(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 683 728**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.06.2008 PCT/US2008/067934**

(87) Fecha y número de publicación internacional: **24.12.2008 WO08157839**

(96) Fecha de presentación y número de la solicitud europea: **23.06.2008 E 08795981 (3)**

(97) Fecha y número de publicación de la concesión europea: **30.05.2018 EP 2163064**

(54) Título: **Cifrado del mensaje de enlace ascendente planificado en procedimiento de acceso aleatorio**

(30) Prioridad:

21.06.2007 US 945465 P
14.08.2007 US 955867 P
10.06.2008 US 136511

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.09.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
International IP Administration 5775 Morehouse Drive
San Diego, California 92121, US

(72) Inventor/es:

KITAZOE, MASATO

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

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

DESCRIPCIÓN

Cifrado del mensaje de enlace ascendente planificado en procedimiento de acceso aleatorio

ANTECEDENTES

I. Campo

[1] La siguiente descripción se refiere en general a comunicaciones inalámbricas y, más en particular, a controlar el cifrado de mensajes de enlace ascendente en un procedimiento de acceso aleatorio en un sistema de comunicación inalámbrica.

II. Antecedentes

[2] Los sistemas de comunicación inalámbrica están ampliamente desplegados para proporcionar diversos tipos de comunicación; por ejemplo, la voz y/o los datos pueden proporcionarse mediante dichos sistemas de comunicación inalámbrica. Un sistema, o red, habitual de comunicación inalámbrica puede proporcionar a múltiples usuarios acceso a uno o más recursos compartidos (por ejemplo, ancho de banda, potencia de transmisión, etc.). Por ejemplo, un sistema puede usar variadas técnicas de acceso múltiple tales como el multiplexado por división de frecuencia (FDM), el multiplexado por división del tiempo (TDM), el multiplexado por división de código (CDM), el multiplexado por división de frecuencia ortogonal (OFDM) y otras.

[3] En general, los sistemas de comunicación inalámbrica de acceso múltiple pueden prestar soporte simultáneamente a la comunicación para terminales de acceso múltiple. Cada terminal de acceso puede comunicarse con una o más estaciones base mediante transmisiones en enlaces directos e inversos. El enlace directo (o enlace descendente) se refiere al enlace de comunicación desde las estaciones base hasta los terminales de acceso, y el enlace inverso (o enlace ascendente) se refiere al enlace de comunicación desde los terminales de acceso hasta las estaciones base. Este enlace de comunicación puede establecerse *mediante* un sistema de única entrada y única salida, un sistema de múltiples entradas y única salida o un sistema de múltiple entradas y múltiples salidas (MIMO).

[4] Los sistemas de MIMO normalmente emplean múltiples (N_T) antenas de transmisión y múltiples (N_R) antenas de recepción para la transmisión de datos. Un canal de MIMO formado por las N_T antenas de transmisión y las N_R antenas de recepción puede descomponerse en N_S canales independientes, que pueden denominarse canales espaciales, donde $N_S \leq \{_{NT}$, N*R*}. Cada uno de los N_S canales independientes corresponde a una dimensión. Además, los sistemas de MIMO pueden proporcionar un rendimiento mejorado (*por ejemplo*, una mayor eficacia espectral, un mayor caudal de tráfico y/o una mayor fiabilidad) si se utilizan las dimensiones adicionales creadas por las múltiples antenas de transmisión y de recepción.

[5] Los sistemas de MIMO pueden prestar soporte a diversas técnicas de duplexado para dividir las comunicaciones de enlace directo e inverso sobre un medio físico común. Por ejemplo, los sistemas de duplexado por división de frecuencia (FDD) pueden utilizar diferentes regiones de frecuencia para las comunicaciones de enlace directo y de enlace inverso. Además, en los sistemas de duplexado por división del tiempo (TDD), las comunicaciones en el enlace directo y el enlace inverso pueden utilizar una región de frecuencia común, de modo que el principio de reciprocidad permita la estimación del canal de enlace directo a partir del canal de enlace inverso.

[6] Los sistemas de comunicación inalámbrica emplean a menudo una o más estaciones base que proporcionan un área de cobertura. Una estación base típica puede transmitir múltiples flujos de datos para servicios de difusión, multidifusión y/o unidifusión, en los que un flujo de datos puede ser un flujo de datos que puede ser de interés de recepción independiente para un terminal de acceso. Puede emplearse un terminal de acceso dentro del área de cobertura de dicha estación base para recibir uno, más de uno o todos los flujos de datos transportados por el flujo compuesto. Asimismo, un terminal de acceso puede transmitir datos a la estación base o a otro terminal de acceso.

[7] Un terminal de acceso puede utilizar un procedimiento de acceso aleatorio para obtener acceso a un sistema (*por ejemplo,* para obtener la asignación de un canal de comunicaciones y / o recursos asociados, ...). Por ejemplo, el procedimiento de acceso aleatorio puede usarse para el acceso inicial al sistema, el traspaso desde una estación base de origen a una estación base de destino, la sincronización de la temporización del enlace ascendente para la transferencia de datos y similares. Habitualmente, un terminal de acceso envía un preámbulo de acceso aleatorio por el enlace ascendente cuando el terminal de acceso desea obtener acceso al sistema. Una estación base puede recibir el preámbulo de acceso aleatorio y responder con una respuesta de acceso aleatorio enviada por el enlace descendente. En función de la respuesta de acceso aleatorio, el terminal de acceso puede intentar enviar una transmisión planificada por el enlace ascendente a la estación base. Sin embargo, en el caso de acceso aleatorio basado en contienda, la estación base puede desconocer una identidad del terminal de acceso que intenta transmitir la transmisión planificada. Por lo tanto, las técnicas convencionales muchas veces no logran tener en cuenta que la estación base no pueda determinar una identidad de un origen desde el cual se origina la transmisión

planificada, lo que puede ser particularmente problemático cuando dicha transmisión planificada está cifrada.

[8] Puede encontrarse un ejemplo de una técnica convencional que presenta tales problemas en la publicación "Actualización sobre movilidad, seguridad, procedimiento de acceso aleatorio" [Redes Nokia Siemens, Borrador del 3GPP], 23 de mayo de 2007.

SUMARIO

[9] A continuación se ofrece un sumario simplificado de uno o más modos de realización con el fin de proporcionar un entendimiento básico de dichos modos de realización. Este sumario no es una visión general extensiva de todos los modos de realización contemplados y no está previsto para identificar ni elementos clave ni críticos de todos los modos de realización, ni delimitar el alcance de algunos o de todos los modos de realización. Su único propósito es presentar algunos conceptos de uno o más modos de realización de una forma simplificada como preludio a la descripción más detallada que se presenta más adelante.

[10] De acuerdo a una o más realizaciones y la correspondiente divulgación de las mismas, se describen varios aspectos en relación con facilitar el empleo de un procedimiento de acceso aleatorio que aprovecha los datos cifrados y / o no cifrados en un mensaje de enlace ascendente planificado. Se puede enviar un preámbulo de acceso aleatorio desde un terminal de acceso a una estación base, y se puede enviar una respuesta de acceso aleatorio desde la estación base al terminal de acceso. Se puede enviar un mensaje de transmisión planificada desde el terminal de acceso a la estación base basándose en una concesión incluida en la respuesta de acceso aleatorio. Cuando se emplea el acceso aleatorio basado en contienda, el mensaje de transmisión planificada, o una parte del mismo, puede descifrarse. Además, la información no crítica para la seguridad puede enviarse de manera no cifrada en el mensaje de transmisión planificada, mientras que la información crítica para la seguridad puede cifrarse para la transmisión (por ejemplo, incluirse en una parte cifrada del mensaje de transmisión planificada y / o transmitirse en un posterior mensaje cifrado normal de transmisión planificada).

[11] De acuerdo a aspectos relacionados, se describe en la presente un procedimiento que facilita el empleo de un proceso de acceso aleatorio en un entorno de comunicación inalámbrica. El procedimiento puede incluir la transmisión de un preámbulo de acceso aleatorio a una estación base.

Además, el procedimiento puede comprender recibir una respuesta de acceso aleatorio desde la estación base en función del preámbulo de acceso aleatorio. Además, el procedimiento puede incluir la transmisión de un mensaje de transmisión planificada, que incluye al menos una parte que no está cifrada, a la estación base, como lo concede la respuesta de acceso aleatorio cuando se emplea el acceso aleatorio basado en contienda.

[12] Otro aspecto más se refiere a un aparato de comunicaciones inalámbricas que permite utilizar un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. El aparato de comunicaciones inalámbricas puede incluir medios para enviar un preámbulo de acceso aleatorio, que incluye una rúbrica común de acceso aleatorio, a una estación base cuando se emplea el acceso aleatorio basado en contienda. Además, el aparato de comunicaciones inalámbricas puede incluir medios para obtener una respuesta de acceso aleatorio desde la estación base, basándose en el preámbulo de acceso aleatorio. Además, el aparato de comunicaciones inalámbricas puede incluir medios para enviar una transmisión planificada, que incluye al menos una parte no cifrada, a la estación base, según lo concedida por la respuesta de acceso aleatorio cuando se emplea acceso aleatorio basado en contienda.

[13] Según otros aspectos, en el presente documento se describe un procedimiento que facilita el descifrado de los datos obtenidos durante un proceso de acceso aleatorio en un entorno de comunicación inalámbrica. El procedimiento puede incluir recibir un preámbulo de acceso aleatorio desde un terminal de acceso. Además, el procedimiento puede incluir la transmisión de una respuesta de acceso aleatorio al terminal de acceso basándose en el preámbulo de acceso aleatorio. El procedimiento también puede comprender recibir un mensaje de transmisión planificada, que incluye al menos una parte que no está cifrada, desde el terminal de acceso, cuando se utiliza el acceso aleatorio basado en contienda. Además, el procedimiento puede incluir reconocer una identidad del terminal de acceso basándose en la información incluida en la parte del mensaje de transmisión planificada que no está cifrada cuando se emplea un acceso aleatorio basado en la contienda.

[14] Otro aspecto se refiere a un aparato de comunicaciones inalámbricas que permite emplear un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. El aparato de comunicaciones inalámbricas puede incluir medios para obtener un mensaje de transmisión planificada que incluye al menos una parte no cifrada desde el terminal de acceso cuando se utiliza el acceso aleatorio basado en contienda. El aparato de comunicaciones inalámbricas puede incluir además medios para reconocer una identidad del terminal de acceso basándose en la información incluida en la parte no cifrada del mensaje de transmisión planificada. El aparato de comunicaciones inalámbricas también puede incluir medios para recuperar un contexto de seguridad asociado al terminal de acceso, basándose en la identidad reconocida del terminal de acceso. Además, el aparato de comunicaciones inalámbricas puede incluir medios para descifrar un mensaje normal cifrado de transmisión planificada, o una parte cifrada del mensaje de transmisión planificada que incluye la parte no cifrada recibida desde

el terminal de acceso, basándose en el contexto de seguridad recuperado.

[15] Otro aspecto adicional se refiere a un producto de programa informático que puede comprender un medio legible por ordenador. El medio legible por ordenador puede incluir código para realizar el procedimiento de acuerdo a las reivindicaciones adjuntas.

[16] Para el cumplimiento de los objetivos anteriores y los relacionados, los uno o más modos de realización comprenden las características descritas con detalle de aquí en adelante y expuestas particularmente en las reivindicaciones. La descripción siguiente y los dibujos adjuntos estipulan con detalle ciertos aspectos ilustrativos de los uno o más modos de realización. Sin embargo, estos aspectos solo indican unas pocas de las diversas maneras en que pueden usarse los principios de diversos modos de realización, y los modos de realización descritos pretenden incluir todos dichos aspectos y sus equivalentes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[17]

La FIG. 1 es una ilustración de un sistema de comunicación inalámbrica de acuerdo a diversos aspectos expuestos en el presente documento.

La FIG. 2 es una ilustración de un sistema ejemplar que controla el cifrado de mensajes de enlace ascendente en un procedimiento de acceso aleatorio.

La FIG. 3 es una ilustración de un ejemplo de diagrama de señalización de un procedimiento básico de acceso aleatorio de acuerdo a diversos aspectos de la divulgación en cuestión.

La FIG. 4 es una ilustración de un diagrama de señalización ejemplar de la transmisión de mensajes de Control de Recursos de Radio (RRC) de enlace ascendente por un terminal de acceso no sincronizado, de acuerdo a diversos aspectos de la presente divulgación.

La FIG. 5 es una ilustración de un ejemplo de diagrama de señalización que muestra un escenario de traspaso de acuerdo a diversos aspectos de la divulgación en cuestión.

La FIG. 6 es una ilustración de un sistema ejemplar que envía mensajes cifrados y / o no cifrados como parte de un procedimiento de acceso aleatorio.

La FIG. 7 es una ilustración de un diagrama de señalización ejemplar de un procedimiento de acceso aleatorio que comunica información cifrada y no cifrada en el mensaje 3 de acuerdo a diversos aspectos de la divulgación en cuestión.

La FIG. 8 es una ilustración de una metodología ejemplar que facilita el empleo de un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica.

La FIG. 9 es una ilustración de una metodología ejemplar que facilita el descifrado de datos obtenidos durante un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica.

La FIG. 10 es una ilustración de un terminal de acceso ejemplar que transmite mensajes de enlace ascendente planificados, cifrados y / o no cifrados, en un sistema de comunicación inalámbrica.

La FIG. 11 es una ilustración de un sistema ejemplar que evalúa mensajes planificados cifrados o no cifrados, recibidos por un enlace ascendente durante un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica.

La FIG. 12 es una ilustración de un entorno ejemplar de red inalámbrica que puede emplearse junto con los diversos sistemas y procedimientos descritos en el presente documento.

La FIG. 13 es una ilustración de un sistema ejemplar que permite utilizar un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica.

La FIG. 14 es una ilustración de un sistema ejemplar que permite emplear un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica.

DESCRIPCIÓN DETALLADA

[18] Se describirán ahora diversos modos de realización con referencia a los dibujos, en los que se usan números de referencia iguales para referirse a elementos iguales de principio a fin. En la descripción siguiente se

exponen, para fines explicativos, numerosos detalles específicos con el fin de proporcionar una exhaustiva comprensión de uno o más modos de realización. Sin embargo, puede resultar evidente que dicho(s) modo(s) de realización puede(n) llevarse a la práctica sin estos detalles específicos. En otros casos, se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques con el fin de facilitar la descripción de uno o más modos de realización.

[19] Como se usa en esta solicitud, los términos "componente", "módulo", "sistema" y similares están previstos para hacer referencia a una entidad relativa al ordenador, ya sea hardware, firmware, una combinación de hardware y software, software o software en ejecución. Por ejemplo, un componente puede ser, pero no se limita a ser, un proceso que se ejecuta en un procesador, un procesador, un objeto, un módulo ejecutable, un hilo de ejecución, un programa y/o un ordenador. A modo de ilustración, tanto una aplicación que se ejecuta en un dispositivo informático como el dispositivo informático puede ser un componente. Uno o más componentes pueden residir dentro de un proceso y/o hilo de ejecución y un componente puede localizarse en un ordenador y/o estar distribuido entre dos o más ordenadores. Además, estos componentes pueden ejecutarse desde diversos medios legibles por ordenador que tengan diversas estructuras de datos almacenadas en los mismos. Los componentes pueden comunicarse mediante procesos locales y/o remotos, tal como de acuerdo a una señal que tenga uno o más paquetes de datos (*por ejemplo*, datos de un componente que interactúa con otro componente en un sistema local, un sistema distribuido y/o, a través de una red, tal como Internet, con otros sistemas por medio de la señal).

[20] Las técnicas descritas en el presente documento pueden usarse en diversos sistemas de comunicación inalámbrica, tales como sistemas de acceso múltiple por división de código (CDMA), sistemas de acceso múltiple por división del tiempo (TDMA), sistemas de acceso múltiple por división de frecuencia (FDMA), sistemas de acceso múltiple por división ortogonal de frecuencia (OFDMA), sistemas de acceso múltiple por división de frecuencia de única portadora (SC-FDMA) y otros sistemas. Los términos "sistema" y "red" se usan a menudo indistintamente. Un sistema de CDMA puede implementar una tecnología de radio, tal como el acceso por radio terrestre universal (UTRA), CDMA2000, *etc.* El UTRA incluye el CDMA de banda ancha (W-CDMA) y otras variantes del CDMA. CDMA2000 abarca las normas IS-2000, IS-95 e IS-856. Un sistema de TDMA puede implementar una tecnología de radio tal como el Sistema Global de Comunicaciones Móviles (GSM). Un sistema de OFDMA puede implementar una tecnología de radio tal como el UTRA Evolucionado (E-UTRA), la Banda Ancha Ultra Móvil (UMB), el IEEE 802.11 (Wi-Fi), el IEEE 802.16 (WiMAX), el IEEE 802.20, el OFDM Flash, *etc.* El UTRA y el E-UTRA forman parte del Sistema Universal de Telecomunicaciones Móviles (UMTS). La Evolución a Largo Plazo (LTE) del 3GPP es una nueva versión de UMTS que usa E-UTRA, que utiliza OFDMA en el enlace descendente y SC-FDMA en el enlace ascendente.

[21] El acceso múltiple por división de frecuencia de única portadora (SC-FDMA) utiliza modulación de única portadora y ecualización en el dominio de la frecuencia. El SC-FDMA tiene prestaciones similares y esencialmente la misma complejidad global que las de un sistema de OFDMA. Una señal de SC-FDMA tiene una razón de potencia entre máxima y media (PAPR) más baja, debido a su estructura intrínseca de única portadora. El SC-FDMA se puede utilizar, por ejemplo, en comunicaciones de enlace ascendente, donde una PAPR más baja beneficia en gran medida a los terminales de acceso, en términos de eficacia de la potencia de transmisión. En consecuencia, el SC-FDMA se puede implementar como un esquema de acceso múltiple de enlace ascendente en la Evolución a Largo Plazo (LTE) o en el UTRA Evolucionado del 3GPP.

[22] Además, en el presente documento se describen diversos modos de realización en relación con un terminal de acceso. Un terminal de acceso también puede denominarse sistema, unidad de abonado, estación de abonado, estación móvil, móvil, estación remota, terminal remoto, dispositivo móvil, terminal de usuario, terminal, dispositivo de comunicación inalámbrica, agente de usuario, dispositivo de usuario o equipo de usuario (UE). Un terminal de acceso puede ser un teléfono móvil, un teléfono sin cables, un teléfono del protocolo de inicio de sesión (SIP), una estación de bucle local inalámbrico (WLL), un asistente digital personal (PDA), un dispositivo manual con capacidad de conexión inalámbrica, un dispositivo informático u otro tipo de dispositivo de procesamiento conectado a un módem inalámbrico. Además, se describen diversos modos de realización en el presente documento en relación con una estación base. Una estación base puede utilizarse para la comunicación con un terminal o terminales de acceso y también puede denominarse un punto de acceso, un nodo B, un nodo B evolucionado (eNodoB) o utilizando alguna otra terminología.

[23] Además, diversos aspectos o características descritos en el presente documento pueden implementarse como un procedimiento, aparato o artículo de fabricación que use técnicas estándar de programación y/o ingeniería. El término "artículo de fabricación", tal como se usa en el presente documento, pretende abarcar un programa informático accesible desde cualquier dispositivo, portadora o medio legible por ordenador. Por ejemplo, los medios legibles por ordenador pueden incluir, pero sin limitarse a, dispositivos de almacenamiento magnético (*por ejemplo*, un disco duro, un disco flexible, cintas magnéticas, *etc.*), discos ópticos (*por ejemplo,* un disco compacto (CD), un disco versátil digital (DVD), *etc.*), tarjetas inteligentes y dispositivos de memoria flash (*por ejemplo,* EPROM, tarjeta, lápiz de memoria, unidad de llavero, *etc.*). Adicionalmente, diversos medios de almacenamiento descritos en el presente documento pueden representar uno o más dispositivos y/u otros medios legibles por máquina para almacenar información. El término "medios legibles por máquina" puede incluir, sin limitarse a, canales inalámbricos y otros diversos medios que pueden almacenar, contener y/o transportar instrucciones y/o datos.

[24] Con referencia ahora a la **Fig. 1**, se ilustra un sistema de comunicación inalámbrica 100 de acuerdo a diversos modos de realización presentados en el presente documento. El sistema 100 comprende una estación base 102 que puede incluir múltiples grupos de antenas. Por ejemplo, un grupo de antenas puede incluir las antenas 104 y 106, otro grupo puede comprender las antenas 108 y 110 y un grupo adicional puede incluir las antenas 112 y 114. Se ilustran dos antenas para cada grupo de antenas; sin embargo, pueden usarse más o menos antenas para cada grupo. La estación base 102 puede incluir adicionalmente una cadena transmisora y una cadena receptora, cada una de las cuales puede comprender a su vez una pluralidad de componentes asociados a la transmisión y la recepción de señales (*por ejemplo*, procesadores, moduladores, multiplexores, desmoduladores, desmultiplexores, antenas, *etc.*), como apreciará un experto en la materia.

[25] La estación base 102 puede comunicarse con uno o más terminales de acceso, tales como el terminal de acceso 116 y el terminal de acceso 122; sin embargo, se apreciará que la estación base 102 puede comunicarse esencialmente con cualquier número de terminales de acceso similares a los terminales de acceso 116 y 122. Los terminales de acceso 116 y 122 pueden ser, por ejemplo, teléfonos celulares, teléfonos inteligentes, ordenadores portátiles, dispositivos de comunicación portátiles, dispositivos informáticos portátiles, radios por satélite, sistemas de localización global, PDA y/o cualquier otro dispositivo adecuado para la comunicación por el sistema de comunicación inalámbrica 100. Como se representa, el terminal de acceso 116 está en comunicación con las antenas 112 y 114, en donde las antenas 112 y 114 transmiten información al terminal de acceso 116 por un enlace directo 118 y reciben información desde el terminal de acceso 116 por un enlace inverso 120. Además, el terminal de acceso 122 está en comunicación con las antenas 104 y 106, en donde las antenas 104 y 106 transmiten información al terminal de acceso 122 por un enlace directo 124 y reciben información desde el terminal de acceso 122 por un enlace inverso 126. En un sistema de duplexado por división de frecuencia (FDD), el enlace directo 118 puede utilizar una banda de frecuencias diferente a la usada por el enlace inverso 120, y el enlace directo 124 puede emplear una banda de frecuencias diferente a la empleada por el enlace inverso 126, por ejemplo. Además, en un sistema de duplexado por división del tiempo (TDD), el enlace directo 118 y el enlace inverso 120 pueden utilizar una banda de frecuencias común, y el enlace directo 124 y el enlace inverso 126 pueden utilizar una banda de frecuencias común.

[26] Cada grupo de antenas y/o el área en la que estén designadas para comunicar puede denominarse un sector de la estación base 102. Por ejemplo, los grupos de antenas pueden diseñarse para comunicar con terminales de acceso en un sector de las áreas cubiertas por la estación base 102. En la comunicación por los enlaces directos 118 y 124, las antenas de transmisión de la estación base 102 pueden utilizar la conformación de haces para mejorar la razón entre señal y ruido de los enlaces directos 118 y 124 para los terminales de acceso 116 y 122. Además, mientras la estación base 102 utiliza la conformación de haces para transmitir a los terminales de acceso 116 y 122 esparcidos de manera aleatoria a través de una cobertura asociada, los terminales de acceso de las células vecinas pueden estar sometidos a menos interferencias en comparación con una estación base que transmite a través de una sola antena a todos sus terminales de acceso.

[27] Se puede utilizar un procedimiento de acceso aleatorio en el sistema 100. Por ejemplo, el procedimiento de acceso aleatorio puede ser usado por los terminales de acceso 116 y 122 para el acceso inicial, el traspaso hacia y / o desde la estación base 102, la sincronización de temporización (por ejemplo, re-entrada desde la modalidad no sincronizada, ...), y similares. Un procedimiento de acceso aleatorio incluye habitualmente la transmisión de un preámbulo de acceso aleatorio (*por ejemplo,* el mensaje 1, ...) por un terminal de acceso (*por ejemplo,* el terminal de acceso 116, el terminal de acceso 122, ...) a la estación base 102 por el enlace ascendente, la transmisión de una respuesta de acceso aleatorio (*por ejemplo,* el mensaje 2, ...) desde la estación base 102 al terminal de acceso por el enlace descendente, basándose en el preámbulo de acceso aleatorio recibido, y la transmisión de una transmisión planificada (*por ejemplo,* el mensaje 3, ...) desde el terminal de acceso a la estación base 102 por el enlace ascendente, donde dicha transmisión planificada es concedida por el mensaje de respuesta de acceso aleatorio. Como se usa en el presente documento, el término "mensaje 3" se refiere a la transmisión planificada enviada por el terminal de acceso a la estación base 102, según lo concedido por el mensaje de respuesta de acceso aleatorio desde la estación base 102.

[28] Además, hay dos tipos de procedimientos de acceso aleatorio que pueden aprovecharse en el sistema 100: acceso aleatorio basado en contienda y acceso aleatorio no basado en contienda. Según una ilustración, en el acceso aleatorio basado en contienda, dos o más terminales de acceso 116, 122 pueden transmitir preámbulos de acceso aleatorio a la estación base 102 en un tiempo esencialmente similar por un recurso compartido (*por ejemplo, un* canal) mientras disputan el acceso al sistema. Sin embargo, la estación base 102, habitualmente, no puede identificar los terminales de acceso 116, 122 que transmiten estos preámbulos de acceso aleatorio (*por ejemplo,* se puede enviar una rúbrica de acceso aleatorio común como al menos parte de los preámbulos de acceso aleatorio desde más de un terminal de acceso 116, 122). La estación base 102 puede enviar una respuesta de acceso aleatorio por el enlace descendente basándose en un preámbulo de acceso aleatorio recibido, y obtener una transmisión planificada desde un terminal de acceso en respuesta a la concesión incluida en la respuesta de acceso aleatorio; sin embargo, la estación base 102 puede ser nuevamente incapaz de identificar el terminal de acceso que transmite la transmisión planificada (*por ejemplo,* el mensaje 3, ...) a menos que se proporcione un identificador específico del terminal de acceso en dicha transmisión planificada. Además, en un acceso aleatorio no basado en

contienda, una rúbrica de acceso aleatorio específica de terminal de acceso puede ser proporcionada a, determinada por, *etc.*, un terminal de acceso antes de enviar el preámbulo de acceso aleatorio, y esta rúbrica de acceso aleatorio específica del terminal de acceso puede ser transmitida por el terminal de acceso (*por ejemplo,* como al menos parte del preámbulo de acceso aleatorio, el mensaje 1 en un procedimiento de acceso aleatorio, ...) a la estación base 102. De este modo, al recibir la rúbrica de acceso aleatorio específica del terminal de acceso en el acceso aleatorio no basado en contienda, la estación base 102 puede identificar el terminal de acceso desde el que se envió la rúbrica de acceso aleatorio. Además, esta información relacionada con la identificación puede ser utilizada por la estación base 102 para identificar un origen de una transmisión planificada recibida (*por ejemplo,* el mensaje 3, ...) que responde a una respuesta de acceso aleatorio enviada por la estación base 102.

[29] De acuerdo a una ilustración, cuando se emplea el acceso aleatorio basado en contienda, la transmisión planificada (*por ejemplo,* el mensaje 3, ...) puede descifrarse. De acuerdo a otro ejemplo, cuando se utiliza el acceso aleatorio basado en contienda, al menos una parte del mensaje de transmisión planificada (*por ejemplo,* el mensaje 3, ...) puede descifrarse. El envío de un mensaje 3 no cifrado o una parte de dicho mensaje 3 sin cifrar puede provenir de que la red (*por ejemplo,* la estación base 102, ...) no pueda determinar qué terminal de acceso transmitió el mensaje 3 al recibirlo. En cambio, el contenido del mensaje 3 puede evaluarse para reconocer el origen asociado de dicho mensaje. Esta evaluación se realiza sobre datos no cifrados (*por ejemplo,* el mensaje no cifrado 3 o una parte no cifrada del mismo) ya que la estación base 102 no puede descifrar un mensaje cifrado sin conocer la identidad del terminal de acceso que transmite el mensaje cifrado. En el acceso aleatorio no basado en contienda, esta limitación no existe. Por consiguiente, cuando se emplea el acceso aleatorio basado en contienda, un terminal de acceso puede enviar información no crítica para la seguridad (*por ejemplo,* el identificador de terminal de acceso, el discriminador de mensaje, ...) en el mensaje de transmisión planificada no cifrado (*por ejemplo,* el mensaje 3, ...) y / o en la parte no cifrada de un mensaje de transmisión planificada (por *ejemplo,* el mensaje 3, ...). Además, el terminal de acceso puede transmitir información crítica para la seguridad en un mensaje cifrado diferente y / o una parte cifrada del mensaje de transmisión planificada (*por ejemplo,* el mensaje 3, ...).

[30] Volviendo ahora a la **Fig. 2**, se ilustra un sistema 200 que controla el cifrado de los mensajes de enlace ascendente en un procedimiento de acceso aleatorio. El sistema 200 incluye un terminal de acceso 202 y una estación base 204; sin embargo, se ha de apreciar que el sistema 200 puede incluir cualquier número de terminales de acceso similares al terminal de acceso 202 y / o cualquier número de estaciones base similares a la estación base 204. El terminal de acceso 202 y la estación base 204 pueden transmitir y / o recibir, cada uno, información, señales, datos, instrucciones, comandos, bits, símbolos y similares.

[31] El terminal de acceso 202 puede incluir además un solicitante de acceso aleatorio 206, un generador de mensajes no cifrados 208 y un generador de mensajes cifrados 210. Además, la estación base 204 puede incluir un otorgante de acceso aleatorio 212, un identificador de origen de mensaje 214 y un determinador de contexto de seguridad 216. El solicitante de acceso aleatorio 206 transmite un preámbulo de acceso aleatorio a la estación base 204. En caso de acceso aleatorio basado en contienda, el solicitante de acceso aleatorio 206 puede enviar una rúbrica genérica de acceso aleatorio como al menos parte del preámbulo de acceso aleatorio. Además, en caso de acceso aleatorio no basado en contienda, el solicitante de acceso aleatorio 206 puede transmitir una rúbrica de acceso aleatorio particular a partir de un conjunto de rúbricas de acceso aleatorio, como al menos parte del preámbulo de acceso aleatorio. Por ejemplo, la rúbrica particular de acceso aleatorio puede asignarse al terminal de acceso 202, mientras que al menos una rúbrica diferente de acceso aleatorio del conjunto puede asignarse a al menos un terminal de acceso diferente (no mostrado). De acuerdo a otra ilustración, se contempla que el solicitante de acceso aleatorio 206 pueda determinar la rúbrica de acceso aleatorio particular a emplear del conjunto al operar en una modalidad de acceso aleatorio no basado en contienda. La rúbrica de acceso aleatorio particular puede ser una rúbrica dedicada que incluye un patrón de bits único para el terminal de acceso 202 (*por ejemplo,* otros terminales de acceso (no mostrados) no usarán esta rúbrica dedicada, ...).

[32] A modo de otra ilustración, el solicitante de acceso aleatorio 206 (y / o el terminal de acceso 202 en general) puede determinar si se está utilizando acceso aleatorio basado en contienda o acceso aleatorio no contencioso en el sistema 200. Por ejemplo, el solicitante de acceso aleatorio 206 puede identificar el tipo de procedimiento de acceso aleatorio que se utiliza en función de si el procedimiento de acceso aleatorio se está empleando para el acceso inicial, la re-entrada desde la modalidad no sincronizada, el traspaso, etc. (*por ejemplo,* el tipo del procedimiento de acceso aleatorio puede predeterminarse en función del uso de dicho procedimiento, ...). Sin embargo, el tema en cuestión reivindicado no está limitado a lo anterior.

[33] El solicitante de acceso aleatorio 206 puede transmitir un preámbulo de acceso aleatorio en el enlace ascendente siempre que el terminal de acceso 202 desee acceder al sistema (*por ejemplo,* si el terminal de acceso 202 tiene datos para enviar, si el sistema localiza el terminal de acceso 202, si el terminal de acceso 202 recibe un comando de traspaso para pasar desde una estación base de origen a una estación base de destino, ...). Un preámbulo de acceso aleatorio también puede denominarse solicitud de acceso, rúbrica de acceso, sonda de acceso, sonda de acceso aleatorio, secuencia de rúbrica, secuencia de rúbrica del Canal de Acceso Aleatorio (RACH), *etc.* El preámbulo de acceso aleatorio puede incluir varios tipos de información y se pueden enviar de varias maneras.

[34] Además, la estación base 204 puede recibir el preámbulo de acceso aleatorio y el otorgante de acceso aleatorio 212 puede responder enviando una respuesta de acceso aleatorio al terminal de acceso 202. Una respuesta de acceso aleatorio también puede denominarse concesión de acceso (AGCH), respuesta de acceso, *etc.* La respuesta de acceso aleatorio puede transportar varios tipos de información y puede enviarse de diversas maneras. Por ejemplo, la respuesta de acceso aleatorio puede incluir recursos de canal de control, recursos de enlace ascendente, información de control y demás para el terminal de acceso 202. A modo de ilustración, los recursos del canal de control pueden incluir recursos del Indicador de Calidad del Canal (CQI), utilizados para enviar el CQI en el enlace ascendente mediante el terminal de acceso 202, recursos de control de potencia utilizados para enviar correcciones de control de potencia en el enlace descendente al terminal de acceso 202, etc. Además, la información de control puede incluir información de temporización utilizada para ajustar la temporización de transmisión del terminal de acceso 202, las correcciones de control de potencia utilizadas para ajustar la potencia de transmisión del terminal de acceso 202 y similares.

[35] El terminal de acceso 202 puede recibir la respuesta de acceso aleatorio enviada por el otorgante de acceso aleatorio 212 de la estación base 204. La respuesta de acceso aleatorio puede otorgar recursos de enlace ascendente para ser usados por el terminal de acceso 202. Además, el terminal de acceso 202 (por ejemplo, el generador de mensajes no cifrados 208, el generador de mensajes cifrados 208, un evaluador de concesiones (no mostrado) incluido en el terminal de acceso 202, ...) puede reconocer los recursos de enlace ascendente concedidos al terminal de acceso 202 en la respuesta de acceso aleatorio. A continuación, el generador de mensajes no cifrados 208 y / o el generador de mensajes cifrados 210 puede producir mensajes de enlace ascendente o partes de mensajes de enlace ascendente que pueden enviarse desde el terminal de acceso 202 a la estación base 204. Por ejemplo, los recursos de enlace ascendente otorgados pueden utilizarse para transmitir un mensaje 3 producido por el generador de mensajes no cifrados 208 y / o el generador de mensajes cifrados 210.

[36] De acuerdo a un ejemplo, cuando se emplea el acceso aleatorio basado en contienda, el generador de mensajes no cifrados 208 puede producir un mensaje 3 no cifrado para su transmisión a la estación base 204. El mensaje no cifrado 3 puede transmitirse a la estación base 204 en lugar de un mensaje cifrado ya que la red (*por ejemplo,* la estación base 204, ...) puede carecer del conocimiento del originador del mensaje 3 (*por ejemplo* el identificador de origen de mensajes 214 puede ser incapaz de determinar una identidad del terminal de acceso 202 a partir de un preámbulo de acceso aleatorio enviado por el enlace ascendente por el solicitante de acceso aleatorio 206 del terminal de acceso 202 cuando se usa el acceso aleatorio basado en contienda, ...). Si la estación base 204 ignora el originador del mensaje 3 y el mensaje 3 fuera a ser cifrado, la estación base 204 no sabría qué configuración de seguridad aplicar para descifrar dicho mensaje cifrado (*por ejemplo,* la estación base 204 no podría descifrar el mensaje cifrado 3 cuando se utiliza el acceso aleatorio basado en contienda, ...). Por lo tanto, el terminal de acceso 202 no puede aplicar el cifrado para el mensaje 3 de enlace ascendente transmitido en el acceso aleatorio basado en contienda, incluso si la seguridad del Control de Recursos de Radio (RRC) está activa. Por el contrario, el terminal de acceso 202 puede enviar el mensaje 3 sin cifrar debido a las limitaciones anteriores en varios escenarios que incluyen, pero no se limitan a, la transmisión de traspaso completo en una célula de destino, la transmisión de un fallo de traspaso en una célula de origen, la sincronización de temporización de enlace ascendente para la transferencia de datos, etc.

[37] Siguiendo este ejemplo, el generador de mensajes no cifrados 208 puede producir un mensaje no cifrado (*por ejemplo,* el mensaje 3 no cifrado, ...) que incluye información, parámetros, *etc.*, que no necesitan ser cifrados. Por ejemplo, el mensaje no cifrado construido por el generador de mensajes no cifrados 208 puede incluir un identificador temporal tal como un Identificador Temporal de Red de Radio Celular (C-RNTI), correspondiente al terminal de acceso 202; sin embargo, ha de apreciarse que puede usarse cualquier tipo de identificador diferente, en lugar de o además del C-RNTI. Además, el generador de mensajes no cifrados 208 puede determinar información, parámetros, *etc.*, dispares (*por ejemplo,* información no crítica para la seguridad, ...) que pueden transmitirse como parte del mensaje de enlace ascendente no cifrado (*por ejemplo,* el mensaje 3 no cifrado, ...). Además, la información crítica para la seguridad puede incluirse en uno o más mensajes cifrados producidos por el generador de mensajes cifrados 210 y transmitidos después de un acceso aleatorio de acuerdo a este ejemplo. Adicionalmente, el mensaje 3 puede ser transmitido por el terminal de acceso 202 *mediante* el uso del Control de Enlace de Radio - Modalidad Transparente (RLCTM).

[38] Al enviar un mensaje 3 no cifrado procedente del generador de mensajes no cifrados 208 según el ejemplo mencionado anteriormente, el identificador de origen de mensaje 214 puede evaluar el mensaje 3 no cifrado para determinar que el terminal de acceso 202 transmitió dicho mensaje 3 no cifrado. El identificador de origen de mensaje 214 puede analizar de manera similar al menos un mensaje no cifrado 3 distinto, enviado desde al menos un terminal de acceso distinto (no mostrado) para identificar el(los) origen(es) correspondiente(s). Por ejemplo, el mensaje no cifrado 3 producido por el generador de mensajes no cifrados 208 y enviado por el terminal de acceso 202 puede incluir el identificador temporal (*por ejemplo,* C-RNTI, ...) asociado al terminal de acceso 202. Además, el identificador de origen de mensaje 214 puede analizar este identificador temporal para reconocer que dicho identificador corresponde al terminal de acceso 202.

[39] Tras la identificación, por el identificador de origen de mensaje 214, del origen del mensaje no cifrado, el determinador de contexto de seguridad 216 puede reconocer un contexto de seguridad asociado al origen

identificado. Por ejemplo, cuando el identificador de origen de mensaje 214 determina que el terminal de acceso 202 es el origen de un mensaje 3 no cifrado, el determinador de contexto de seguridad 216 puede identificar, recuperar, generar, *etc.*, el contexto de seguridad correspondiente al terminal de acceso 202. A modo de ilustración, la estación base 204 puede haber asociado previamente el terminal de acceso 202 a un contexto de seguridad dado mientras el terminal de acceso 202 estaba en modalidad conectada en un momento anterior, y este contexto de seguridad dado puede retenerse en la memoria asociada a la estación base 204 para una recuperación posterior cuando se realice el procedimiento de acceso aleatorio. Alternativamente, en el escenario de traspaso, el contexto de seguridad asociado al terminal de acceso 202 puede obtenerse desde una estación base diferente (no mostrada) cuando al terminal de acceso 202 se envía un comando de traspaso desde la estación base diferente para iniciar el traspaso a la estación base 204. El contexto de seguridad, tal como se reconoce, puede utilizarse a continuación para descifrar el(los) mensaje(s) codificado(s) generado(s) por el generador de mensajes cifrados 210 y enviado(s) por el terminal de acceso 202.

[40] Además, el identificador de origen de mensaje 214 y / o la estación base 204, en general, pueden enviar un mensaje de resolución de contienda (*por ejemplo,* el mensaje 4, ...) al terminal de acceso 202 al determinar una identidad del origen del mensaje 3 no cifrado. A continuación, el generador de mensajes cifrados 210 puede producir una transmisión cifrada planificada normal que puede enviarse por el enlace ascendente. Además, se contempla que el generador de mensajes cifrados 210 puede utilizar esencialmente cualquier tipo de técnica(s) de cifrado. Además, el contexto de seguridad correspondiente al terminal de acceso 202, según lo reconocido por el determinador de contexto de seguridad 216, puede ser aprovechado por la estación base 204 para descifrar los mensajes cifrados producidos por el generador de mensajes cifrados 210 y enviados por el enlace ascendente.

[41] A modo de otra ilustración, cuando se emplea el acceso aleatorio no basado en contienda, el identificador de origen de mensaje 214 puede identificar el terminal de acceso 202 como el origen de un preámbulo de acceso aleatorio cuando es transmitido por el solicitante de acceso aleatorio 206 del terminal de acceso 202. Por ejemplo, el identificador de origen de mensaje 214 puede reconocer una rúbrica dada de acceso aleatorio específica de terminal de acceso, incluida en el preámbulo de acceso aleatorio como asociada al terminal de acceso 202. Por lo tanto, el terminal de acceso 202 puede enviar un mensaje cifrado 3 generado por el generador de mensajes cifrados 210 por el enlace ascendente a la estación base 204, ya que el determinador de contexto de seguridad 216 de la estación base 204 puede identificar un contexto de seguridad asociado al terminal de acceso 202 a ser utilizado para el descifrado, basándose en el preámbulo de acceso aleatorio (*por ejemplo,* en lugar de basarse en el mensaje 3 como es el caso para el acceso aleatorio basado en contienda). En un aspecto, el terminal de acceso 202 puede enviar un mensaje de RRC cifrado producido por el generador de mensajes cifrados 210 cuando sea posible (*por ejemplo,* en el acceso aleatorio no basado en contienda, el mensaje 3 está cifrado si la seguridad está activa, ...). A diferencia del acceso aleatorio basado en contienda, el terminal de acceso 202 no tiene una restricción específica en cuanto a lo que puede enviar en el mensaje 3 en el escenario de acceso aleatorio no basado en contienda. Por lo tanto, el terminal de acceso 202 puede aplicar diferentes restricciones (*por ejemplo,* realizar diferentes acciones, ...) según el tipo de procedimiento de acceso aleatorio que se utilice. Sin embargo, el tema en cuestión reivindicado no está limitado a los ejemplos antes mencionados.

[42] Ahora, haciendo referencia a la **Fig. 3**, se ilustra un ejemplo de diagrama de señalización 300 de un procedimiento de acceso aleatorio básico. El procedimiento de acceso aleatorio puede llevarse a cabo entre un terminal de acceso (*por ejemplo,* el terminal de acceso 202 de la figura 2, ...) y una estación base (*por ejemplo,* la estación base 204 de la figura 2, ...). En 302, el terminal de acceso transmite un preámbulo de acceso aleatorio a la estación base. El preámbulo de acceso aleatorio se puede denominar mensaje 1. En 304, la estación base transmite una respuesta de acceso aleatorio al terminal de acceso. La respuesta de acceso aleatorio se puede denominar mensaje 2. En 306, el terminal de acceso transmite una transmisión planificada a la estación base de acuerdo a una concesión proporcionada por la respuesta de acceso aleatorio. La transmisión planificada se puede denominar mensaje 3. Además, la transmisión planificada se puede transmitir con el Control de Enlace de Radio - Modalidad Transparente (RLC-TM). En 308, la estación base transmite un mensaje de resolución de contienda al terminal de acceso. El mensaje de resolución de contienda se puede denominar mensaje 4. Además, el mensaje de resolución de contienda puede significar un final del procedimiento de acceso aleatorio.

[43] Pasando a la **Fig. 4**, se ilustra un ejemplo de diagrama de señalización 400 de transmisión de mensajes de Control de Recursos de Radio (RRC) de enlace ascendente por un terminal de acceso no sincronizado. El diagrama de señalización 400 ilustra el uso del acceso aleatorio basado en contienda para el reingreso por el terminal de acceso desde una modalidad no sincronizada. En 402, el terminal de acceso transmite un preámbulo de acceso aleatorio a una estación base de servicio. Por ejemplo, se puede incluir una rúbrica de acceso aleatorio común como al menos parte del preámbulo de acceso aleatorio y, por lo tanto, la estación base de servicio puede ser incapaz de determinar el origen del preámbulo de acceso aleatorio. En 404, la estación base servidora puede enviar una respuesta de acceso aleatorio al terminal de acceso. La respuesta de acceso aleatorio puede responder al preámbulo de acceso aleatorio y / o puede proporcionar una concesión de enlace ascendente al terminal de acceso.

[44] En 406, el terminal de acceso puede utilizar la concesión de enlace ascendente para transmitir el mensaje 3, que no está cifrado, a la estación base de servicio. A modo de ejemplo, el mensaje 3 puede incluir un identificador correspondiente al terminal de acceso. Además, el mensaje 3 puede indicar a la estación base de servicio que el

procedimiento es para datos de enlace ascendente, transmisión de mensajes, *etc.* (*por ejemplo,* el mensaje 3 puede incluir un discriminador de mensajes, ...). En 408, en respuesta al mensaje 3, la estación base de servicio puede enviar un mensaje de resolución de contienda al terminal de acceso. Por ejemplo, el mensaje de resolución de contienda puede incluir otra concesión de enlace ascendente para el terminal de acceso. Además, el mensaje de resolución de contienda puede indicar al terminal de acceso que se ha completado la re-entrada a la modalidad sincronizada y / o que el terminal de acceso puede emplear cifrado para posteriores transmisiones de enlace ascendente (*por ejemplo,* el mensaje de resolución de contienda puede significar un final para el procedimiento de acceso aleatorio, ...). En 410, el terminal de acceso transmite un mensaje de transmisión planificada normal, que está cifrado, a la estación base de servicio. Por ejemplo, el terminal de acceso puede utilizar la concesión de enlace ascendente incluida en el mensaje de resolución de contienda para enviar este mensaje cifrado. A diferencia del mensaje 3 no cifrado, que puede incluir el identificador relacionado con el terminal de acceso y / o un indicador en cuanto al tipo de datos a transmitir por el terminal de acceso, el mensaje normal cifrado de transmisión planificada puede ser un mensaje efectivo del RRC (*por ejemplo,* un informe de medición, que incluye información crítica para la seguridad, ...). Además, las posteriores transmisiones de enlace ascendente planificadas desde el terminal de acceso a la estación base de servicio, mientras el terminal de acceso permanece en modalidad sincronizada, pueden cifrarse de manera similar.

[45] Con referencia a la **Fig. 5**, se ilustra un ejemplo de diagrama de señalización 500 que muestra un escenario de traspaso. El traspaso puede llevarse a cabo de manera tal que un terminal de acceso pase de ser servido por una estación base de origen a ser servido por una estación base de destino. El traspaso puede implicar un cambio de configuración de seguridad, que puede provocar que el terminal de acceso envíe información crítica relacionada con la seguridad a la estación base de destino.

[46] En 502, la estación base de origen puede transmitir un comando de traspaso al terminal de acceso. El comando de traspaso puede iniciar el terminal de acceso para el traspaso a la estación base de destino. Además, aunque no se muestra, se contempla que la estación base de origen pueda interactuar con la estación base de destino antes de que el terminal de acceso comience el procedimiento de acceso aleatorio. Por ejemplo, la estación base de origen puede emplear tal interacción para transmitir un contexto de seguridad, asociado al terminal de acceso, a la estación base de destino.

[47] En 504, el terminal de acceso transmite un preámbulo de acceso aleatorio a la estación base de destino en respuesta a la recepción del comando de traspaso desde la estación base de origen. Como se puede emplear el acceso aleatorio basado en contienda, la estación base de destino puede ser incapaz de determinar una identidad del origen del preámbulo de acceso aleatorio. En 506, se puede transmitir una respuesta de acceso aleatorio desde la estación base de destino al terminal de acceso. En 508, el terminal de acceso transmite un mensaje no cifrado 3 a la estación base de destino en respuesta a la respuesta de acceso aleatorio recibida. El mensaje 3 no cifrado puede ser utilizado por el terminal de acceso para la transmisión de información no crítica para la seguridad (*por ejemplo,* información completa de traspaso no crítico, un identificador relacionado con el terminal de acceso, tal como un C-RNTI, un discriminador de mensajes, ...). En 510, la estación base de destino transmite un mensaje de resolución de contienda al terminal de acceso. En 512, el terminal de acceso envía una transmisión planificada normal, que está cifrada, a la estación base de destino. Por ejemplo, esta transmisión planificada, normal y cifrada puede incluir información crítica para la seguridad (*por ejemplo,* información crítica de traspaso completo, ...).

[48] Como se muestra en los ejemplos de las Figuras 4 y 5, en el acceso aleatorio basado en contienda, el mensaje 3 puede estar no cifrado. Además, el terminal de acceso puede transmitir información no crítica con el mensaje 3 que no está cifrado. Además, el terminal de acceso puede utilizar otro mensaje (*por ejemplo,* transmisión planificada normal en 410 o 512, ...) para transmitir información que necesita cifrado después del procedimiento de acceso aleatorio basado en contienda. Además, en el acceso aleatorio no basado en contienda, el mensaje 3 se puede cifrar si la seguridad está activa. En consecuencia, el terminal de acceso puede realizar diferentes acciones según el tipo de procedimiento de acceso aleatorio (*por ejemplo,* cifrar o descifrar el mensaje 3 en función del tipo de procedimiento de acceso aleatorio, incluir o excluir un identificador en el mensaje 3 como una función del tipo de procedimiento de acceso aleatorio, controlar la información incluida en el mensaje 3 basándose en el tipo de procedimiento de acceso aleatorio, retrasar la información crítica para la seguridad a incluir en un mensaje cifrado basándose en el tipo de procedimiento de acceso aleatorio, ...). Aunque los ejemplos anteriores describen la totalidad o la mayor parte del mensaje 3 como no cifrado para el acceso aleatorio basado en contienda, se contempla que una parte del mensaje 3 pueda ser no cifrado, mientras que el resto del mensaje 3 pueda ser cifrado como se describe en los ejemplos siguientes.

[49] Con referencia a la **Fig. 6**, se ilustra un sistema 600 que envía mensajes cifrados y / o no cifrados como parte de un procedimiento de acceso aleatorio. El sistema 600 incluye el terminal de acceso 202 y la estación base 204, donde el terminal de acceso 202 puede incluir el solicitante de acceso aleatorio 206, el generador de mensajes no cifrados 208 y el generador de mensajes cifrados 210, y la estación base 204 pueden incluir el otorgante de acceso aleatorio 212, el identificador de origen de mensaje 214 y el determinador del contexto de seguridad 216. Aunque no se muestra, ha de apreciarse que el sistema 600 puede incluir cualquier número de terminales de acceso adicionales, similares al terminal de acceso 202 y / o cualquier cantidad de estaciones base adicionales, similares a la estación base 204.

[50] De acuerdo a un ejemplo, el terminal de acceso 202 puede transmitir un mensaje 3 a la estación base 204 como parte de un procedimiento de acceso aleatorio, como se describe en el presente documento. Cuando se emplea acceso aleatorio basado en contienda, el mensaje 3 enviado por el terminal de acceso 202 puede incluir una parte no cifrada (*por ejemplo,* producida por el generador de mensajes no cifrados 208) y una parte cifrada (*por ejemplo,* producida por el generador de mensajes cifrados 210). El terminal de acceso 202 puede incluir un concatenador de mensajes 602 que puede combinar la parte no cifrada proporcionada por el generador de mensajes no cifrados 208 y la parte cifrada proporcionada por el generador de mensajes cifrados 210 para producir el mensaje 3. Además, la parte no cifrada del mensaje 3 generado por el generador de mensajes no cifrados 208 puede incluir un identificador correspondiente al terminal de acceso 202, que puede ser utilizado por el identificador de origen de mensaje 214 para reconocer el terminal de acceso 202 como el origen del mensaje 3. A continuación, el determinador de contexto de seguridad 216 puede reconocer el contexto de seguridad asociado al terminal de acceso 202 basándose en la identidad determinada, y el contexto de seguridad puede emplearse para descifrar la parte cifrada del mensaje 3 (así como uno o más mensajes cifrados posteriores) producida por el generador de mensajes cifrados 210 y enviada por el terminal de acceso 202 a la estación base 204 por el enlace ascendente.

[51] Además, el Control de Enlace de Radio - Modalidad no Confirmada (RLC-UM) y / o el Control de Enlace de Radio - Modalidad Confirmada (RLC-AM) se pueden utilizar en el mensaje 3. El RLCUM no proporciona retro-alimentación desde el lado del receptor, mientras que el RLC-AM usa un acuse de recibo desde el lado del receptor (*por ejemplo,* si no se obtiene un acuse de recibo en el lado del transmisor, entonces el transmisor puede reenviar el(los) paquete(s), ...). Además, el RLC-AM presta soporte a la segmentación como se describe a continuación. Se observa que, a excepción del primer mensaje de RRC en la transición de estado de LTE_REPOSO a LTE_ACTIVO, es posible que el terminal de acceso 202 use el RLC-UM y el RLC-AM en el mensaje 3. Por consiguiente, el terminal de acceso 202 puede usar el RLC en modalidad no transparente para enviar información no crítica para la seguridad, que no está cifrada. Además, el concatenador de mensajes 602 puede concatenar información cifrada dentro del mensaje 3.

[52] Puede complicar el comportamiento de la red si el terminal de acceso 202 usa el RLC-AM antes de que el identificador de origen de mensaje 214 identifique al terminal de acceso 202 como el originador del mensaje 3, debido a que el RLC-AM tiene el contexto para el terminal de acceso 202. Por lo tanto, el terminal de acceso 202 puede usar el RLC-UM con un indicador de longitud especial para el primer mensaje de RRC por este motivo, ya que el RLC-UM proporciona información sobre el tamaño de la Unidad de Datos del Protocolo (PDU) de RLC. Además, se contempla que el RLC-TM se pueda usar si el Control de Acceso al Medio (MAC) proporciona la información de tamaño para la PDU del RLC-TM. Además, el mensaje de RRC normal que sigue puede usar el RLC-AM.

[53] El generador de mensajes cifrados 210 puede incluir además un segmentador 604. Dado que el tamaño del mensaje 3 puede ser limitado, un mensaje cifrado (*por ejemplo,* un mensaje de RRC, ...) producido por el generador de mensajes cifrados 210 puede ser incapaz de encajar en la parte cifrada del mensaje 3. Por lo tanto, el segmentador 604 puede segmentar este mensaje cifrado (*por ejemplo,* un mensaje de RRC, ...) en partes separadas, permitiendo así que el terminal de acceso 202 transfiera una parte del mensaje cifrado en la parte cifrada del mensaje 3 y la parte restante del cifrado mensaje en una transmisión planificada normal.

[54] La estación base 204 puede incluir además una memoria intermedia 606. La memoria intermedia 606 se puede utilizar para retener la parte cifrada del mensaje 3 y en adelante, hasta que la primera parte no cifrada del mensaje 3 se procese en la capa de RRC en la red. Por lo tanto, la capa del Protocolo de convergencia de datos en paquetes (PDCP) en la red puede ser un protocolo de detención y espera, al menos para el mensaje 3. Por lo tanto, lo anterior puede permitir la transmisión del mensaje 3 con el RLC-TM, con reglas sobre lo que el terminal de acceso 202 puede transmitir y sin ningún tratamiento especial para la transmisión de mensajes de RRC para los mensajes de RRC posteriores. Por lo tanto, puede haber una reducción en la latencia del plano de control (plano C).

[55] Además, en caso de acceso aleatorio no basado en contienda, el solicitante de acceso aleatorio 206 puede enviar un preámbulo de acceso aleatorio que permita que el identificador de origen de mensaje 214 (*por ejemplo,* red, ...) identifique el terminal de acceso 202. Por lo tanto, es posible que el terminal de acceso 202 cifre la totalidad del mensaje 3 y que la red use la configuración de seguridad correcta para el mensaje 3. Además, a diferencia del acceso aleatorio basado en contienda, el terminal de acceso 202 no tiene impuesta una restricción específica en cuanto a lo que puede enviar en el mensaje 3 en este escenario.

[56] De acuerdo a un ejemplo, el terminal de acceso 202 puede comportarse de manera diferente según el tipo de procedimiento de acceso aleatorio (*por ejemplo,* basado en contienda contra no basado en contienda); sin embargo, el tema en cuestión reivindicado no está limitado de ese modo. Por ejemplo, cuando la totalidad del mensaje 3 no está cifrada para el acceso aleatorio basado en contienda, según el ejemplo descrito en relación con las Figuras 2, 4 y 5, el envío de información crítica para la seguridad en el mensaje 3 en el acceso aleatorio no basado en contienda puede reducir la latencia del plano C en comparación con el acceso aleatorio basado en la contienda. En tal escenario, permitir que el terminal de acceso 202 implemente diferentes comportamientos en función del tipo de procedimiento de acceso aleatorio puede reducir la latencia para el caso de acceso aleatorio no basado en contienda. Siguiendo el ejemplo donde el mensaje 3 incluye una parte no cifrada y una parte cifrada,

como se describe en la Fig. 6, diferentes comportamientos para el acceso aleatorio basado en contienda y el acceso aleatorio no basado en contienda pueden o no ser utilizados.

[57] Pasando ahora a la **Fig. 7**, se ilustra un ejemplo de diagrama de señalización 700 de un procedimiento de acceso aleatorio que comunica información cifrada y no cifrada en el mensaje 3. El diagrama de señalización 700 representa el uso del acceso aleatorio por un terminal de acceso para volver a entrar a la modalidad sincronizada desde la modalidad no sincronizada. Sin embargo, ha de apreciarse que la señalización similar a la siguiente descripción puede utilizarse junto con el traspaso desde una estación base de origen a una estación base de destino (*por ejemplo,* la señalización descrita en el diagrama 700 puede realizarse entre la estación base de destino y el terminal de acceso al recibir el terminal de acceso un comando de traspaso desde la estación base de origen, como se muestra en la figura 5, ...).

[58] En 702, se puede transmitir un preámbulo de acceso aleatorio desde el terminal de acceso a la estación base de servicio. En 704, la estación base servidora puede transmitir una respuesta de acceso aleatorio al terminal de acceso. En 706, el mensaje 3 puede transmitirse desde el terminal de acceso a la estación base de servicio. El mensaje 3 puede incluir una parte no cifrada y una parte cifrada. La parte no cifrada puede incluir un identificador (*por ejemplo,* C-RNTI, ...) asociado al terminal de acceso, un discriminador de mensajes, un indicador de longitud especial para la parte no cifrada del mensaje 3, y así sucesivamente. Por ejemplo, la parte no cifrada se puede enviar usando el RLCUM. De acuerdo a otra ilustración, la parte no cifrada se puede transmitir usando el RLC-TM. A modo de ejemplo adicional, se puede usar una PDU de la capa de MAC para la parte no cifrada del mensaje 3. Además, un mensaje de RRC, que incluye información crítica para la seguridad, tal como un informe de medición (o una parte del mismo) se puede transmitir en la parte cifrada del mensaje 3. La parte cifrada se puede enviar utilizando el RLC-AM, que da soporte a la segmentación. Por ejemplo, este informe de medición puede segmentarse de modo que una primera parte del informe de medición pueda concatenarse con la parte no cifrada y enviarse como el mensaje 3, mientras que un resto del informe de medición puede enviarse en posterior(es) transmisión(es) de enlace ascendente. En 708, un mensaje de resolución de contienda puede ser transmitido por la estación base de servicio al terminal de acceso. En 710, el terminal de acceso puede enviar una transmisión planificada normal, que está cifrada, a la estación base de servicio. Esta transmisión planificada normal puede incluir el resto del informe de medición. Además, la transmisión planificada normal se puede enviar utilizando el RLC-AM.

[59] Según un ejemplo, la señalización, como se muestra en el diagrama 700, puede utilizarse tanto para el acceso aleatorio basado en contienda como para el acceso aleatorio no basado en contienda (*por ejemplo,* el mensaje 3 puede incluir una parte no cifrada y una parte cifrada tanto para el acceso aleatorio basado en contienda como para el acceso aleatorio no basado en contienda, ...). De acuerdo a otra ilustración, el diagrama de señalización 700 se puede emplear para el acceso aleatorio basado en contienda, mientras que se puede usar una señalización diferente para el acceso aleatorio no basado en contienda. Siguiendo esta ilustración, para el acceso aleatorio no basado en contienda, la totalidad o la mayor parte del mensaje 3 puede cifrarse y / o enviarse usando el RLC-AM en lugar de cifrar y / o usar el RLC-AM solo para una parte del mensaje 3.

[60] Con referencia a las **Figs. 8 a 9**, se ilustran las metodologías relacionadas con la utilización de mensajes cifrados y no cifrados para un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. Si bien, con el fin de simplificar la explicación, las metodologías se muestran y se describen como una serie de actos, ha de entenderse y apreciarse que las metodologías no están limitadas por el orden de los actos, ya que ciertos actos pueden, de acuerdo a uno o más modos de realización, producirse en órdenes diferentes y/o de forma concurrente con otros actos con respecto a los mostrados y descritos en el presente documento. Por ejemplo, los expertos en la materia entenderán y apreciarán que una metodología podría representarse de forma alternativa como una serie de estados o sucesos interrelacionados, tal como en un diagrama de estados. Además, puede que no se requiera que todos los actos ilustrados implementen una metodología de acuerdo a uno o más modos de realización.

[61] Con referencia a la **Fig. 8**, se ilustra una metodología 800 que facilita el empleo de un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. En 802, se puede transmitir un preámbulo de acceso aleatorio a una estación base. Por ejemplo, el preámbulo de acceso aleatorio puede incluir una rúbrica de acceso aleatorio que es utilizado comúnmente por los terminales de acceso en el entorno de comunicación inalámbrica (*por ejemplo,* la rúbrica de acceso aleatorio común se puede usar para el acceso aleatorio basado en contienda, ...). De acuerdo a otra ilustración, el preámbulo de acceso aleatorio puede incluir una rúbrica de acceso aleatorio específica del terminal de acceso (*por ejemplo,* usada para el acceso aleatorio no basado en contienda, ...). El preámbulo de acceso aleatorio se puede enviar a la estación base para comenzar el acceso inicial o la re-entrada desde un estado no sincronizado, por ejemplo. Según otro ejemplo, el preámbulo de acceso aleatorio se puede transmitir a la estación base (*por ejemplo,* la estación base de destino) en respuesta a recibir un comando de traspaso desde una estación base de origen diferente.

[62] En 804, se puede recibir una respuesta de acceso aleatorio desde la estación base, basándose en el preámbulo de acceso aleatorio. La respuesta de acceso aleatorio puede proporcionar una concesión para una posterior transmisión planificada de enlace ascendente.

[63] En 806, un mensaje de transmisión planificada, que incluye al menos una parte que no está cifrada, se puede transmitir a la estación base según lo otorgado por la respuesta de acceso aleatorio cuando se emplea el acceso aleatorio basado en contienda. De acuerdo a una ilustración, la parte no cifrada puede incluir un identificador temporal (*por ejemplo,* el Identificador Temporal de Red de Radio Celular (C-RNTI), ...) del terminal de acceso desde el cual se transmite la transmisión planificada. El identificador temporal puede permitir que la estación base reconozca una identidad del terminal de acceso, determine un contexto de seguridad asociado al terminal de acceso y emplee dicho contexto de seguridad para descifrar la(s) posterior(es) transmisión(es) de enlace ascendente desde el terminal de acceso. Además, la parte no cifrada puede incluir información no crítica para la seguridad (*por ejemplo,* un discriminador de mensajes, ...). Además, se puede recibir un mensaje de resolución de contienda desde la estación base en respuesta al mensaje de transmisión planificada.

[64] De acuerdo a un ejemplo, la totalidad o, esencialmente, la mayor parte del mensaje de transmisión planificada puede no cifrarse cuando se utiliza el acceso aleatorio basado en contienda. Además, este mensaje de transmisión planificada se puede transmitir con el Control de Enlace de Radio - Modalidad Transparente (RLC-TM); sin embargo, el asunto en cuestión reivindicado no está limitado de ese modo. Además, un mensaje posterior normal de transmisión planificada, que está cifrado, se puede enviar a la estación base después de recibir el mensaje de resolución de contienda desde la estación base. Este mensaje posterior normal de transmisión planificada puede incluir información crítica para la seguridad (*por ejemplo,* datos críticos relacionados con un informe de medición de Control de Recursos de Radio (RCR), finalización de traspaso, fallo de traspaso, ...). Además, cuando se emplea acceso aleatorio no basado en contienda según este ejemplo, el mensaje de transmisión planificada puede cifrarse. Por lo tanto, se puede identificar el tipo de procedimiento de acceso aleatorio utilizado y si el mensaje de transmisión planificada, enviado en respuesta a la concesión incluida en la respuesta de acceso aleatorio, está cifrado o no cifrado puede variar en función del tipo de procedimiento de acceso aleatorio identificado.

[65] A modo de otro ejemplo, el mensaje de transmisión planificada puede incluir la parte no cifrada y una parte cifrada cuando se emplea el acceso aleatorio basado en contienda. Por lo tanto, la parte no cifrada y la parte cifrada pueden concatenarse dentro del mensaje de transmisión planificada. Por ejemplo, la parte no cifrada se puede transmitir con Control de Enlace de Radio - Modalidad no Confirmada (RLC-UM) o RLC-TM, mientras que la parte cifrada se puede transmitir con Control de Enlace de Radio - Modalidad Confirmada (RLC-AM). Además, la parte no cifrada puede incluir información no crítica para la seguridad y la parte cifrada puede incluir información crítica para la seguridad (*por ejemplo,* datos críticos relacionados con un informe de medición de Control de Recursos de Radio (RRC), finalización de traspaso, falla de traspaso, ...). La información no crítica para la seguridad, por ejemplo, puede incluir un indicador de longitud especial con el RLC-UM. De acuerdo a otra ilustración, la Unidad de Datos de Protocolo (PDU) de la capa de Control de Acceso Medio (MAC) se puede usar en lugar del RLC-UM. Además, la información crítica para la seguridad incluida en la parte cifrada puede segmentarse de manera que una primera parte se incluya en la parte cifrada del mensaje de transmisión planificada y el resto se incluya en al menos un mensaje posterior normal de transmisión planificada que sea cifrado y enviado a la estación base después de recibir el mensaje de resolución de contienda. Además, siguiendo este ejemplo, se contempla que el uso similar de la parte no cifrada y la parte cifrada para el mensaje de transmisión planificada enviado en respuesta a la concesión incluida en la respuesta de acceso aleatorio se puede emplear cuando se emplea el acceso aleatorio no basado en contienda (*por ejemplo,* un comportamiento similar del terminal de acceso tanto para el acceso aleatorio basado en contienda como para el acceso aleatorio no basado en contienda). Adicional o alternativamente, el acceso aleatorio no basado en contienda puede producir un comportamiento diferente para dicho mensaje de transmisión planificada, por lo cual todo, o esencialmente la mayor parte de, el mensaje de transmisión planificada (*por ejemplo,* el mensaje 3, ...) está cifrado.

[66] Pasando a la **Fig. 9**, se ilustra una metodología 900 que facilita el descifrado de los datos obtenidos durante un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. En 902, se puede recibir un preámbulo de acceso aleatorio desde un terminal de acceso. El preámbulo de acceso aleatorio puede incluir una rúbrica de acceso aleatorio común (*por ejemplo,* para el acceso aleatorio basado en contienda, ...) y, por lo tanto, la identidad del terminal de acceso puede ser incapaz de ser reconocida. Además, para el acceso aleatorio no basado en contienda, el preámbulo de acceso aleatorio puede incluir una rúbrica de acceso aleatorio que sea única para el terminal de acceso a partir del cual se obtuvo el preámbulo de acceso aleatorio. En 904, se puede transmitir una respuesta de acceso aleatorio al terminal de acceso basándose en el preámbulo de acceso aleatorio. En 906, se puede recibir una transmisión planificada, que incluye al menos una parte que no está cifrada, desde el terminal de acceso cuando se utiliza el acceso aleatorio basado en contienda. Por ejemplo, la parte no cifrada puede incluir un identificador del terminal de acceso (*por ejemplo,* el Identificador Temporal de Red de Radio Celular (C-RNTI), ...). A modo de otra ilustración, para el acceso aleatorio no basado en contienda, la transmisión planificada se puede cifrar; sin embargo, el tema en cuestión reivindicado no está limitado de ese modo (*por ejemplo,* se puede emplear un comportamiento similar de terminal de acceso para el acceso aleatorio basado en contienda y el acceso aleatorio no basado en contienda, ...). Además, se puede enviar un mensaje de resolución de contienda al terminal de acceso en respuesta a la transmisión planificada recibida. En 908, se puede reconocer una identidad del terminal de acceso basándose en la información incluida en la parte de la transmisión planificada que no está cifrada cuando se emplea un acceso aleatorio basado en contienda. Además, se puede determinar un contexto de seguridad del terminal de acceso basándose en la identidad reconocida del terminal de acceso. Además, este contexto de seguridad se puede utilizar para descifrar la información cifrada posterior, obtenida desde el terminal de acceso. Por ejemplo, la

información cifrada posterior puede incluirse en una parte cifrada del mensaje de transmisión planificada (así como un posterior mensaje normal de transmisión planificada que está cifrado). Siguiendo este ejemplo, la parte cifrada del mensaje de transmisión planificada (y / o el posterior mensaje normal de transmisión planificada) puede almacenarse temporalmente hasta que se procese la parte no cifrada (*por ejemplo,* para determinar la identidad del terminal de acceso, ...). De acuerdo a otro ejemplo, la información cifrada posterior puede incluirse en un posterior mensaje normal de transmisión planificada.

[67] Se apreciará que, de acuerdo a uno o más aspectos descritos en este documento, se pueden realizar deducciones con respecto al empleo de mensajes de enlace ascendente planificados, cifrados y / o no cifrados, en un procedimiento de acceso aleatorio. Como se usa en el presente documento, el término "deducir" o "deducción" se refiere, en general, al proceso de razonar sobre, o deducir, los estados del sistema, del entorno y/o del usuario a partir de un conjunto de observaciones según lo recopilado *mediante* sucesos y/o datos. La deducción puede emplearse para identificar un contexto o una acción específicos o puede generar una distribución de probabilidades sobre los estados, por ejemplo. La deducción puede ser probabilística, es decir, el cálculo de una distribución de probabilidades sobre los estados de interés basándose en una consideración de datos y sucesos. La deducción puede referirse también a las técnicas empleadas para componer los sucesos de nivel superior a partir de un conjunto de sucesos y/o datos. Dicha deducción da como resultado la construcción de nuevos sucesos o acciones a partir de un conjunto de sucesos observados y/o de datos de sucesos almacenados, independientemente de si están o no correlacionados los sucesos en una proximidad temporal cercana, o de si los sucesos y los datos proceden de una o más fuentes de sucesos y datos.

[68] De acuerdo a un ejemplo, uno o más procedimientos presentados anteriormente pueden incluir hacer deducciones correspondientes a la determinación de un tipo de procedimiento de acceso aleatorio a emplear. A modo de ilustración adicional, puede hacerse una deducción relacionada con la determinación de si se altera la operación de cifrado para el mensaje 3 como una función del tipo de procedimiento de acceso aleatorio que se utiliza. Se apreciará que los ejemplos anteriores son de naturaleza ilustrativa y no pretenden limitar el número de deducciones que pueden hacerse o la manera en la que dichas deducciones se hacen conjuntamente con los diversos modos de realización y/o procedimientos descritos en el presente documento.

[69] La **figura 10** es una ilustración de un terminal de acceso 1000 que transmite mensajes de enlace ascendente planificados, cifrados y / o no cifrados, en un sistema de comunicación inalámbrica. El terminal de acceso 1000 comprende un receptor 1002 que recibe una señal desde, por ejemplo, una antena de recepción (no mostrada), y realiza acciones típicas (*por ejemplo,* filtra, amplifica, disminuye en frecuencia, *etc.*) en la señal recibida y digitaliza la señal acondicionada para obtener muestras. El receptor 1002 puede ser, por ejemplo, un receptor de MMSE y puede comprender un demodulador 1004 que puede demodular los símbolos recibidos y proporcionarlos a un procesador 1006 para la estimación de canal. El procesador 1006 puede ser un procesador dedicado a analizar la información recibida por el receptor 1002 y/o a generar información para su transmisión mediante un transmisor 1016, un procesador que controla uno o más componentes del terminal de acceso 1000 y/o un procesador que tanto analiza información recibida por el receptor 1002, como genera información para su transmisión mediante el transmisor 1016 y controla uno o más componentes del terminal de acceso 1000.

[70] El terminal de acceso 1000 puede comprender además una memoria 1008 que está acoplada de manera operativa al procesador 1006 y que puede almacenar datos a transmitir, datos recibidos y cualquier otra información apropiada relativa a la realización de las diversas acciones y funciones expuestas en el presente documento. Por ejemplo, la memoria 1008 puede almacenar un identificador relacionado con el terminal de acceso 1000, una rúbrica de acceso aleatorio a incluir en un preámbulo de acceso aleatorio, y así sucesivamente. La memoria 1008 puede almacenar adicionalmente protocolos y / o algoritmos asociados a la determinación de un tipo de procedimiento de acceso aleatorio a emplear, la generación de un preámbulo de acceso aleatorio para transmitir a una estación base, la generación de mensajes de enlace ascendente, la concatenación de mensajes cifrados y no cifrados, y similares.

[71] Se apreciará que el almacén de datos (*por ejemplo,* la memoria 1008) descrito en el presente documento puede ser una memoria volátil o una memoria no volátil, o puede incluir tanto una memoria volátil como una memoria no volátil. A modo de ilustración, y no de limitación, la memoria no volátil puede incluir memoria de solo lectura (ROM), ROM programable (PROM), ROM eléctricamente programable (EPROM), PROM eléctricamente borrable (EEPROM) o memoria flash. La memoria volátil puede incluir memoria de acceso aleatorio (RAM), que actúa como memoria caché externa. A modo de ilustración, y no de limitación, la RAM está disponible de muchas formas, tales como RAM síncrona (SRAM), RAM dinámica (DRAM), DRAM síncrona (SDRAM), SDRAM de doble velocidad de datos (DDR SDRAM), SDRAM mejorada (ESDRAM), DRAM de enlace síncrono (SLDRAM) y RAM de Rambus directo (DRRAM). La memoria 1008 de los sistemas y procedimientos de la materia está concebida para comprender, sin limitarse a, estos y otros tipos adecuados de memoria.

[72] El receptor 1002 está además acoplado operativamente a un generador de mensajes no cifrados 1010 y / o a un generador de mensajes cifrados 1012, que puede ser esencialmente similar al generador de mensajes no cifrados 208 de la figura 2 y al generador de mensajes cifrados 210 de la figura 2, respectivamente. El generador de mensajes no cifrados 1010 y / o el generador de mensajes cifrados 1012 pueden producir un mensaje 3 para su transmisión por un enlace ascendente a una estación base. Por ejemplo, el terminal de acceso 1000 puede

transmitir un preámbulo de acceso aleatorio y recibir una respuesta de acceso aleatorio basada en eso. Cuando se emplea acceso aleatorio basado en contienda, el generador de mensajes no cifrados 1010 puede producir al menos una parte del mensaje 3 para su transmisión por el enlace ascendente, y esta parte no está cifrada. De acuerdo a un ejemplo, el mensaje 3 puede ser generado por el generador de mensajes no cifrados 1010 y, por lo tanto, puede estar no cifrado. De acuerdo a otra ilustración, el generador de mensajes no cifrados 1010 puede generar la parte no cifrada del mensaje 3, mientras que el generador de mensajes cifrados 1012 puede producir una parte cifrada del mensaje 3. Además, el generador de mensajes cifrados 1012 puede proporcionar un posterior mensaje normal de transmisión planificada de enlace ascendente. Además, el generador de mensajes no cifrados 1010 puede incluir información no crítica para la seguridad tal como, por ejemplo, un identificador relacionado con el terminal de acceso 1000, un discriminador de mensajes, *etc.*, en los mensajes no cifrados, mientras que el generador de mensajes cifrados 1012 puede incluir información crítica para la seguridad en mensajes cifrados. El terminal de acceso 1000 aún comprende adicionalmente un modulador 1014 y un transmisor 1016 que transmite la señal, por ejemplo, a una estación base, otro terminal de acceso, *etc.* Aunque se han representado como independientes del procesador 1006, ha de apreciarse que el generador de mensajes no cifrados 1010, el generador de mensajes cifrados 1012 y/o el modulador 1014 pueden ser parte del procesador 1006 o de varios procesadores (no mostrados).

[73] La **figura 11** es una ilustración de un sistema 1100 que evalúa mensajes planificados, no cifrados y cifrados, recibidos por un enlace ascendente durante un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. El sistema 1100 comprende una estación base 1102 (*por ejemplo,* un punto de acceso, …) con un receptor 1110 que recibe una o más señales desde uno o más terminales de acceso 1104 a través de una pluralidad de antenas de recepción 1106, y un transmisor 1122 que transmite a los uno o más terminales de acceso 1104 a través de una antena de transmisión 1108. El receptor 1110 puede recibir información desde las antenas receptoras 1106 y está asociado de forma operativa a un demodulador 1112 que demodula la información recibida. Los símbolos demodulados son analizados por un procesador 1114 que puede ser similar al procesador descrito anteriormente con respecto a la **Fig. 10**, y que está acoplado a una memoria 1116 que almacena datos a transmitir a, o a recibir desde, el terminal o terminales de acceso 1104 (o una estación base diferente (no mostrada)), y/o cualquier otra información adecuada relacionada con la ejecución de las diversas acciones y funciones expuestas en el presente documento. El procesador 1114 está además acoplado a un identificador de origen de mensaje 1118 que evalúa un mensaje recibido 3, que incluye al menos una parte no cifrada, desde uno o más terminales de acceso 1104 para reconocer una identidad de ese terminal de acceso particular. Tal mensaje 3 puede recibirse cuando el terminal de acceso particular emplea un acceso aleatorio basado en contienda; sin embargo, el tema en cuestión reivindicado no está limitado de ese modo. El identificador de origen de mensaje 1118 puede estar acoplado operativamente a un determinador de contexto de seguridad 1120 que descifra un contexto de seguridad correspondiente al terminal de acceso particular identificado, del cual se obtuvo el mensaje 3. Además, el contexto de seguridad según lo identificado puede emplearse para descifrar posteriores transmisiones planificadas cifradas de enlace ascendente. Se contempla que el identificador de origen de mensaje 1118 puede ser esencialmente similar al identificador de origen de mensaje 214 de la figura 2 y / o que el determinador de contexto de seguridad 1120 puede ser esencialmente similar al determinador de contexto de seguridad 216 de la figura 2. Además, el identificador de origen de mensaje 1118 y / o el determinador de contexto de seguridad 1120 pueden proporcionar información a transmitir a un modulador 1122. El modulador 1122 puede multiplexar una trama para su transmisión, mediante un transmisor 1126 a través de las antenas 1108, al terminal o terminales de acceso 1104. Aunque se representa como independiente del procesador 1114, ha de apreciarse que el identificador de origen de mensaje 1118, el determinador de contexto de seguridad 1120 y / o el modulador 1122 pueden ser parte del procesador 1114 o de una serie de procesadores (no mostrados).

[74] La **Fig. 12** muestra un sistema de comunicación inalámbrica 1200 ejemplar. El sistema de comunicación inalámbrica 1200 representa una estación base 1210 y un terminal de acceso 1250, con fines de brevedad. Sin embargo, ha de apreciarse que el sistema 1200 puede incluir más de una estación base y/o más de un terminal de acceso, en donde las estaciones base y/o los terminales de acceso adicionales pueden ser esencialmente similares o diferentes a la estación base 1210 ejemplar y al terminal de acceso 1250 que se describen a continuación. Además, ha de apreciarse que la estación base 1210 y/o el terminal de acceso 1250 pueden emplear los sistemas (**Figuras 1, 2, 6, 10 a 11** y **13 a 14**) y / o los procedimientos (**Figuras 8 a 9**) descritos en el presente documento para facilitar la comunicación inalámbrica entre los mismos.

[75] En la estación base 1210, los datos de tráfico para una serie de flujos de datos se proporcionan desde un origen de datos 1212 a un procesador de datos de transmisión (TX) 1214. De acuerdo a un ejemplo, cada flujo de datos puede transmitirse a través de una respectiva antena. El procesador de datos de TX 1214 formatea, codifica e intercala el flujo de datos de tráfico basándose en un esquema de codificación particular seleccionado para que ese flujo de datos proporcione datos codificados.

[76] Los datos codificados para cada flujo de datos pueden multiplexarse con datos piloto usando técnicas de multiplexado por división ortogonal de frecuencia (OFDM). Adicionalmente, o de forma alternativa, los símbolos piloto pueden multiplexarse por división de frecuencia (FDM), multiplexarse por división del tiempo (TDM) o multiplexarse por división de código (CDM). Los datos piloto son habitualmente un patrón de datos conocidos que se procesa de manera conocida y que puede usarse en el terminal de acceso 1250 para estimar la respuesta de canal. Los datos piloto multiplexados y los datos codificados para cada flujo de datos pueden modularse (*por ejemplo,* correlacionarse

con símbolos) en función de un sistema de modulación particular (*por ejemplo*, modulación por desplazamiento de fase binaria (BPSK), modulación por desplazamiento de fase en cuadratura (QPSK), modulación por desplazamiento de fase M (M-PSK), modulación de amplitud en cuadratura M (M-QAM), *etc*.) seleccionado para que ese flujo de datos proporcione símbolos de modulación. La velocidad de transferencia de datos, la codificación y la modulación de cada flujo de datos pueden determinarse mediante instrucciones realizadas o proporcionadas por un procesador 1230.

[77] Los símbolos de modulación para los flujos de datos pueden proporcionarse a un procesador de MIMO de TX 1220, que puede procesar además los símbolos de modulación (*por ejemplo,* para el OFDM). El procesador de MIMO de TX 1220 proporciona entonces N_T flujos de símbolos de modulación a N_T transmisores (TMTR) 1222a a 1222t. En diversos modos de realización, el procesador de MIMO de TX 1220 aplica ponderaciones de formación de haces a los símbolos de los flujos de datos y a la antena desde la cual está transmitiéndose el símbolo.

[78] Cada transmisor 1222 recibe y procesa un flujo de símbolos respectivo para proporcionar una o más señales analógicas, y acondiciona adicionalmente (*por ejemplo*, amplifica, filtra y aumenta en frecuencia) las señales analógicas para proporcionar una señal modulada adecuada para su transmisión por el canal de MIMO. Además, N_T señales moduladas desde los transmisores 1222a a 1222t se transmiten desde las N_T antenas 1224a a 1224t, respectivamente.

[79] En el terminal de acceso 1250, las señales moduladas transmitidas son recibidas por las N_R antenas 1252a a 1252r y la señal recibida desde cada antena 1252 se proporciona a un receptor respectivo (RCVR) 1254a a 1254r. Cada receptor 1254 acondiciona (*por ejemplo,* filtra, amplifica y reduce en frecuencia) una señal respectiva, digitaliza la señal acondicionada para proporcionar muestras y procesa adicionalmente las muestras para proporcionar un correspondiente flujo de símbolos "recibidos".

[80] Un procesador de datos de RX 1260 puede recibir y procesar los N_R flujos de símbolos recibidos desde los N_R receptores 1254 basándose en una técnica particular de procesamiento de receptor para proporcionar N_T flujos de símbolos "detectados". El procesador de datos de RX 1260 puede demodular, desintercalar y decodificar cada flujo de símbolos detectado para recuperar los datos de tráfico para el flujo de datos. El procesamiento mediante el procesador de datos de RX 1260 es complementario al realizado por el procesador de MIMO de TX 1220 y por el procesador de datos de TX 1214 en la estación base 1210.

[81] Un procesador 1270 puede determinar de forma periódica qué tecnología disponible utilizar, como se ha expuesto anteriormente. Además, el procesador 1270 puede formular un mensaje de enlace inverso que comprenda una parte de índice matricial y una parte de valor de rango.

[82] El mensaje de enlace inverso puede comprender diversos tipos de información respecto al enlace de comunicación y/o al flujo de datos recibido. El mensaje de enlace inverso puede ser procesado por un procesador de datos de TX 1238, que también recibe datos de tráfico para una serie de flujos de datos desde un origen de datos 1236, modulado por un modulador 1280, acondicionado por los transmisores 1254a a 1254r y transmitido de vuelta a la estación base 1210.

[83] En la estación base 1210, las señales moduladas del terminal de acceso 1250 son recibidas mediante las antenas 1224, acondicionadas mediante los receptores 1222, demoduladas mediante un demodulador 1240 y procesadas mediante un procesador de datos de RX 1242 para extraer el mensaje de enlace inverso transmitido por el terminal de acceso 1250. Además, el procesador 1230 puede procesar el mensaje extraído para determinar qué matriz de precodificación usar para determinar las ponderaciones de conformación de haces.

[84] Los procesadores 1230 y 1270 pueden dirigir (*por ejemplo*, controlar, coordinar, gestionar, *etc.)* el funcionamiento de la estación base 1210 y del terminal de acceso 1250, respectivamente. Los respectivos procesadores 1230 y 1270 pueden asociarse con las memorias 1232 y 1272 que almacenan códigos de programa y datos. Los procesadores 1230 y 1270 también pueden realizar cálculos para obtener las estimaciones de respuesta de frecuencia y de impulso para el enlace ascendente y el enlace descendente, respectivamente.

[85] En un aspecto, los canales lógicos se clasifican en canales de control y canales de tráfico. Los canales de control lógico pueden incluir un canal de control de difusión (BCCH), que es un canal de enlace descendente para difundir información de control del sistema. Además, los canales de control lógico pueden incluir un canal de control de paginación (PCCH), que es un canal de enlace descendente que transmite información de paginación. Además, los canales de control lógico pueden comprender un canal de control de multidifusión (MCCH), que es un canal de enlace descendente de punto a multi-punto, utilizado para la transmisión de la información de planificación y control del servicio de difusión y multi-difusión de multimedios (MBMS) para uno o varios MTCH. Por lo general, después de establecer una conexión de control de recursos de radio (RRC), este canal es utilizado únicamente por los UE que reciben el MBMS (*por ejemplo,* los antiguos MCCH+MSCH). Adicionalmente, los canales de control lógicos pueden incluir un canal de control dedicado (DCCH), que es un canal bidireccional de punto a punto que transmite información de control dedicada y que puede ser utilizada por los UE que tienen una conexión de RRC. En un aspecto, los canales lógicos de tráfico pueden comprender un canal de tráfico dedicado (DTCH), que es un canal

bidireccional de punto a punto dedicado a un UE para la transferencia de información de usuario. Además, los canales lógicos de tráfico pueden incluir un canal de tráfico de multidifusión (MTCH) para el canal de enlace descendente de punto a multi-punto, para transmitir datos de tráfico.

[86] En un aspecto, los canales de transporte se clasifican en enlace descendente y enlace ascendente. Los canales de transporte de enlace descendente comprenden un canal de difusión (BCH), un canal compartido de datos de enlace descendente (DL-SDCH) y un canal de paginación (PCH). El PCH puede prestar soporte al ahorro de energía del UE (*por ejemplo,* la red puede indicar al UE un ciclo de recepción discontinua (DRX), ...) mediante su difusión sobre una célula completa y su correlación con recursos de la capa física (PHY) que pueden ser usados para otros canales de control/tráfico. Los canales de transporte de enlace ascendente pueden comprender un canal de acceso aleatorio (RACH), un canal de petición (REQCH), un canal compartido de datos de enlace ascendente (UL-SDCH) y una pluralidad de canales PHY.

[87] Los canales PHY pueden incluir un conjunto de canales de enlace descendente y canales de enlace ascendente. Por ejemplo, los canales PHY de enlace descendente pueden incluir: Canal piloto común (CPICH); Canal de Sincronización (SCH); Canal de Control Común (CCCH); Canal Compartido de Control de Enlace Descendente (SDCCH); Canal de control de multidifusión (MCCH); Canal compartido de Asignación de Enlace Ascendente (SUACH); Canal de confirmación (ACKCH); Canal Físico Compartido de Datos de Enlace Descendente (DL-PSDCH); Canal de Control de Potencia de Enlace Ascendente (UPCCH); Canal Indicador de Paginación (PICH); y/o Canal Indicador de Carga (LICH). A modo de ilustración adicional, los canales PHY de enlace ascendente pueden incluir: Canal Físico de Acceso Aleatorio (PRACH); Canal Indicador de Calidad de Canal (CQICH); Canal de Confirmación (ACKCH); Canal Indicador de Subconjuntos de Antenas (ASICH); Canal compartido de solicitud (SREQCH); Canal Físico Compartido de Datos de Enlace Ascendente (ULPSDCH); y/o Canal Piloto de Banda Ancha (BPICH).

[88] Se entenderá que los modos de realización descritos en el presente documento pueden implementarse en hardware, software, firmware, middleware, microcódigo o en cualquier combinación de los mismos. Para una implementación de hardware, las unidades de procesamiento pueden implementarse dentro de uno o más circuitos integrados específicos de la aplicación (ASIC), procesadores de señales digitales (DSP), dispositivos de procesamiento de señales digitales (DSPD), dispositivos lógicos programables (PLD), formaciones de compuertas programables en el terreno (FPGA), procesadores, controladores, micro-controladores, microprocesadores, otras unidades electrónicas diseñadas para realizar las funciones descritas en el presente documento o una combinación de los mismos.

[89] Cuando los modos de realización se implementen en software, firmware, middleware o microcódigo, código de programa o segmentos de código, pueden almacenarse en un medio legible por máquina, tal como un componente de almacenamiento. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o instrucciones de programa. Un segmento de código puede acoplarse a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. La información, los argumentos, los parámetros, los datos, *etc.*, pueden pasarse, reenviarse o transmitirse usando cualquier medio adecuado, incluyendo el uso compartido de la memoria, la transferencia de mensajes, la transferencia de testigos, la transmisión en red, *etc.*

[90] Para una implementación de software, las técnicas descritas en el presente documento pueden implementarse con módulos (*por ejemplo,* procedimientos, funciones, etcétera) que realicen las funciones descritas en el presente documento. Los códigos de software pueden almacenarse en unidades de memoria y ejecutarse mediante procesadores. La unidad de memoria puede implementarse dentro del procesador o ser externa al procesador, en cuyo caso puede acoplarse de forma comunicativa al procesador mediante diversos medios, según lo conocido en la técnica.

[91] Con referencia a la **Fig. 13**, se ilustra un sistema 1300 que permite utilizar un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. Por ejemplo, el sistema 1300 puede residir dentro de un terminal de acceso. Debe apreciarse que el sistema 1300 se representa incluyendo bloques funcionales, que pueden ser bloques funcionales que representan funciones implementadas por un procesador, software o una combinación de los mismos (*por ejemplo*, firmware). El sistema 1300 incluye una agrupación lógica 1302 de componentes eléctricos que pueden actuar en conjunto. Por ejemplo, la agrupación lógica 1302 puede incluir un componente eléctrico para enviar un preámbulo de acceso aleatorio que incluye una rúbrica común de acceso aleatorio a una estación base cuando se emplea el acceso aleatorio basado en contienda 1304. Además, aunque no se muestra, la agrupación lógica 1302 puede incluir un componente eléctrico para enviar un preámbulo de acceso aleatorio que incluye una rúbrica de acceso aleatorio específica de terminal de acceso a la estación base cuando se emplea un acceso aleatorio no basado en contienda. Además, la agrupación lógica 1302 puede incluir un componente eléctrico para obtener una respuesta de acceso aleatorio desde la estación base basándose en el preámbulo de acceso aleatorio 1306. Además, la agrupación lógica 1302 puede incluir un componente eléctrico para enviar una transmisión planificada, que incluye al menos una parte no cifrada, a la estación base, según lo concedido por la respuesta de acceso aleatorio cuando se emplea el acceso aleatorio basado en contienda 1308. Por ejemplo, tanto

la parte no cifrada como una parte cifrada se pueden enviar como parte de la transmisión planificada. A modo de otra ilustración, la transmisión planificada puede estar no cifrada y una posterior transmisión planificada normal puede estar cifrada. Adicionalmente, el sistema 1300 puede incluir una memoria 1310 que retiene instrucciones para ejecutar funciones asociadas a los componentes eléctricos 1304, 1306 y 1308. Aunque se muestran como externos a la memoria 1310, se entenderá que uno o más de los componentes eléctricos 1304, 1306 y 1308 pueden existir dentro de la memoria 1310.

[92] Pasando a la **figura 14**, se ilustra un sistema 1400 que permite emplear un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica. El sistema 1400 puede residir, al menos parcialmente, dentro de una estación base, por ejemplo. Como se representa, el sistema 1400 incluye bloques funcionales que pueden representar funciones implementadas por un procesador, un software o una combinación de los mismos (*por ejemplo,* firmware). El sistema 1400 incluye una agrupación lógica 1402 de componentes eléctricos que pueden actuar en conjunto. La agrupación lógica 1402 puede incluir un componente eléctrico para obtener un mensaje de transmisión planificada que incluye al menos una parte no cifrada desde el terminal de acceso cuando se utiliza el acceso aleatorio basado en contienda 1404. Además, la agrupación lógica 1402 puede incluir un componente eléctrico para reconocer una identidad del terminal de acceso basándose en la información incluida en la parte no cifrada del mensaje de transmisión planificada 1406. Por ejemplo, la parte no cifrada del mensaje de transmisión planificada puede incluir un identificador relacionado con el terminal de acceso. Además, la agrupación lógica 1402 puede incluir un componente eléctrico para recuperar un contexto de seguridad asociado al terminal de acceso basándose en la identidad reconocida del terminal de acceso 1408. Además, la agrupación lógica 1402 puede incluir un componente eléctrico para descifrar un mensaje normal cifrado de transmisión planificada o una parte cifrada del mensaje de transmisión planificada que incluye la parte no cifrada recibida desde el terminal de acceso basándose en el contexto de seguridad recuperado 1410. Adicionalmente, el sistema 1400 puede incluir una memoria 1412 que retiene instrucciones para ejecutar funciones asociadas a los componentes eléctricos 1404, 1406 1408 y 1410. Aunque se muestran como externos a la memoria 1412, ha de comprenderse que los componentes eléctricos 1404, 1406, 1408 y 1410 pueden existir dentro de la memoria 1412.

[93] Lo que se ha descrito anteriormente incluye ejemplos de uno o más modos de realización. Por supuesto, no es posible describir toda combinación concebible de componentes o metodologías con fines de describir los modos de realización mencionados anteriormente, pero uno medianamente experto en la materia puede reconocer que son posibles muchas otras combinaciones y permutaciones de diversos modos de realización. Por consiguiente, los modos de realización descritos están concebidos para abarcar todas dichas alteraciones, modificaciones y variaciones que entren dentro del alcance de las reivindicaciones adjuntas. Además, en la medida en que se usa el término “incluye” en la descripción detallada o en las reivindicaciones, dicho término está concebido para ser inclusivo, de manera similar al término “que comprende” según se interprete “que comprende” cuando se emplee como una palabra de transición en una reivindicación.

REIVINDICACIONES

1. Un procedimiento que facilita el empleo de un proceso de acceso aleatorio en un entorno de comunicación inalámbrica, que comprende:

transmitir (802) un preámbulo de acceso aleatorio a una estación base;

recibir (804) una respuesta de acceso aleatorio desde la estación base basándose en el preámbulo de acceso aleatorio; y

transmitir (806) un mensaje de transmisión planificada (706), **caracterizado por que** incluye al menos una parte que no está cifrada, a la estación base según lo concedido por la respuesta de acceso aleatorio cuando se emplea un acceso aleatorio basado en contienda.

2. El procedimiento de la reivindicación 1,

que comprende además la transmisión del preámbulo de acceso aleatorio para al menos uno entre acceso inicial, re-entrada desde un estado no sincronizado o traspaso desde una estación base de origen a la estación base,

o en el que la parte del mensaje de transmisión planificada que no está cifrada incluye información no crítica para la seguridad y un identificador temporal específico del terminal de acceso que permite que la estación base reconozca un origen del preámbulo de acceso aleatorio y el mensaje de transmisión planificada.

3. El procedimiento de la reivindicación 1, que comprende además recibir un mensaje de resolución de contienda desde la estación base en respuesta al mensaje de transmisión planificada.

4. El procedimiento de la reivindicación 3, en el que todo, o una parte de, el mensaje de transmisión planificada no está cifrado cuando se utiliza el acceso aleatorio basado en contienda.

5. El procedimiento de la reivindicación 4,

que comprende además la transmisión del mensaje de transmisión planificada que no está cifrado con el Control de Enlace de Radio - Modalidad Transparente, RLC-TM,

o que comprende además la transmisión de un posterior mensaje de transmisión normal cifrado en respuesta al mensaje de resolución de contienda recibido, el posterior mensaje de transmisión normal cifrado incluye información crítica para la seguridad,

o que comprende además transmitir el mensaje de transmisión planificada como un mensaje cifrado cuando se emplea un acceso aleatorio no basado en contienda,

o que comprende adicionalmente: identificar un tipo de procedimiento de acceso aleatorio empleado; y determinar si se cifra o no el mensaje de transmisión planificada, en función del tipo identificado de procedimiento de acceso aleatorio.

6. El procedimiento de la reivindicación 3, que comprende además concatenar la parte no cifrada con una parte cifrada dentro del mensaje de transmisión planificada.

7. El procedimiento de la reivindicación 6, que comprende además: transmitir la parte no cifrada del mensaje de transmisión planificada con al menos uno entre el Control de enlace de radio - Modalidad no confirmada (RLC - UM) y el Control de enlace de radio - Modalidad transparente (RLC - TM); y transmitir la parte cifrada del mensaje de transmisión planificada con el Control de Enlace de Radio - Modalidad confirmada, RLC-AM.

8. El procedimiento de la reivindicación 6,

en el que la parte no cifrada del mensaje de transmisión planificada incluye información no crítica para la seguridad que incluye un identificador temporal específico del terminal de acceso y la parte cifrada del mensaje de transmisión planificada incluye información crítica para la seguridad,

en particular, que comprende además: segmentar la información crítica para la seguridad en al menos dos partes; incorporar una primera parte de la información crítica para la seguridad en la parte cifrada del mensaje de transmisión planificada; e incorporar al menos una parte del resto de la información crítica para la seguridad en un posterior mensaje normal cifrado de transmisión planificada, enviado a la estación base después de recibir el mensaje de resolución de contienda.

9. El procedimiento de la reivindicación 6, en el que la parte no cifrada usa una Unidad de datos de protocolo, PDU, de la capa de control de acceso al medio, MAC, o que comprende además emplear la parte no cifrada y la parte cifrada del mensaje de transmisión planificada cuando se usa el acceso aleatorio no basado en contienda, o que comprende además transmitir el mensaje de transmisión planificada como un mensaje cifrado cuando se usa el acceso aleatorio no basado en contienda.

10. Un aparato de comunicaciones inalámbricas que permite utilizar un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica, que comprende:

medios para enviar un preámbulo de acceso aleatorio, que incluye una rúbrica común de acceso aleatorio, a una estación base cuando se utiliza el acceso aleatorio basado en contienda;

medios para obtener una respuesta de acceso aleatorio desde la estación base basándose en el preámbulo de acceso aleatorio; y

medios para enviar una transmisión planificada, **caracterizada por** incluir al menos una parte no cifrada, a la estación base según lo concedido por la respuesta de acceso aleatorio cuando se emplea el acceso aleatorio basado en contienda.

11. El aparato inalámbrico de la reivindicación 10, en el que el aparato inalámbrico está adaptado para transmitir el preámbulo de acceso aleatorio para al menos uno entre el acceso inicial, el reingreso desde un estado no sincronizado y el traspaso desde una estación base de origen a la estación base;

o en el que la parte del mensaje de transmisión planificada que no está cifrada incluye información no crítica para la seguridad y un identificador temporal específico del terminal de acceso que permite que la estación base reconozca un origen del preámbulo de acceso aleatorio y el mensaje de transmisión planificada.

12. Un procedimiento que facilita el descifrado de datos obtenidos durante un proceso de acceso aleatorio en un entorno de comunicación inalámbrica, que comprende:

recibir (902) un preámbulo de acceso aleatorio desde un terminal de acceso;

transmitir (904) una respuesta de acceso aleatorio al terminal de acceso basándose en el preámbulo de acceso aleatorio;

recibir (906) un mensaje de transmisión planificada (706), **caracterizado por que** incluye al menos una parte que no está cifrada, desde el terminal de acceso cuando se utiliza el acceso aleatorio basado en contienda; y

reconocer (908) una identidad del terminal de acceso basándose en la información incluida en la parte del mensaje de transmisión planificada que no está cifrada cuando se utiliza el acceso aleatorio basado en contienda.

13. El procedimiento de la reivindicación 12,

en el que la parte del mensaje de transmisión planificada que no está cifrada incluye un Identificador Temporal de Red de Radio Celular, C-RNTI,

o que comprende además recibir el mensaje de transmisión planificada como un mensaje cifrado cuando se utiliza el acceso aleatorio no basado en contienda.

14. El procedimiento de la reivindicación 12, que comprende además determinar un contexto de seguridad asociado al terminal de acceso basándose en la identidad reconocida del terminal de acceso.

15. El procedimiento de la reivindicación 14, que comprende además descifrar la información cifrada posterior, obtenida del terminal de acceso utilizando el contexto de seguridad determinado.

16. El procedimiento de la reivindicación 15,

que comprende además recibir la información cifrada posterior como una parte cifrada del mensaje de transmisión planificada que acompaña a la parte no cifrada,

en particular, que comprende además almacenar temporalmente la parte cifrada del mensaje de transmisión planificada hasta que se procese la parte no cifrada del mensaje de transmisión planificada;

o el procedimiento de la reivindicación 15, que comprende además recibir la información cifrada posterior como un posterior mensaje normal cifrado de transmisión planificada, obtenido en respuesta al envío de un mensaje de resolución de contienda al terminal de acceso.

17. Un aparato de comunicaciones inalámbricas que permite el empleo de un procedimiento de acceso aleatorio en un entorno de comunicación inalámbrica, que comprende:

medios para obtener un mensaje de transmisión planificada **caracterizado por** incluir al menos una parte no cifrada desde el terminal de acceso cuando se emplea un acceso aleatorio basado en contienda;

medios para reconocer una identidad del terminal de acceso basándose en la información incluida en la parte no cifrada del mensaje de transmisión planificada;

medios para recuperar un contexto de seguridad asociado al terminal de acceso basándose en la identidad reconocida del terminal de acceso; y medios para descifrar un mensaje normal cifrado de transmisión planificada o una parte cifrada del mensaje de transmisión planificada que incluye la parte no cifrada recibida desde el terminal de acceso basándose en el contexto de seguridad recuperado.

18. Un producto de programa informático, que comprende: un medio legible por ordenador, que comprende: código para realizar un procedimiento de acuerdo a una de las reivindicaciones 1 a 9 o 12 a 16 cuando se ejecuta en al menos un ordenador.

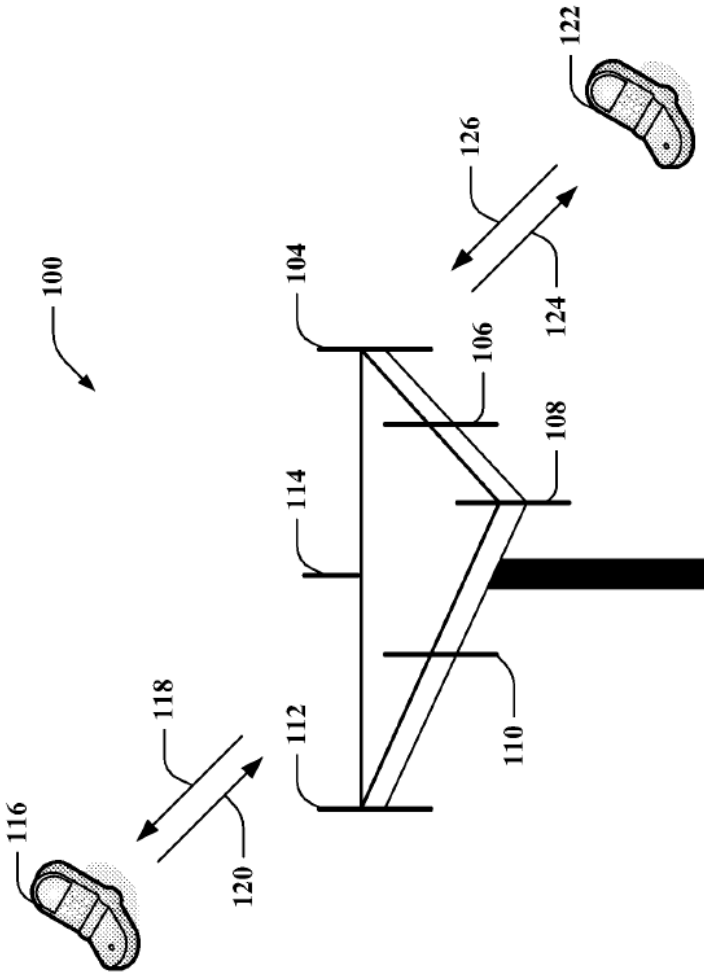

FIG. 1

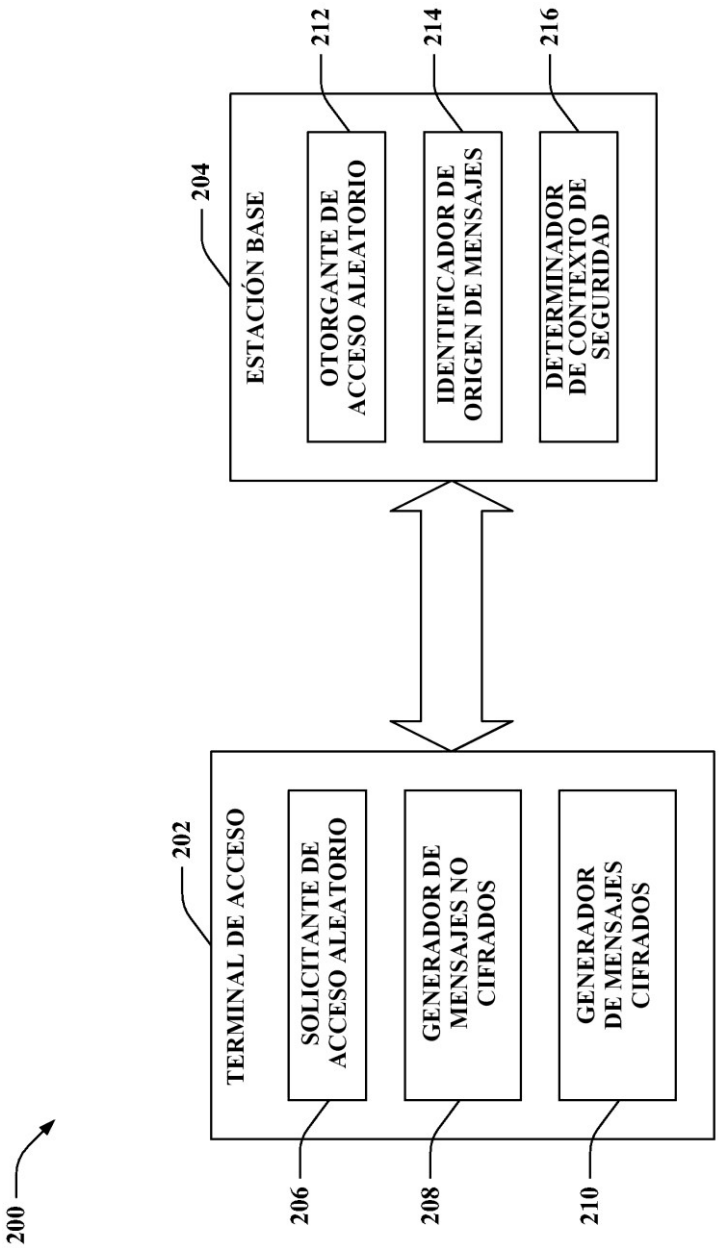
200
202
TERMINAL DE ACCESO
SOLICITANTE DE ACCESO ALEATORIO
GENERADOR DE MENSAJES NO CIFRADOS
GENERADOR DE MENSAJES CIFRADOS
206
208
210
204
ESTACIÓN BASE
OTORGANTE DE ACCESO ALEATORIO
IDENTIFICADOR DE ORIGEN DE MENSAJES
DETERMINADOR DE CONTEXTO DE SEGURIDAD
212
214
216

FIG. 2

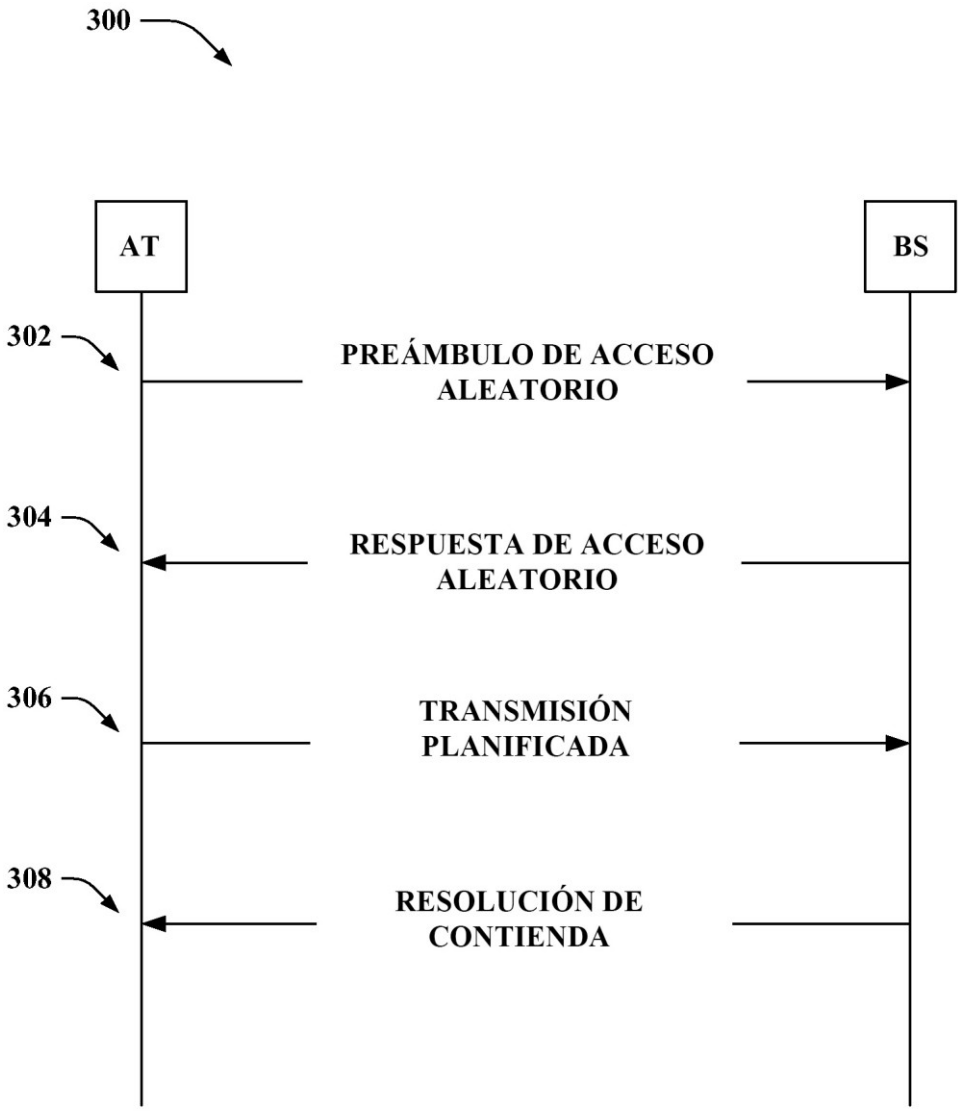
300
AT
BS
302
PREÁMBULO DE ACCESO ALEATORIO
304
RESPUESTA DE ACCESO ALEATORIO
306
TRANSMISIÓN PLANIFICADA
308
RESOLUCIÓN DE CONTIENDA

FIG. 3

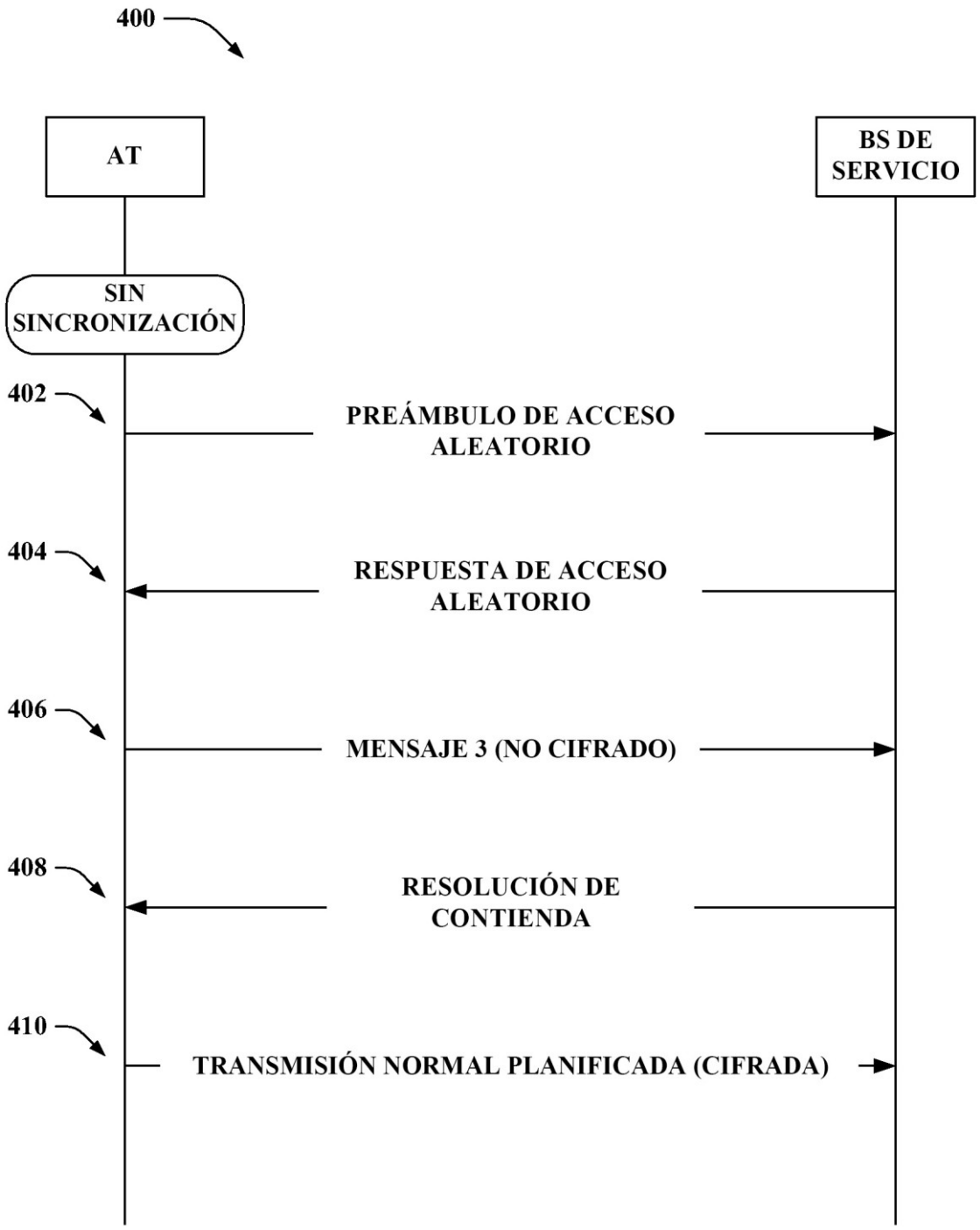
400
AT
BS DE SERVICIO
SIN SINCRONIZACIÓN
402
PREÁMBULO DE ACCESO ALEATORIO
404
RESPUESTA DE ACCESO ALEATORIO
406
MENSAJE 3 (NO CIFRADO)
408
RESOLUCIÓN DE CONTIENDA
410
TRANSMISIÓN NORMAL PLANIFICADA (CIFRADA)

FIG. 4

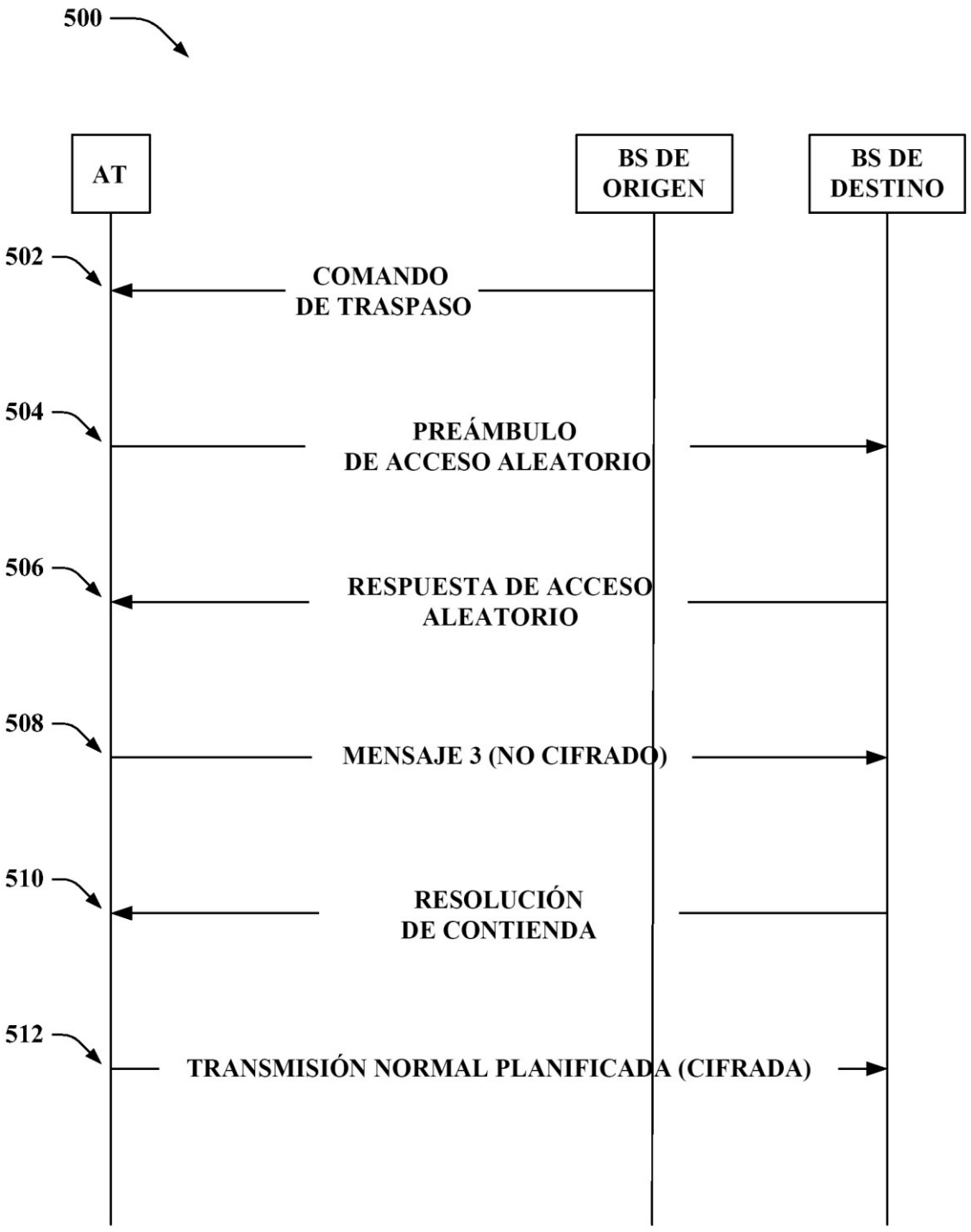
500
AT
BS DE ORIGEN
BS DE DESTINO
502
COMANDO DE TRASPASO
504
PREÁMBULO DE ACCESO ALEATORIO
506
RESPUESTA DE ACCESO ALEATORIO
508
MENSAJE 3 (NO CIFRADO)
510
RESOLUCIÓN DE CONTIENDA
512
TRANSMISIÓN NORMAL PLANIFICADA (CIFRADA)

FIG. 5

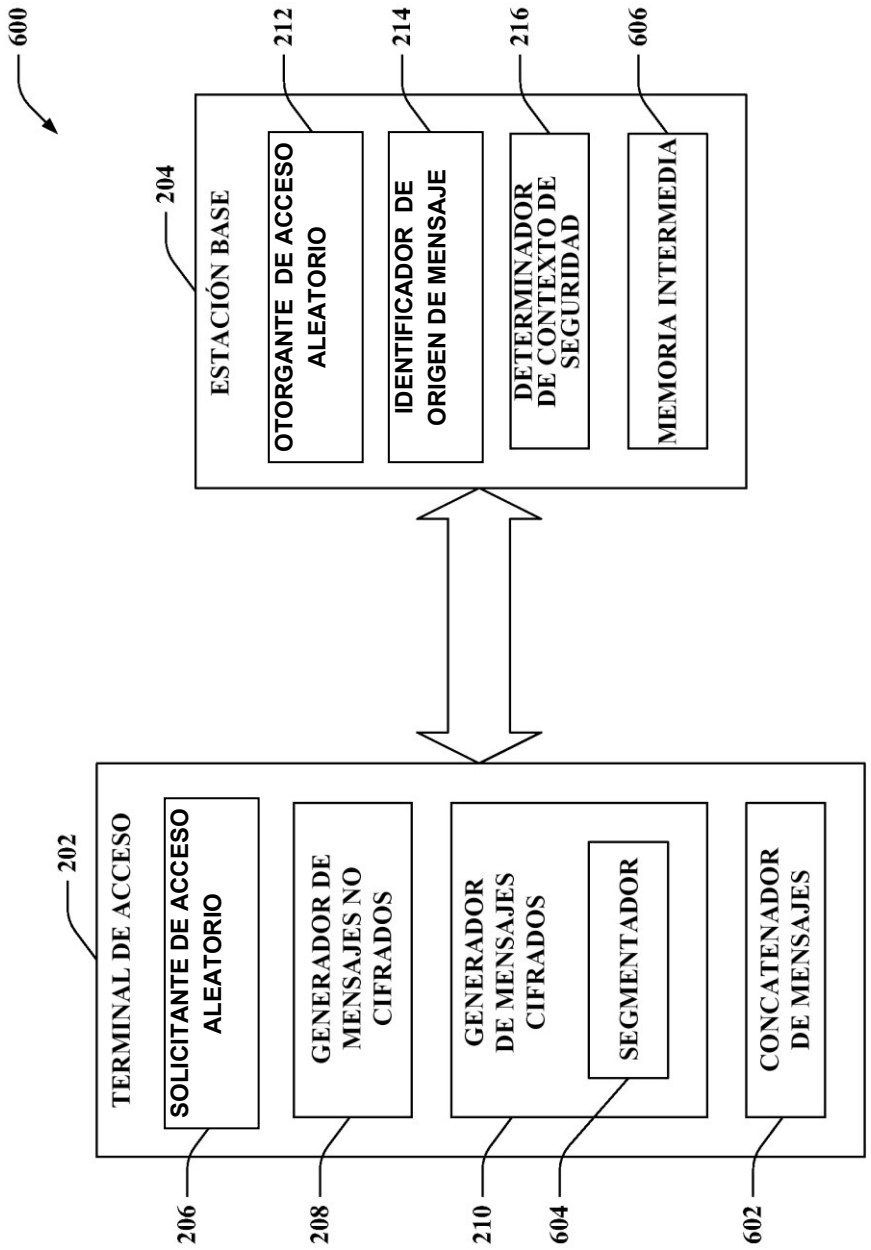
600
212
214
216
606
204
ESTACIÓN BASE
OTORGANTE DE ACCESO ALEATORIO
IDENTIFICADOR DE ORIGEN DE MENSAJE
DETERMINADOR DE CONTEXTO DE SEGURIDAD
MEMORIA INTERMEDIA
202
TERMINAL DE ACCESO
SOLICITANTE DE ACCESO ALEATORIO
GENERADOR DE MENSAJES NO CIFRADOS
GENERADOR DE MENSAJES CIFRADOS
SEGMENTADOR
CONCATENADOR DE MENSAJES
206
208
210
604
602

FIG. 6

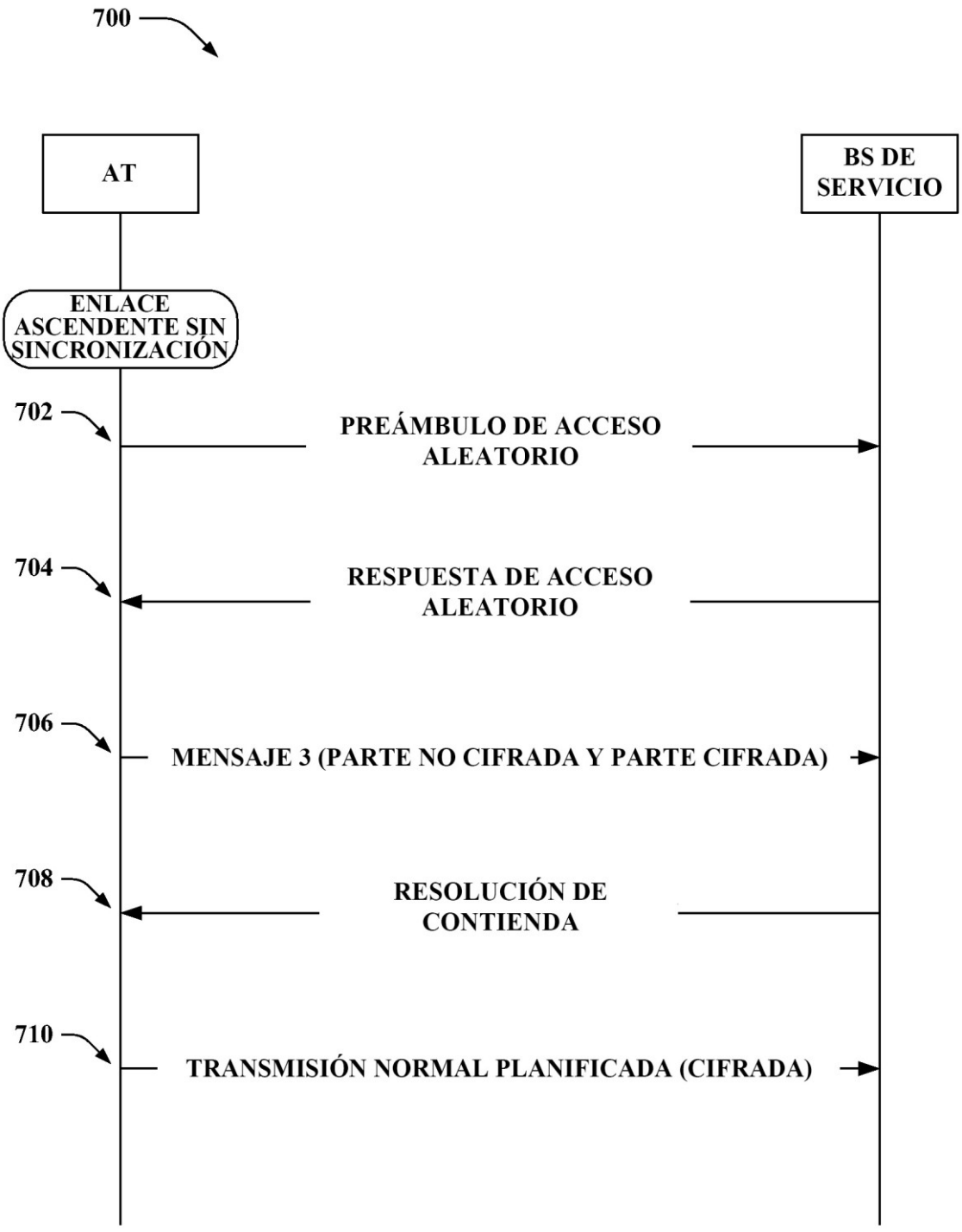
700
AT
BS DE SERVICIO
ENLACE ASCENDENTE SIN SINCRONIZACIÓN
702
PREÁMBULO DE ACCESO ALEATORIO
704
RESPUESTA DE ACCESO ALEATORIO
706
MENSAJE 3 (PARTE NO CIFRADA Y PARTE CIFRADA)
708
RESOLUCIÓN DE CONTIENDA
710
TRANSMISIÓN NORMAL PLANIFICADA (CIFRADA)

FIG. 7

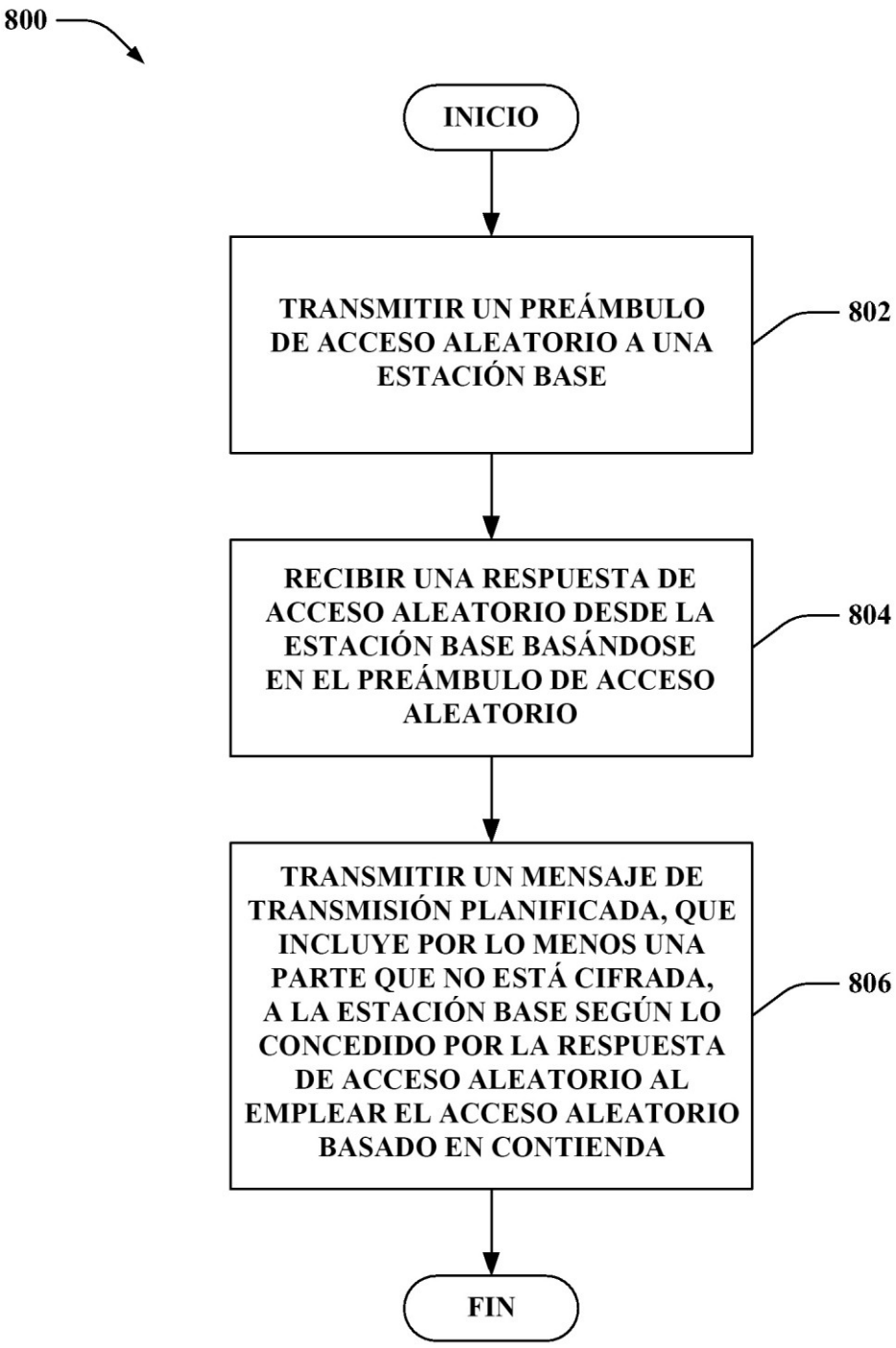
800
INICIO
TRANSMITIR UN PREÁMBULO DE ACCESO ALEATORIO A UNA ESTACIÓN BASE
802
RECIBIR UNA RESPUESTA DE ACCESO ALEATORIO DESDE LA ESTACIÓN BASE BASÁNDOSE EN EL PREÁMBULO DE ACCESO ALEATORIO
804
TRANSMITIR UN MENSAJE DE TRANSMISIÓN PLANIFICADA, QUE INCLUYE POR LO MENOS UNA PARTE QUE NO ESTÁ CIFRADA, A LA ESTACIÓN BASE SEGÚN LO CONCEDIDO POR LA RESPUESTA DE ACCESO ALEATORIO AL EMPLEAR EL ACCESO ALEATORIO BASADO EN CONTIENDA
806
FIN

FIG. 8

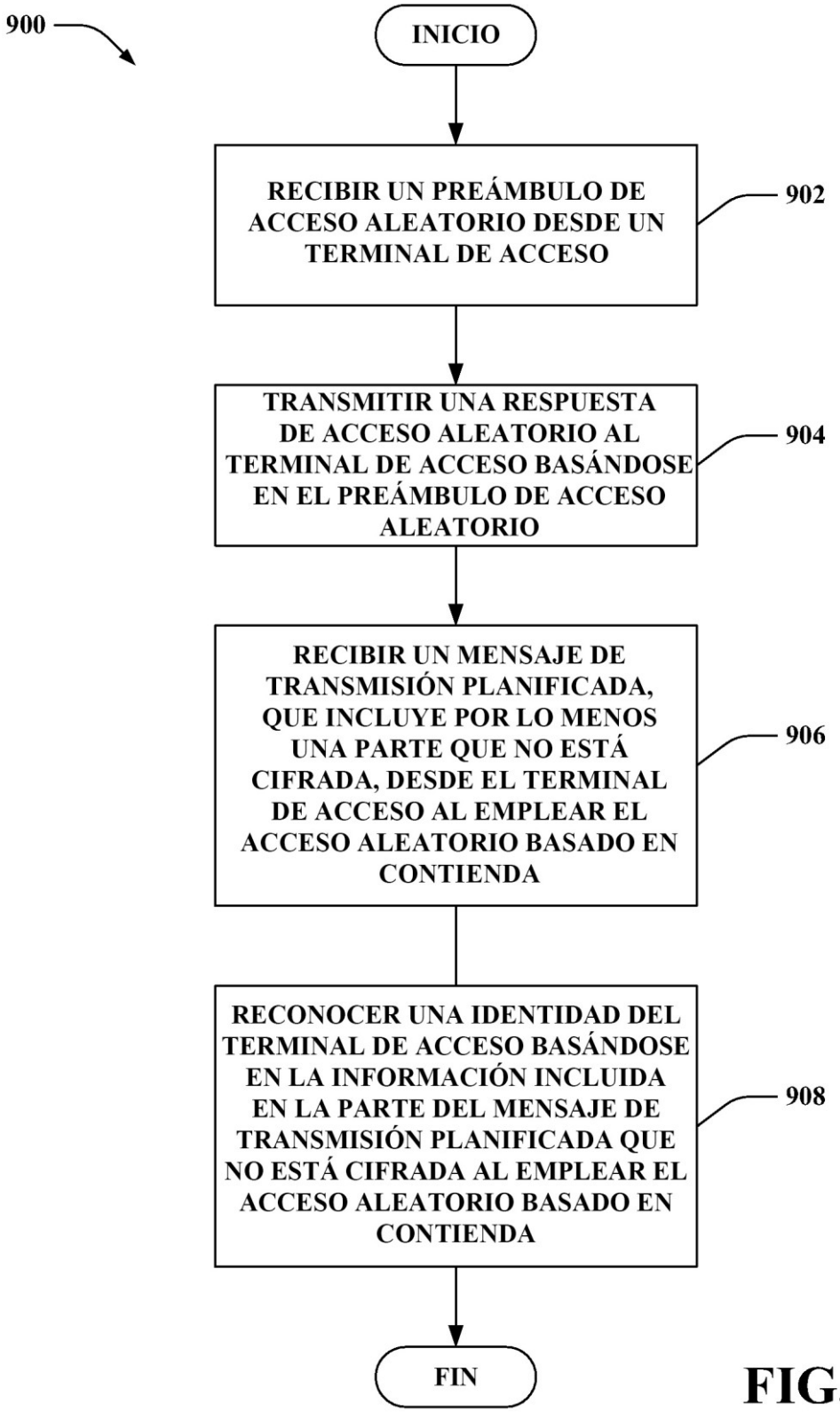
900
INICIO
RECIBIR UN PREÁMBULO DE ACCESO ALEATORIO DESDE UN TERMINAL DE ACCESO
902
TRANSMITIR UNA RESPUESTA DE ACCESO ALEATORIO AL TERMINAL DE ACCESO BASÁNDOSE EN EL PREÁMBULO DE ACCESO ALEATORIO
904
RECIBIR UN MENSAJE DE TRANSMISIÓN PLANIFICADA, QUE INCLUYE POR LO MENOS UNA PARTE QUE NO ESTÁ CIFRADA, DESDE EL TERMINAL DE ACCESO AL EMPLEAR EL ACCESO ALEATORIO BASADO EN CONTIENDA
906
RECONOCER UNA IDENTIDAD DEL TERMINAL DE ACCESO BASÁNDOSE EN LA INFORMACIÓN INCLUIDA EN LA PARTE DEL MENSAJE DE TRANSMISIÓN PLANIFICADA QUE NO ESTÁ CIFRADA AL EMPLEAR EL ACCESO ALEATORIO BASADO EN CONTIENDA
908
FIN

FIG. 9

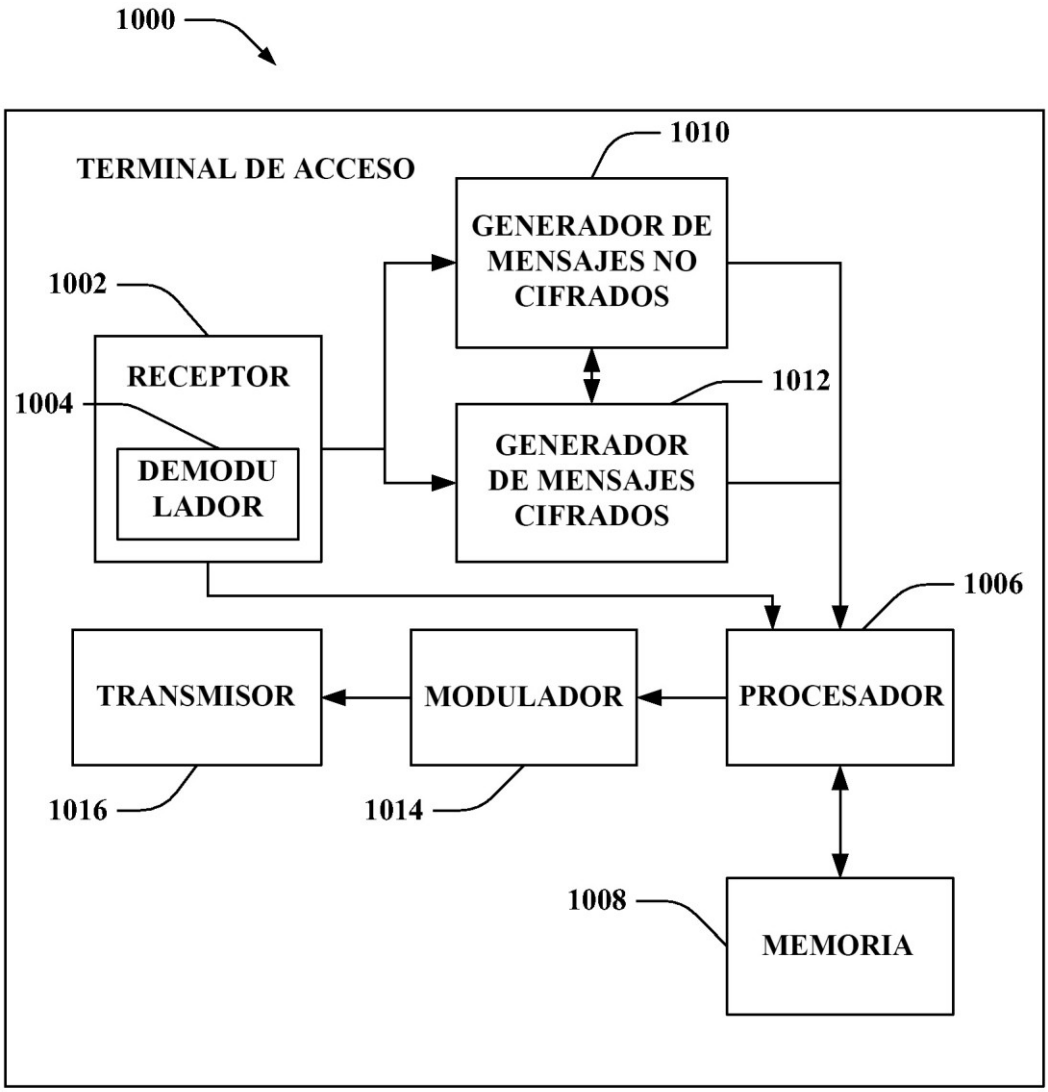
1000
TERMINAL DE ACCESO
1010
GENERADOR DE MENSAJES NO CIFRADOS
1002
RECEPTOR
1004
DEMODU LADOR
1012
GENERADOR DE MENSAJES CIFRADOS
1006
TRANSMISOR
MODULADOR
PROCESADOR
1016
1014
1008
MEMORIA

FIG. 10

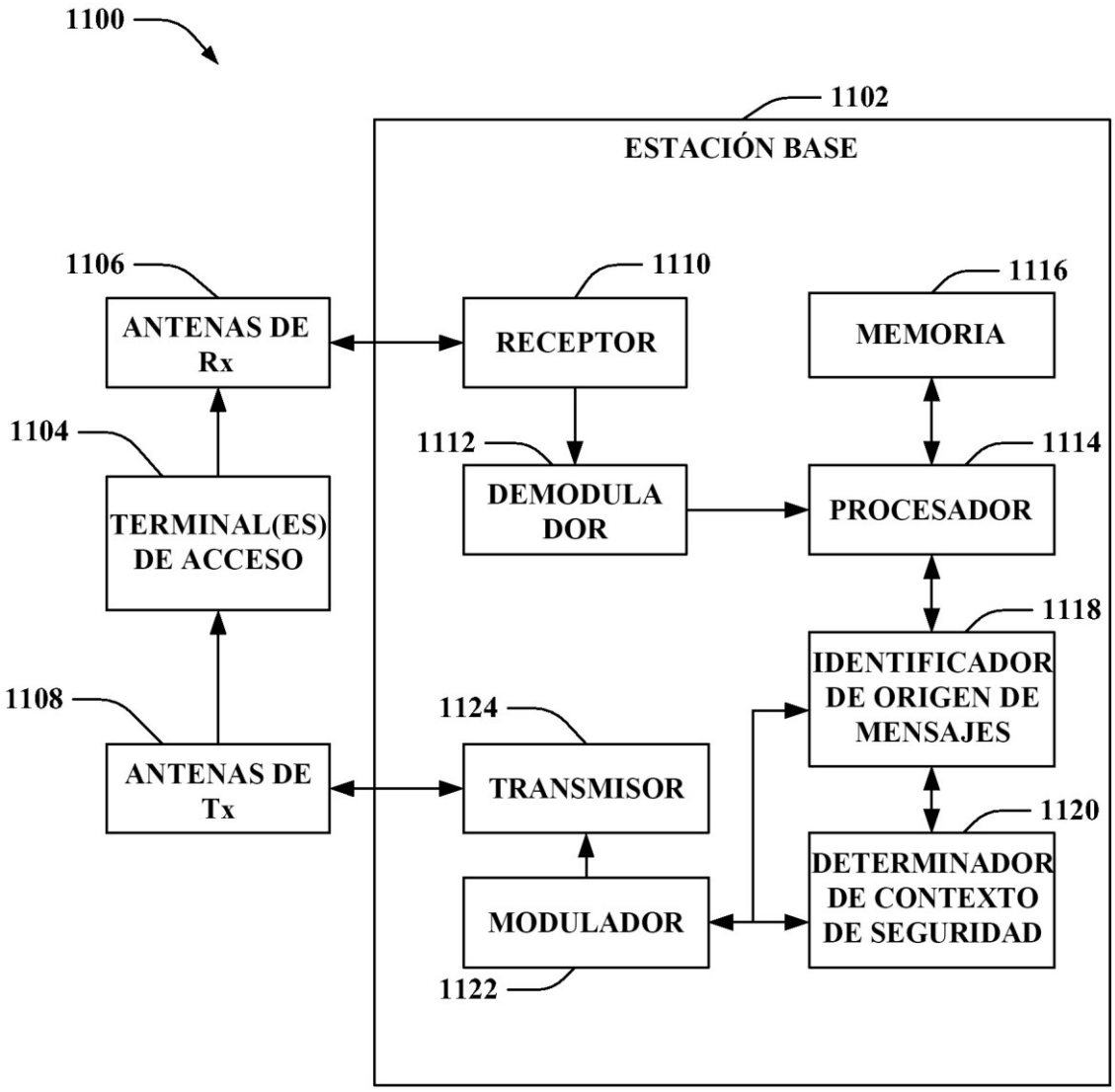
1100
1102
ESTACIÓN BASE
1106
ANTENAS DE Rx
1110
RECEPTOR
1116
MEMORIA
1104
TERMINAL(ES) DE ACCESO
1112
DEMODULADOR
1114
PROCESADOR
1118
IDENTIFICADOR DE ORIGEN DE MENSAJES
1108
ANTENAS DE Tx
1124
TRANSMISOR
1120
DETERMINADOR DE CONTEXTO DE SEGURIDAD
MODULADOR
1122

FIG. 11

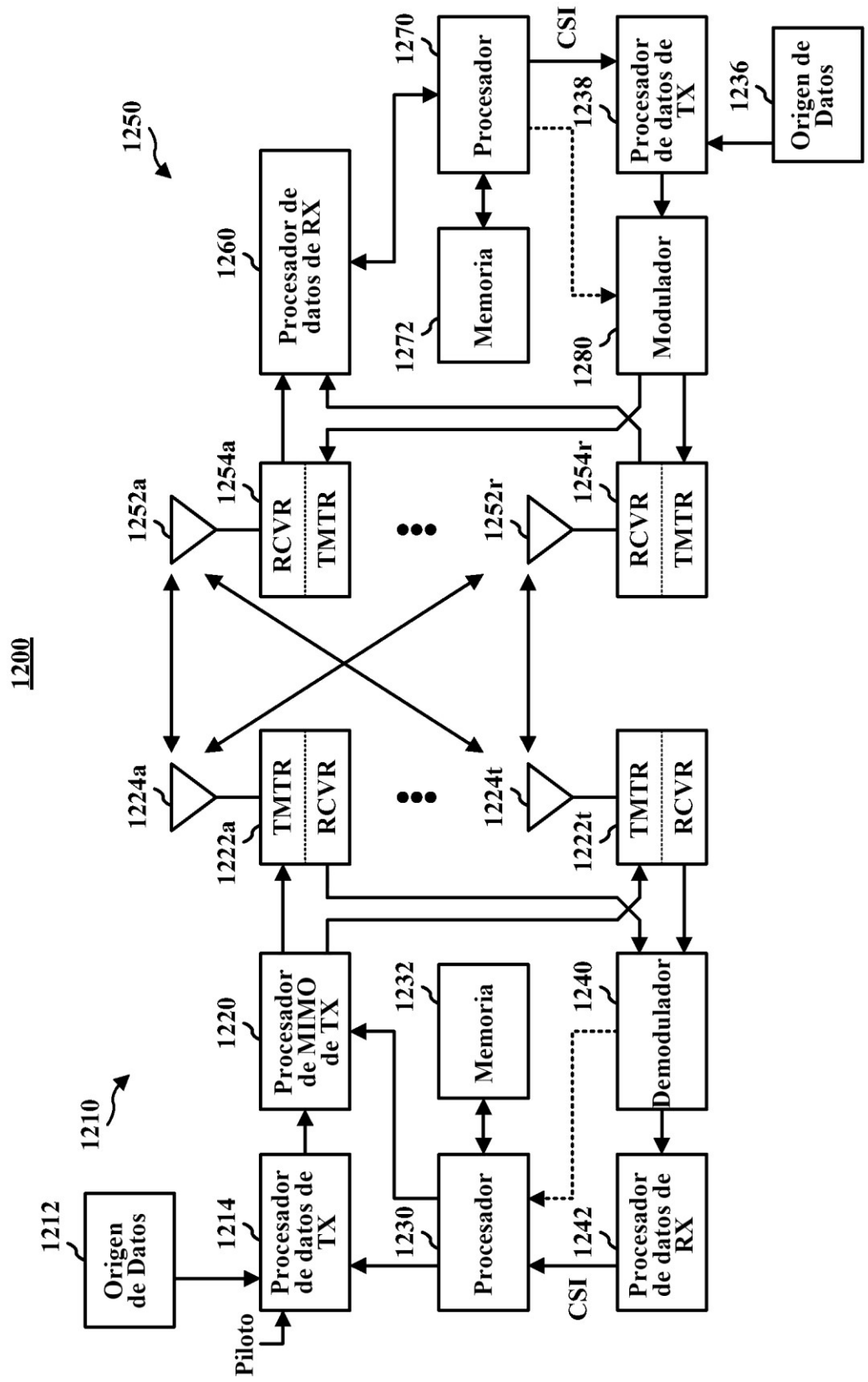
1200
1210
1212
Origen de Datos
1214
Procesador de datos de TX
Piloto
1220
Procesador de MIMO de TX
1222a
TMTR
RCVR
1222t
TMTR
RCVR
1224a
1224t
1230
Procesador
1232
Memoria
1240
Demodulador
1242
Procesador de datos de RX
CSI
1250
1252a
1252r
1254a
RCVR
TMTR
1254r
RCVR
TMTR
1260
Procesador de datos de RX
1270
Procesador
CSI
1272
Memoria
1280
Modulador
1238
Procesador de datos de TX
1236
Origen de Datos

FIG. 12

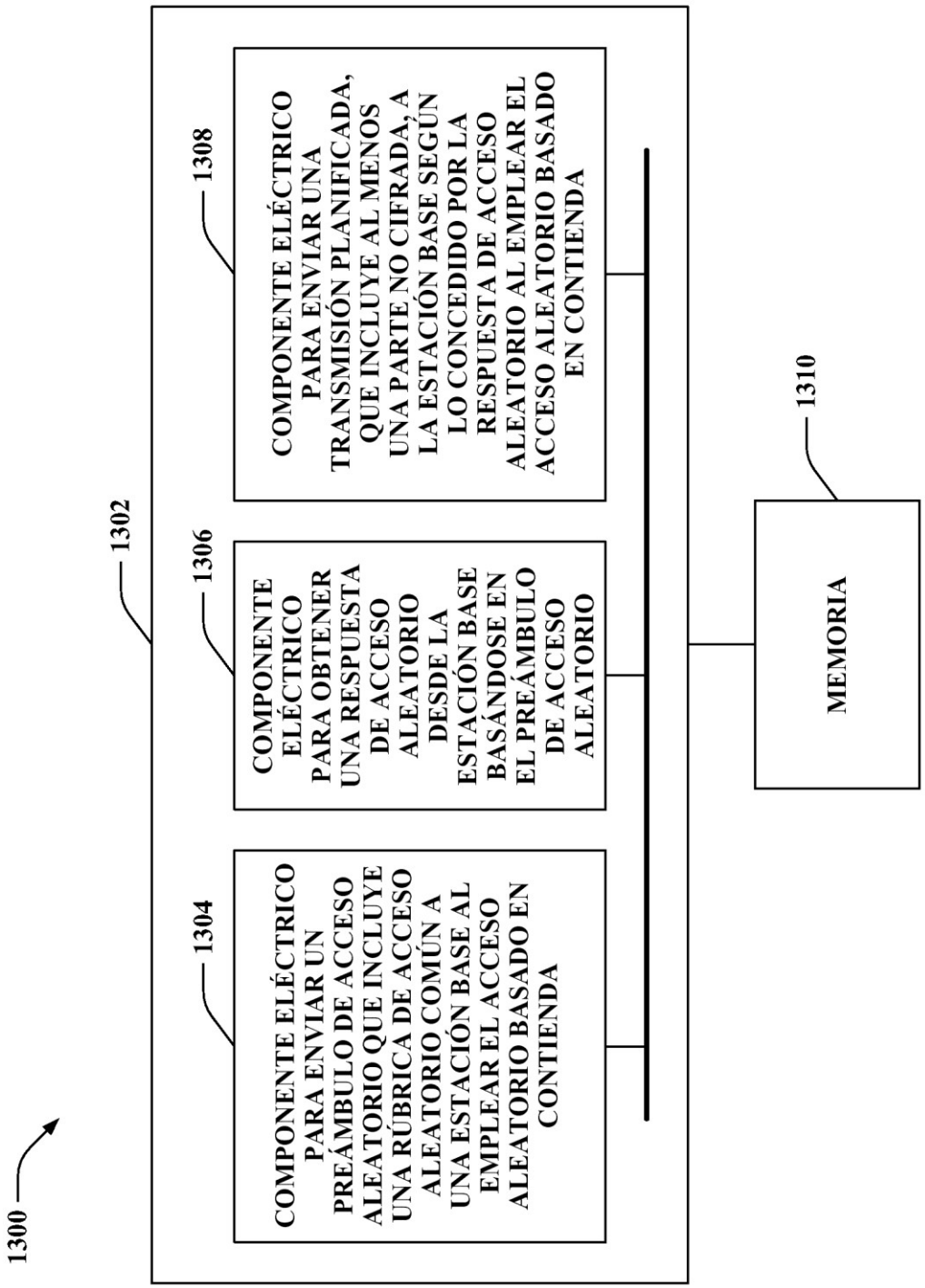
1300
1302
1304
COMPONENTE ELÉCTRICO PARA ENVIAR UN PREÁMBULO DE ACCESO ALEATORIO QUE INCLUYE UNA RÚBRICA DE ACCESO ALEATORIO COMÚN A UNA ESTACIÓN BASE AL EMPLEAR EL ACCESO ALEATORIO BASADO EN CONTIENDA
1306
COMPONENTE ELÉCTRICO PARA OBTENER UNA RESPUESTA DE ACCESO ALEATORIO DESDE LA ESTACIÓN BASE BASÁNDOSE EN EL PREÁMBULO DE ACCESO ALEATORIO
1308
COMPONENTE ELÉCTRICO PARA ENVIAR UNA TRANSMISIÓN PLANIFICADA, QUE INCLUYE AL MENOS UNA PARTE NO CIFRADA, A LA ESTACIÓN BASE SEGÚN LO CONCEDIDO POR LA RESPUESTA DE ACCESO ALEATORIO AL EMPLEAR EL ACCESO ALEATORIO BASADO EN CONTIENDA
1310
MEMORIA

FIG. 13

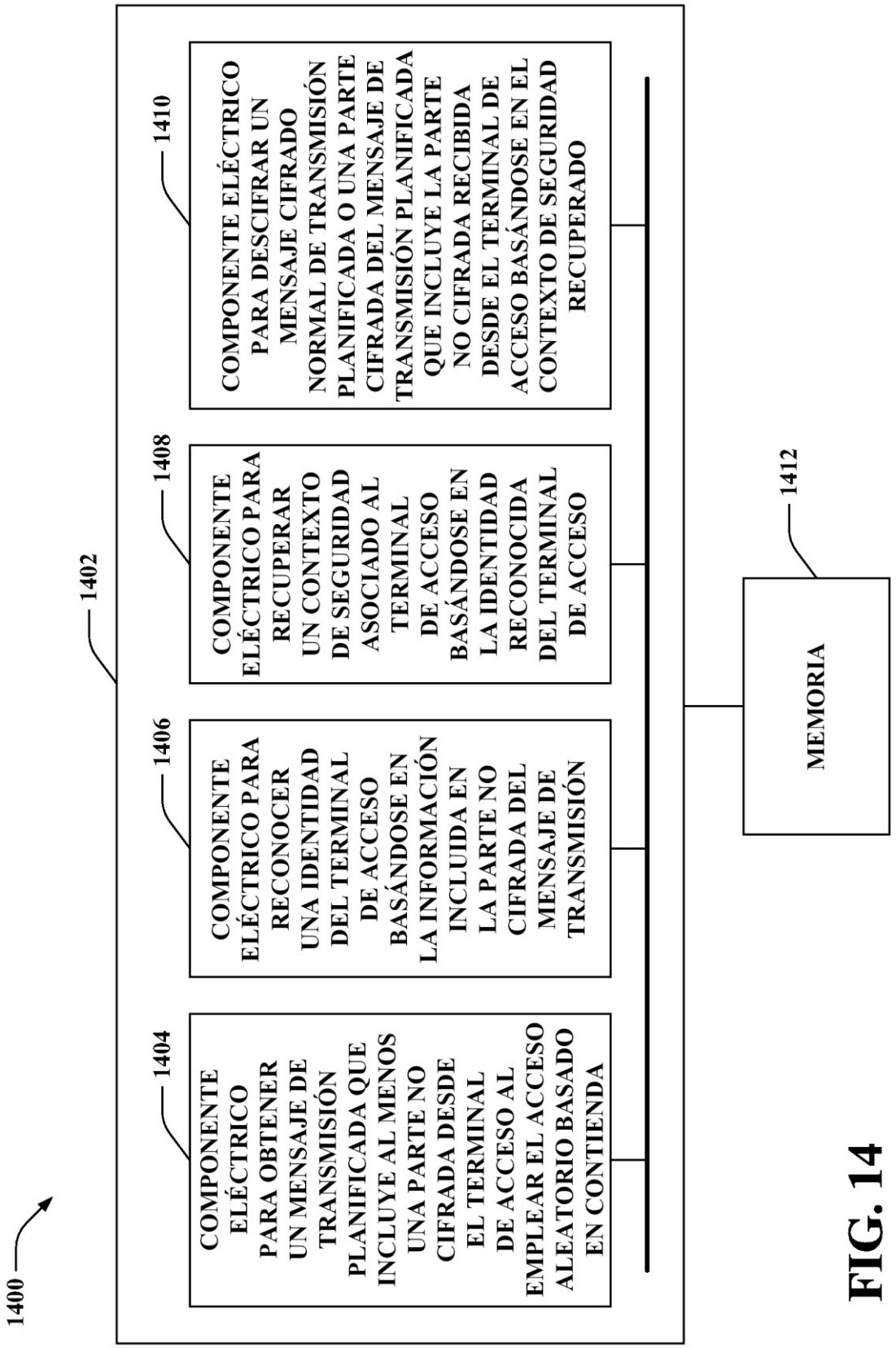
1400
1402
1404
COMPONENTE ELÉCTRICO PARA OBTENER UN MENSAJE DE TRANSMISIÓN PLANIFICADA QUE INCLUYE AL MENOS UNA PARTE NO CIFRADA DESDE EL TERMINAL DE ACCESO AL EMPLEAR EL ACCESO ALEATORIO BASADO EN CONTIENDA
1406
COMPONENTE ELÉCTRICO PARA RECONOCER UNA IDENTIDAD DEL TERMINAL DE ACCESO BASÁNDOSE EN LA INFORMACIÓN INCLUIDA EN LA PARTE NO CIFRADA DEL MENSAJE DE TRANSMISIÓN
1408
COMPONENTE ELÉCTRICO PARA RECUPERAR UN CONTEXTO DE SEGURIDAD ASOCIADO AL TERMINAL DE ACCESO BASÁNDOSE EN LA IDENTIDAD RECONOCIDA DEL TERMINAL DE ACCESO
1410
COMPONENTE ELÉCTRICO PARA DESCIFRAR UN MENSAJE CIFRADO NORMAL DE TRANSMISIÓN PLANIFICADA O UNA PARTE CIFRADA DEL MENSAJE DE TRANSMISIÓN PLANIFICADA QUE INCLUYE LA PARTE NO CIFRADA RECIBIDA DESDE EL TERMINAL DE ACCESO BASÁNDOSE EN EL CONTEXTO DE SEGURIDAD RECUPERADO
1412
MEMORIA

FIG. 14