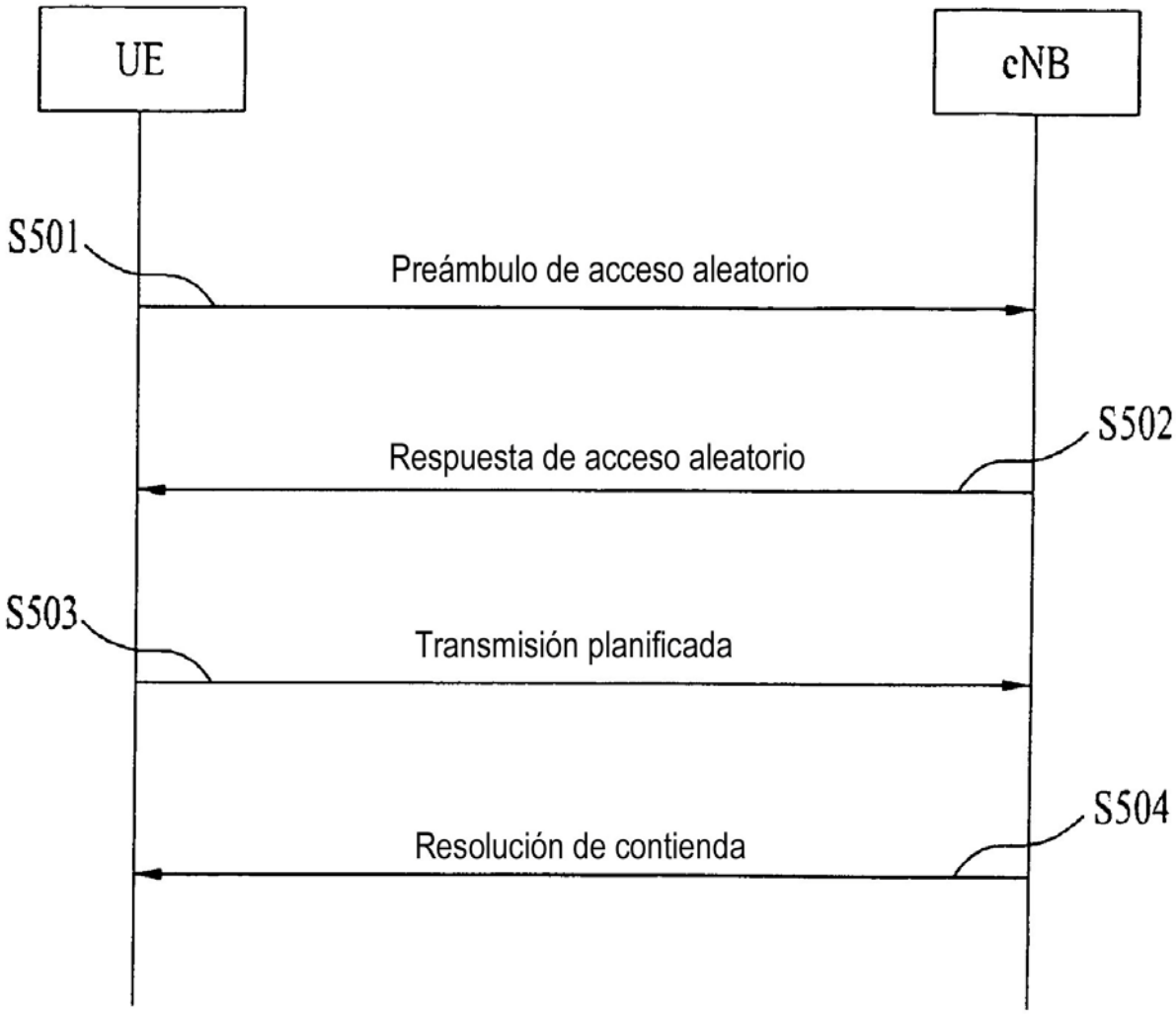

UE
eNB
S501
Preámbulo de acceso aleatorio
S502
Respuesta de acceso aleatorio
S503
Transmisión planificada
S504
Resolución de contienda

FIG. 6

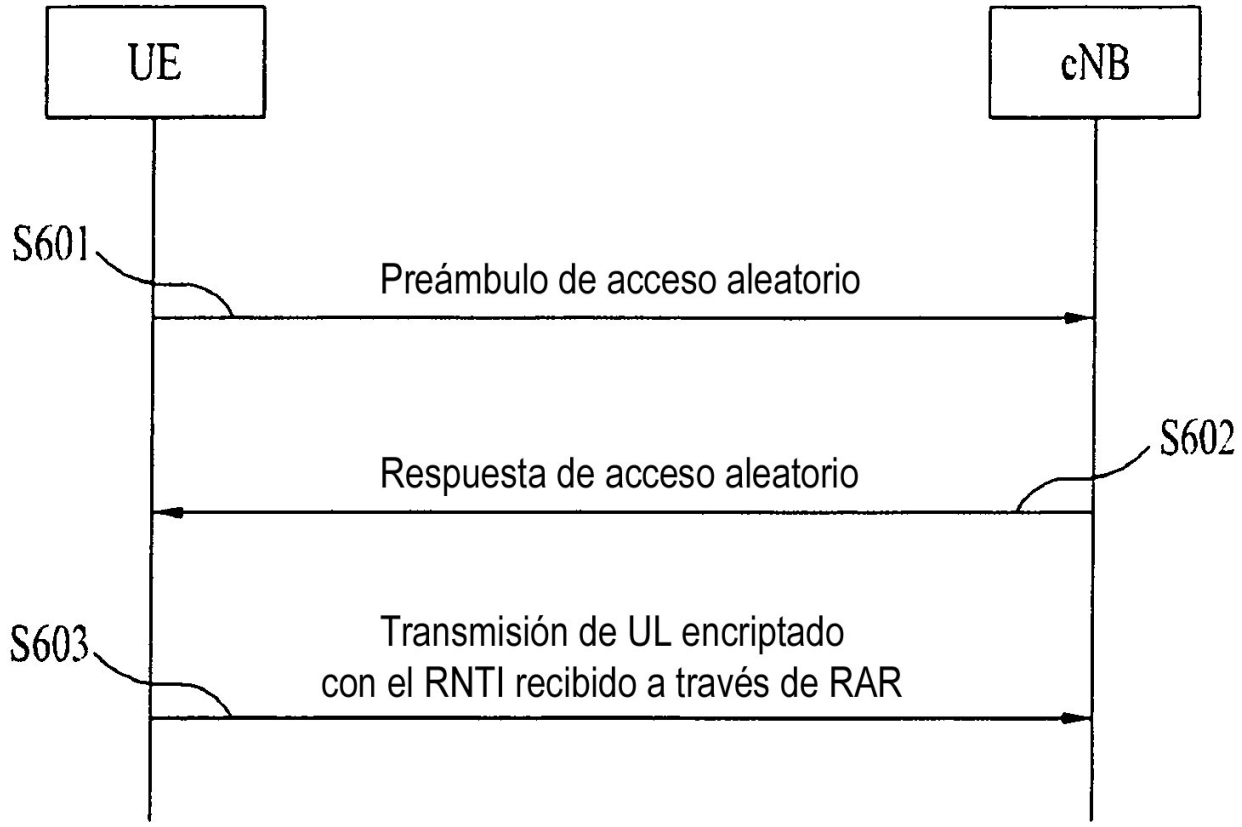

UE
eNB
S601
Preámbulo de acceso aleatorio
S602
Respuesta de acceso aleatorio
S603
Transmisión de UL encriptado
con el RNTI recibido a través de RAR

FIG. 7

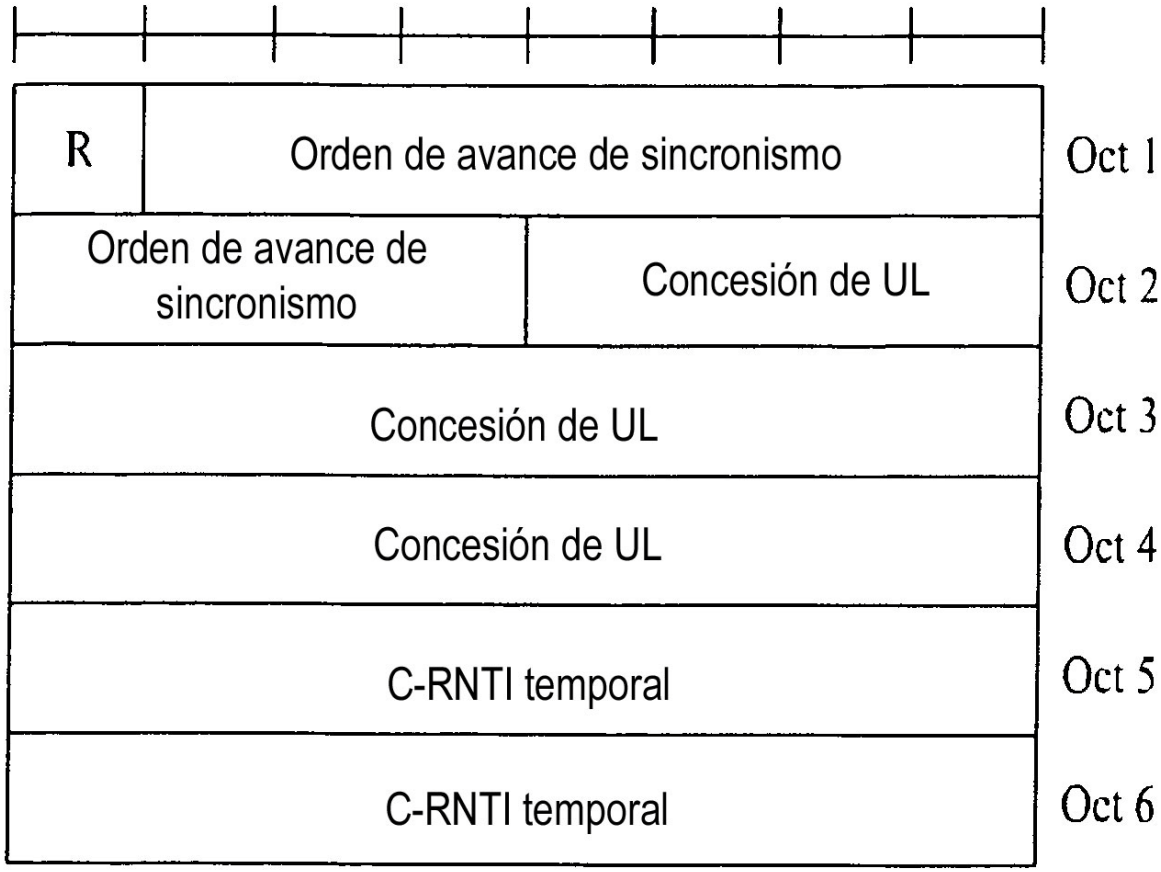

R
Orden de avance de sincronismo
Oct 1
Orden de avance de sincronismo
Concesión de UL
Oct 2
Concesión de UL
Oct 3
Concesión de UL
Oct 4
C-RNTI temporal
Oct 5
C-RNTI temporal
Oct 6

FIG. 8

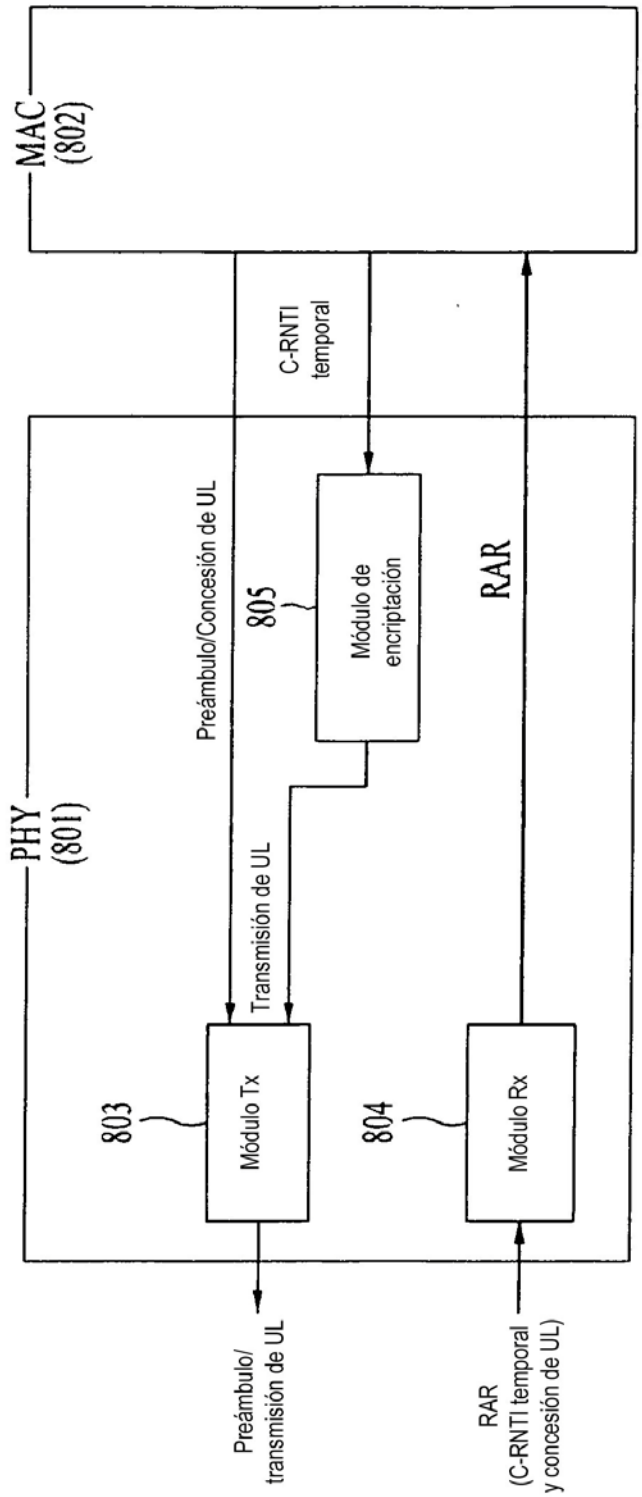
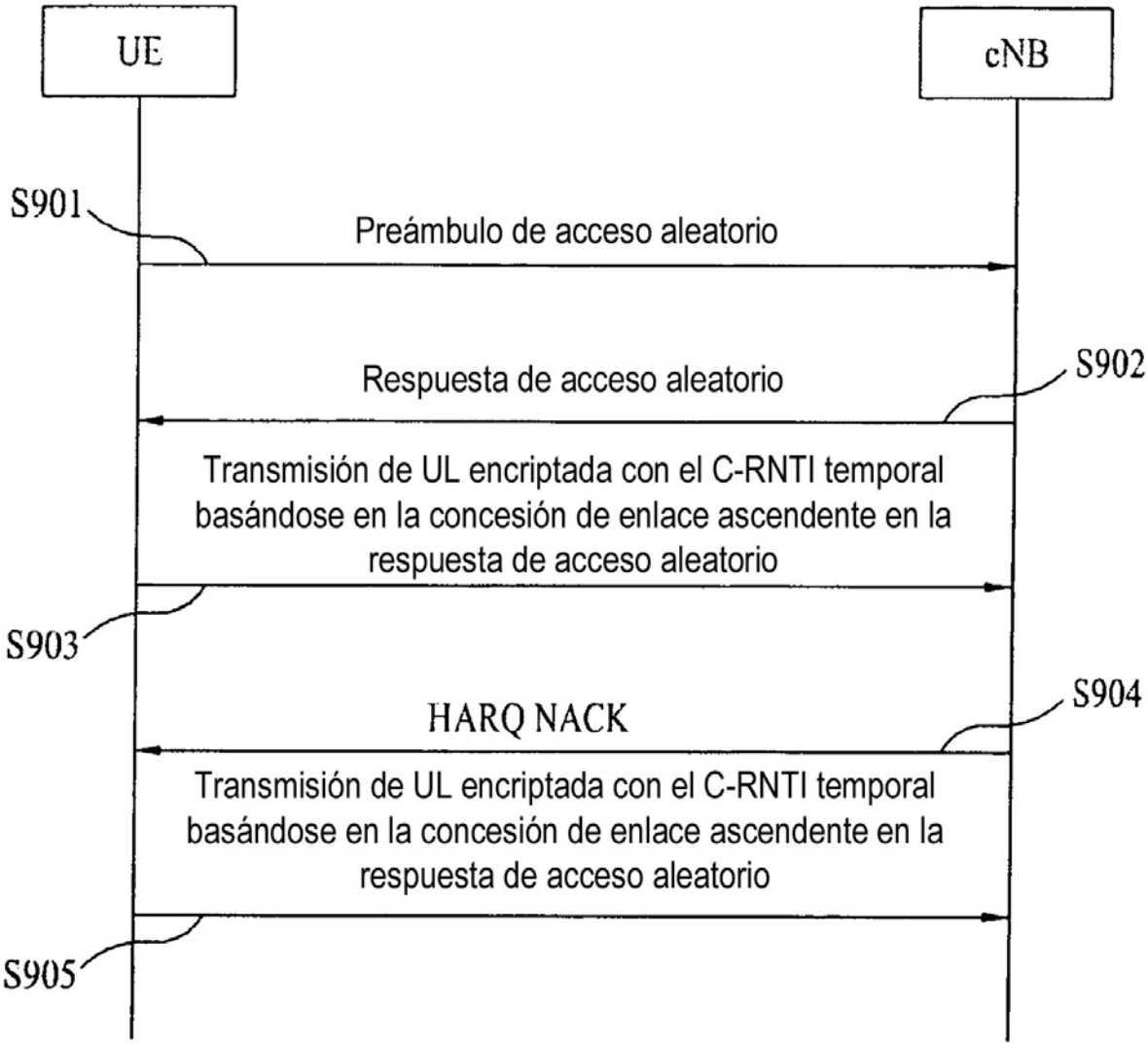

MAC
(802)
C-RNTI
temporal
PHY
(801)
Preámbulo/Concesión de UL
805
Módulo de
encriptación
RAR
Transmisión de UL
803
Módulo Tx
804
Módulo Rx
Preámbulo/
transmisión de UL
RAR
(C-RNTI temporal
y concesión de UL)

FIG. 9


UE
cNB
S901
Preámbulo de acceso aleatorio
Respuesta de acceso aleatorio
S902
Transmisión de UL encriptada con el C-RNTI temporal basándose en la concesión de enlace ascendente en la respuesta de acceso aleatorio
S903
HARQ NACK
S904
Transmisión de UL encriptada con el C-RNTI temporal basándose en la concesión de enlace ascendente en la respuesta de acceso aleatorio
S905