(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 598 104**

(51) Int. CI.:

H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.01.2014 PCT/US2014/010419**

(87) Fecha y número de publicación internacional: **10.07.2014 WO14107701**

(96) Fecha de presentación y número de la solicitud europea: **07.01.2014 E 14703187 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.07.2016 EP 2941911**

(54) Título: **Mecanismo implícito de cambio de claves**

(30) Prioridad:

07.01.2013 US 201361749760 P
06.01.2014 US 201414148349

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2017

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

WENTINK, MAARTEN MENZO y
MALINEN, JOUNI

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Mecanismo implícito de cambio de claves

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

La presente solicitud de patente reivindica la prioridad sobre la solicitud provisional estadounidense n.º 61/749.760, presentada el 7 de enero de 2013, cedida al cesionario de la presente solicitud.

ANTECEDENTES

Campo de la invención

Ciertos aspectos de la presente divulgación se refieren, en general, a las comunicaciones inalámbricas y, más particularmente, a técnicas que pueden permitir la transmisión segura de paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre dispositivos transmisores y receptores.

Antecedentes

Las redes de comunicación inalámbrica están ampliamente implantadas para proporcionar diversos servicios de comunicación, tales como voz, vídeo, datos en paquetes, mensajería, radiodifusión etc. Estas redes inalámbricas pueden ser redes de acceso múltiple que pueden dar soporte a múltiples usuarios compartiendo los recursos de red disponibles. Ejemplos de tales redes de acceso múltiple incluyen redes de acceso múltiple por división de código (CDMA), redes de acceso múltiple por división del tiempo (TDMA), redes de acceso múltiple por división de frecuencia (FDMA), redes de acceso múltiple por división de frecuencia ortogonal (OFDMA) y redes de FDMA de portadora única (SC-FDMA).

Con el fin de abordar el deseo de una mayor cobertura y una mayor gama de comunicación, se están desarrollando diversos esquemas. Uno de estos esquemas es el rango de frecuencias por debajo de 1 GHz (por ejemplo, la que opera en el rango entre 902 y 928 MHz en Estados Unidos), que está siendo desarrollada por la fuerza de tareas 802.11ah del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Este desarrollo es impulsado por el deseo de utilizar un rango de frecuencias que tenga mayor alcance inalámbrico que otros grupos IEEE 802.11 y que tenga pérdidas inferiores por obstrucción.

El documento US 2011/0150223 A1 divulga un dispositivo inalámbrico y procedimientos para el cambio de claves, con pérdida de paquetes reducida en una red inalámbrica. Durante las operaciones de cambio de claves, puede ser instalada tempranamente una nueva clave para la recepción (es decir, antes de la recepción de un mensaje de confirmación de cambio de claves). El uso de la nueva clave para la transmisión puede retrasarse hasta después de la recepción del mensaje de confirmación de cambio de claves. La instalación temprana de la nueva clave para la recepción puede permitir que tanto la nueva clave como la vieja clave estén activas al mismo tiempo, para su uso al descifrar los paquetes recibidos para reducir la pérdida de paquetes durante las operaciones de cambio de claves. El mensaje de confirmación de cambio de claves puede ser el cuarto mensaje de un establecimiento de comunicación de cuatro vías para el cambio de claves. Dos identificadores de clave se pueden alternar entre establecimientos de comunicación de cuatro vías, para impedir la eliminación de la clave antigua.

RESUMEN

La invención se define en las reivindicaciones independientes 1, 4, 7, 10 y 15.

Determinados aspectos de la presente divulgación proporcionan un aparato para comunicaciones inalámbricas. El aparato incluye habitualmente un receptor configurado para recibir paquetes cortos desde un dispositivo, careciendo dichos paquetes pequeños de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo; y un decodificador configurado para decodificar, utilizando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos; participar en un procedimiento de cambio de clave con el dispositivo y decodificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de clave, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

Ciertos aspectos de la presente divulgación proporcionan un aparato para comunicaciones inalámbricas. El aparato incluye habitualmente un codificador configurado para codificar, usando un primer Identificador por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo; participar en un procedimiento de cambio de claves con el dispositivo y codificar, utilizando un segundo Identificador de Clave por defecto establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves; y un transmisor configurado para transmitir los primeros y segundos paquetes cortos.

Ciertos aspectos de la presente divulgación proporcionan un aparato para comunicaciones inalámbricas. El aparato incluye habitualmente medios para recibir paquetes cortos desde un dispositivo, careciendo dichos paquetes cortos de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo, medios para la decodificación, utilizando un primer identificador de clave por defecto, de algunos de los paquetes cortos recibidos y medios para participar en un procedimiento de cambio de claves con el dispositivo, en el que el medio para la decodificación está configurado para decodificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

Ciertos aspectos de la presente divulgación proporcionan un aparato para comunicaciones inalámbricas. El aparato incluye habitualmente medios para codificar, utilizando un primer identificador de clave por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo, medios para participar en un procedimiento de cambio de claves con el dispositivo, en el que el medio para la codificación está configurado para codificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves, y medios para transmitir los primeros y segundos paquetes cortos.

Ciertos aspectos de la presente divulgación proporcionan un procedimiento para comunicaciones inalámbricas por un aparato. El procedimiento incluye habitualmente la recepción de paquetes cortos desde un dispositivo, careciendo dichos paquetes cortos de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo; la decodificación, utilizando un primer identificador de clave por defecto, de algunos de los paquetes cortos recibidos, la participación en un procedimiento de cambio de claves con el dispositivo, y la decodificación, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, de algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

Ciertos aspectos de la presente divulgación proporcionan un procedimiento para comunicaciones inalámbricas por un aparato. El procedimiento incluye habitualmente la codificación, utilizando un primer identificador de clave por defecto, de primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo, la participación en un procedimiento de cambio de claves con el dispositivo, la codificación, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, de segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves, y la transmisión de los primeros y segundos paquetes cortos.

Ciertos aspectos de la presente divulgación proporcionan un producto de programa informático para comunicaciones inalámbricas por un aparato que comprende un medio legible por ordenador que tiene instrucciones almacenadas en el mismo. Las instrucciones son generalmente ejecutables por uno o más procesadores para recibir paquetes cortos desde un dispositivo, careciendo dichos paquetes cortos de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo; decodificar, utilizando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos, participar en un procedimiento de cambio de claves con el dispositivo y decodificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

Ciertos aspectos de la presente divulgación proporcionan un producto de programa informático para comunicaciones inalámbricas por un aparato que comprende un medio legible por ordenador que tiene instrucciones almacenadas en el mismo. Las instrucciones son generalmente ejecutables por uno o más procesadores, para codificar, utilizando un primer identificador de clave por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo, participar en un procedimiento de cambio de claves con el dispositivo, codificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves, y transmitir los primeros y segundos paquetes cortos.

Ciertos aspectos de la presente divulgación proporcionan un terminal de acceso para comunicaciones inalámbricas. El terminal de acceso incluye habitualmente al menos una antena, un receptor configurado para recibir, a través de la al menos una antena, paquetes cortos desde un dispositivo, careciendo dichos paquetes cortos de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo; y un decodificador configurado para decodificar, utilizando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos, participar en un procedimiento de cambio de claves con el dispositivo, y decodificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

Ciertos aspectos de la presente divulgación proporcionan un punto de acceso. El punto de acceso incluye habitualmente al menos una antena, un codificador configurado para codificar, utilizando un primer identificador de clave por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo; participar en un procedimiento de cambio de claves con el dispositivo y codificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento

de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves; y un transmisor configurado para transmitir, a través de la al menos una antena, los primeros y segundos paquetes cortos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A fin de que la forma en que se presentan las características mencionadas anteriormente de la presente divulgación pueda ser entendida en detalle, se ofrece una descripción más específica, resumida anteriormente de manera breve, haciendo referencia a sus aspectos, algunos de los cuales se ilustran en los dibujos adjuntos. Sin embargo, debe observarse que los dibujos adjuntos solo ilustran determinados aspectos típicos de esta divulgación y, por lo tanto, no deben considerarse limitadores de su alcance, ya que la descripción puede admitir otros aspectos igualmente eficaces.

La figura 1 ilustra un diagrama de una red ejemplar de comunicaciones inalámbricas de acuerdo con ciertos aspectos de la presente divulgación.

La figura 2 ilustra un diagrama de bloques de un punto de acceso y terminales de usuario ejemplares, según determinados aspectos de la presente divulgación.

La figura 3 ilustra un diagrama de bloques de un dispositivo inalámbrico ejemplar de acuerdo con ciertos aspectos de la presente divulgación.

La figura 4A ilustra una estructura ejemplar de paquetes que utiliza una cabecera corta de MAC.

La figura 4B ilustra una estructura ejemplar de paquete que utiliza una cabecera corta de MAC sin un campo de Identificador de Clave, de acuerdo con ciertos aspectos de la presente divulgación.

La figura 5 ilustra un diagrama de bloques de operaciones ejemplares para comunicaciones inalámbricas por parte de un receptor, de acuerdo con ciertos aspectos de la presente divulgación.

La figura 5A ilustra medios ejemplares que pueden realizar las operaciones mostradas en la figura 5.

La figura 6 ilustra un diagrama de bloques de operaciones ejemplares para comunicaciones inalámbricas por parte de un transmisor, de acuerdo con ciertos aspectos de la presente divulgación.

La figura 6A ilustra medios ejemplares que pueden realizar las operaciones mostradas en la figura 6.

DESCRIPCIÓN DETALLADA

Diversos aspectos de la divulgación se describen a continuación en el presente documento en mayor detalle con referencia a los dibujos adjuntos. Sin embargo, esta divulgación puede realizarse de muchas formas diferentes, y no debería interpretarse como limitada a alguna estructura o función específica, presentada a lo largo de esta divulgación. En cambio, estos aspectos se proporcionan para que esta divulgación sea exhaustiva y completa, y transmita completamente el alcance de la divulgación a los expertos en la técnica. En base a las enseñanzas del presente documento, un experto en la técnica apreciará que el alcance de la divulgación pretende abarcar cualquier aspecto de la divulgación divulgada en el presente documento, ya sea implementada de manera independiente de, o en combinación con, cualquier otro aspecto de la divulgación. Por ejemplo, un aparato puede implementarse, o un procedimiento puede llevarse a la práctica, usando cualquier número de los aspectos dados a conocer en el presente documento. Además, el alcance de la divulgación pretende abarcar un aparato o procedimiento de este tipo, que sea llevado a la práctica usando otra estructura, funcionalidad, o estructura y funcionalidad, además de, o diferentes de, los diversos aspectos de la divulgación expuestos en el presente documento. Debería entenderse que cualquier aspecto de la divulgación divulgado en el presente documento puede realizarse mediante uno o más elementos de una reivindicación.

Aunque en el presente documento se describen aspectos particulares, muchas variaciones y permutaciones de estos aspectos están dentro del alcance de la divulgación. Aunque se mencionan algunos beneficios y ventajas de los aspectos preferidos, el alcance de la divulgación no pretende limitarse a beneficios, usos u objetivos particulares. En cambio, los aspectos de la divulgación están concebidos para ser aplicables, en sentido amplio, a diferentes tecnologías inalámbricas, configuraciones de sistema, redes y protocolos de transmisión, algunos de los cuales se ilustran a modo de ejemplo en las figuras y en la siguiente descripción de los aspectos preferidos. La descripción detallada y los dibujos simplemente ilustran la divulgación, en lugar de limitar el alcance de la divulgación, el cual está definido por las reivindicaciones adjuntas y los equivalentes de las mismas.

UN SISTEMA EJEMPLAR DE COMUNICACIÓN INALÁMBRICA

Las técnicas descritas en el presente documento pueden usarse para diversos sistemas de comunicación

inalámbrica de banda ancha, incluyendo sistemas de comunicación que están basados en un esquema de multiplexado ortogonal. Ejemplos de tales sistemas de comunicación incluyen sistemas de acceso múltiple por división espacial (SDMA), de acceso múltiple por división del tiempo (TDMA), sistemas de acceso múltiple por división de frecuencia ortogonal (OFDMA), sistemas de acceso múltiple por división de frecuencia de portadora única (SC-FDMA), etc. Un sistema de SDMA puede utilizar direcciones suficientemente diferentes para transmitir simultáneamente datos que pertenecen a múltiples terminales de usuario. Un sistema de TDMA puede permitir que múltiples terminales de usuario compartan el mismo canal de frecuencia dividiendo la señal de transmisión en diferentes ranuras temporales, estando asignada cada ranura temporal a diferentes terminales de usuario. Un sistema de OFDMA utiliza el multiplexado por división de frecuencia ortogonal (OFDM), que es una técnica de modulación que divide el ancho de banda global del sistema en múltiples sub-portadoras ortogonales. Estas sub-portadoras también pueden denominarse tonos, contenedores, etc. Con el OFDM, cada sub-portadora puede modularse de manera independiente con datos. Un sistema de SC-FDMA puede utilizar el FDMA entrelazado (IFDMA) para transmitir, en sub-portadoras que están distribuidas entre el ancho de banda del sistema, el FDMA localizado (LFDMA) para transmitir en un bloque de sub-portadoras adyacentes, o el FDMA mejorado (EFDMA) para transmitir en múltiples bloques de sub-portadoras adyacentes. En general, los símbolos de modulación se envían en el dominio de frecuencia con el OFDM y en el dominio del tiempo con el SC-FDMA.

Las enseñanzas del presente documento pueden incorporarse en (por ejemplo, implementarse dentro de, o realizarse por) varios aparatos cableados o inalámbricos (por ejemplo, nodos). En algunos aspectos, un nodo inalámbrico implementado según las enseñanzas en el presente documento puede comprender un punto de acceso o un terminal de acceso.

Un punto de acceso (“AP”) puede comprender, implementarse como, o conocerse como, un Nodo B, un controlador de red de radio (“RNC”), un Nodo B evolucionado (eNB), un controlador de estación base (“BSC”), una estación transceptora base (“BTS”), una estación base (“BS”), una función transceptora (“TF”), un encaminador de radio, un transceptor de radio, un conjunto de servicios básicos (“BSS”), un conjunto de servicios extendidos (“ESS”), una estación base de radio (“RBS”), o alguna otra terminología.

Un terminal de acceso (“AT”) puede comprender, implementarse como, o conocerse como, una estación de abonado, una unidad de abonado, una estación móvil (MS), una estación remota, un terminal remoto, un terminal de usuario (UT), un agente de usuario, un dispositivo de usuario, un equipo de usuario (UE), una estación de usuario, o alguna otra terminología. En algunas implementaciones, un terminal de acceso puede comprender un teléfono celular, 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, una estación ("STA") o algún otro dispositivo de procesamiento adecuado conectado a un módem inalámbrico. Por consiguiente, uno o más aspectos dados a conocer en el presente documento pueden incorporarse en un teléfono (por ejemplo, un teléfono celular o teléfono inteligente), un ordenador (por ejemplo, un ordenador portátil), una tableta, un dispositivo de comunicación portátil, un dispositivo informático portátil (por ejemplo, un asistente personal de datos), un dispositivo de entretenimiento (por ejemplo, un dispositivo de música o vídeo, o una radio por satélite), un dispositivo del sistema de localización global (GPS) o cualquier otro dispositivo adecuado que esté configurado para comunicarse a través de un medio inalámbrico o cableado. En algunos aspectos, el nodo es un nodo inalámbrico. El nodo inalámbrico de ese tipo puede proporcionar, por ejemplo, conectividad para, o con, una red (por ejemplo, una red de área extensa tal como Internet o una red celular) a través de un enlace de comunicación cableado o inalámbrico.

La figura 1 ilustra un sistema de acceso múltiple, múltiples entradas y múltiples salidas (MIMO) 100 con puntos de acceso y terminales de usuario. Por motivos de simplicidad, únicamente se muestra un punto de acceso 110 en la figura 1. Un punto de acceso es generalmente una estación fija que se comunica con los terminales de usuario y que también puede denominarse una estación base, o alguna otra terminología. Un terminal de usuario puede ser fijo o móvil, y puede denominarse también como una estación móvil, un dispositivo inalámbrico, o alguna otra terminología. El punto de acceso 110 puede comunicarse con uno o más terminales de usuario 120 en cualquier momento dado, en el enlace descendente y en el enlace ascendente. El enlace descendente (es decir, el enlace directo) es el enlace de comunicación desde el punto de acceso a los terminales de usuario, y el enlace ascendente (es decir, el enlace inverso) es el enlace de comunicación desde los terminales de usuario al punto de acceso. Un terminal de usuario también puede comunicarse entre iguales con otro terminal de usuario. Un controlador de sistema 130 se acopla a, y proporciona coordinación y control para, los puntos de acceso.

Si bien partes de la siguiente divulgación describirán terminales de usuario 120 capaces de comunicarse mediante el acceso múltiple por división espacial (SDMA), para ciertos aspectos, los terminales de usuario 120 también pueden incluir algunos terminales de usuario que no dan soporte al SDMA. Por lo tanto, para tales aspectos, un AP 110 puede configurarse para comunicarse con terminales de usuario, tanto de SDMA como no de SDMA. Este enfoque puede permitir convenientemente que versiones anteriores de terminales de usuario (estaciones "heredadas") permanezcan implantadas en una empresa, ampliando su vida útil, permitiendo a la vez que se introduzcan nuevos terminales de usuario de SDMA según se considere adecuado.

El sistema 100 emplea antenas de transmisión múltiple y recepción múltiple para la transmisión de datos en el

enlace descendente y en el enlace ascendente. El punto de acceso 110 está equipado con N_{ap} antenas y representa la entrada múltiple (MI) para transmisiones de enlace descendente y la salida múltiple (MO) para transmisiones de enlace ascendente. Un conjunto de $_K$ terminales de usuario 120 seleccionados representa en conjunto la salida múltiple para transmisiones de enlace descendente y la entrada múltiple para transmisiones de enlace ascendente. Para un SDMA puro, se desea tener $N_{ap} \geq K \geq 1$ si los flujos de símbolos de datos para los K terminales de usuario no están multiplexados en código, frecuencia o tiempo por algún medio. $_K$ puede ser mayor que N_{ap} si los flujos de símbolos de datos pueden multiplexarse usando una técnica de TDMA, diferentes canales de código con CDMA, conjuntos disjuntos de sub-bandas con OFDM, etc. Cada terminal de usuario seleccionado transmite datos específicos de usuario a, y/o recibe datos específicos de usuario desde, el punto de acceso. En general, cada terminal de usuario seleccionado puede equiparse con una o más antenas (es decir, $N_{ut} \geq 1$). Los $_K$ terminales de usuario seleccionados pueden tener el mismo número, o un número diferente, de antenas.

El sistema de SDMA puede ser un sistema de dúplex por división del tiempo (TDD) o un sistema de dúplex por división de frecuencia (FDD). Para un sistema de TDD, el enlace descendente y el enlace ascendente comparten la misma banda de frecuencia. Para un sistema de FDD, el enlace descendente y el enlace ascendente usan diferentes bandas de frecuencia. El sistema de MIMO 100 también puede utilizar una única portadora o múltiples portadoras para la transmisión. Cada terminal de usuario puede estar equipado con una única antena (por ejemplo, para mantener los costes reducidos) o múltiples antenas (por ejemplo, cuando puede asumirse el coste adicional). El sistema 100 también puede ser un sistema de TDMA si los terminales de usuario 120 comparten el mismo canal de frecuencia dividiendo la transmisión/recepción en diferentes intervalos de tiempo, estando cada intervalo de tiempo asignado a un terminal de usuario diferente 120.

La figura 2 ilustra un diagrama de bloques del punto de acceso 110 y dos terminales de usuario 120m y 120x en el sistema de MIMO 100. El punto de acceso 110 está equipado con N_t antenas 224a a 224t. El terminal de usuario 120m está equipado con $N_{ut,m}$ antenas 252ma a 252mu, y el equipo de usuario 120x está equipado con $N_{ut,x}$ antenas 252xa a 252xu. El punto de acceso 110 es una entidad de transmisión para el enlace descendente y una entidad de recepción para el enlace ascendente. Cada terminal de usuario 120 es una entidad de transmisión para el enlace ascendente y una entidad de recepción para el enlace descendente. Tal y como se usa en el presente documento, una "entidad de transmisión" es un aparato o dispositivo operado de forma independiente, capaz de transmitir datos a través de un canal inalámbrico, y una "entidad de recepción" es un aparato o dispositivo operado de forma independiente, capaz de recibir datos a través de un canal inalámbrico. En la siguiente descripción, el subíndice *"dn"* representa el enlace descendente, el subíndice *"up"* representa el enlace ascendente, se seleccionan N_{up} terminales de usuario para la transmisión simultánea en el enlace ascendente, se seleccionan N_{dn} terminales de usuario para la transmisión simultánea en el enlace descendente, N_{up} puede ser igual o no a N_{dn}, y N_{up} y N_{dn} pueden ser valores estáticos o pueden cambiar para cada intervalo de planificación. Puede usarse la orientación de haces o alguna otra técnica de procesamiento espacial en el punto de acceso y el terminal de usuario.

En el enlace ascendente, en cada terminal de usuario 120 seleccionado para la transmisión de enlace ascendente, un procesador de datos de transmisión (TX) 288 recibe datos de tráfico desde un origen de datos 286 y datos de control desde un controlador 280. El procesador de datos de TX 288 procesa (por ejemplo, codifica, entrelaza y modula) los datos de tráfico para el terminal de usuario basándose en los esquemas de codificación y modulación asociados a la velocidad seleccionada para el terminal de usuario y proporciona un flujo de símbolos de datos. Un procesador espacial de TX 290 realiza un procesamiento espacial en el flujo de símbolos de datos y proporciona $N_{ut,m}$ flujos de símbolos de transmisión para las $N_{ut,m}$ antenas. Cada unidad de transmisión (TMTR) 254 recibe y procesa (por ejemplo, convierte a analógico, amplifica, filtra y aumenta en frecuencia) un respectivo flujo de símbolos de transmisión para generar una señal de enlace ascendente. $N_{ut,m}$ unidades de transmisión 254 proporcionan $N_{ut,m}$ señales de enlace ascendente para su transmisión desde $N_{ut,m}$ antenas 252 al punto de acceso.

Pueden planificarse N_{up} terminales de usuario para la transmisión simultánea en el enlace ascendente. Cada uno de estos terminales de usuario lleva a cabo un procesamiento espacial en su flujo de símbolos de datos y transmite al punto de acceso su conjunto de flujos de símbolos de transmisión en el enlace ascendente.

En el punto de acceso 110, N_{ap} antenas 224a a 224ap reciben las señales de enlace ascendente desde todos los N_{up} terminales de usuario que transmiten en el enlace ascendente. Cada antena 224 proporciona una señal recibida a una respectiva unidad de recepción (RCVR) 222. Cada unidad de recepción 222 realiza un procesamiento complementario al realizado por la unidad de transmisión 254 y proporciona un flujo de símbolos recibidos. Un procesador espacial de RX 240 realiza el procesamiento espacial de recepción en los N_{ap} flujos de símbolos recibidos desde las N_{ap} unidades de recepción 222 y proporciona N_{up} flujos recuperados de símbolos de datos de enlace ascendente. El procesamiento espacial de recepción se realiza según la inversión matricial de correlación de canal (CCMI), el mínimo error cuadrático medio (MMSE), la cancelación suave de interferencias (SIC) o alguna otra técnica. Cada flujo recuperado de símbolos de datos de enlace ascendente es una estimación de un flujo de símbolos de datos transmitido por un respectivo terminal de usuario. Un procesador de datos de RX 242 procesa (por ejemplo, desmodula, desentrelaza y decodifica) cada flujo recuperado de símbolos de datos de enlace ascendente según la velocidad usada para ese flujo, para obtener datos decodificados. Los datos decodificados para cada terminal de usuario pueden proporcionarse a un colector de datos 244 para su almacenamiento y/o a un controlador 230 para un procesamiento adicional.

En el enlace descendente, en el punto de acceso 110, un procesador de datos de TX 210 recibe datos de tráfico desde un origen de datos 208 para N_{dn} terminales de usuario planificados para la transmisión en el enlace descendente, datos de control desde un controlador 230 y, posiblemente, otros datos desde un planificador 234. Los diversos tipos de datos pueden enviarse en diferentes canales de transporte. El procesador de datos de TX 210 procesa (por ejemplo, codifica, entrelaza y modula) los datos de tráfico para cada terminal de usuario basándose en la velocidad seleccionada para ese terminal de usuario. El procesador de datos de TX 210 proporciona N_{dn} flujos de símbolos de datos de enlace descendente para los N_{dn} terminales de usuario. Un procesador espacial de TX 220 realiza un procesamiento espacial (tal como una pre-codificación o conformación de haces, como se describe en la presente divulgación) en los N_{dn} flujos de símbolos de datos de enlace descendente, y proporciona N_{ap} flujos de símbolos de transmisión para las N_{ap} antenas. Cada unidad de transmisión 222 recibe y procesa un respectivo flujo de símbolos de transmisión para generar una señal de enlace descendente. N_{ap} unidades de transmisión 222 proporcionan N_{ap} señales de enlace descendente para su transmisión desde N_{ap} antenas 224 a los terminales de usuario.

En cada terminal de usuario 120, $N_{ut,m}$ antenas 252 reciben las N_{ap} señales de enlace descendente desde el punto de acceso 110. Cada unidad de recepción 254 procesa una señal recibida desde una antena asociada 252 y proporciona un flujo de símbolos recibido. Un procesador espacial de RX 260 realiza el procesamiento espacial de recepción en los $N_{ut,m}$ flujos de símbolos recibidos desde $N_{ut,m}$ unidades de recepción 254 y proporciona un flujo recuperado de símbolos de datos de enlace descendente para el terminal de usuario. El procesamiento espacial de recepción se realiza según la CCMI, el MMSE o alguna otra técnica. Un procesador de datos de RX 270 procesa (por ejemplo, desmodula, des-entrelaza y decodifica) el flujo recuperado de símbolos de datos de enlace descendente, para obtener datos decodificados para el terminal de usuario.

En cada terminal de usuario 120, un estimador de canal 278 estima la respuesta de canal de enlace descendente y proporciona estimaciones de canal de enlace descendente, que pueden incluir estimaciones de ganancia de canal, estimaciones de SNR, varianza de ruido, etc. Asimismo, un estimador de canal 228 estima la respuesta de canal de enlace ascendente y proporciona estimaciones de canal de enlace ascendente. El controlador 280 para cada terminal de usuario obtiene normalmente la matriz de filtro espacial para el terminal de usuario basándose en la matriz de respuesta de canal de enlace descendente $H_{dn,m}$ para ese terminal de usuario. El controlador 230 obtiene la matriz de filtro espacial para el punto de acceso basándose en la matriz efectiva de respuesta de canal de enlace ascendente $H_{up,eff}$. El controlador 280 para cada terminal de usuario puede enviar información de retro-alimentación (por ejemplo, los auto-vectores, los auto-valores, las estimaciones de la SNR, etc., de enlace descendente y/o de enlace ascendente) al punto de acceso. Los controladores 230 y 280 controlan además el funcionamiento de varias unidades de procesamiento en el punto de acceso 110 y el terminal de usuario 120, respectivamente.

La figura 3 ilustra diversos componentes que pueden utilizarse en un dispositivo inalámbrico 302 que puede emplearse en el sistema de MIMO 100. El dispositivo inalámbrico 302 es un ejemplo de un dispositivo que puede configurarse para implementar los diversos procedimientos descritos en el presente documento. El dispositivo inalámbrico 302 puede ser un punto de acceso 110 o un terminal de usuario 120.

El dispositivo inalámbrico 302 puede incluir un procesador 304 que controla el funcionamiento del dispositivo inalámbrico 302. El procesador 304 también puede denominarse una unidad central de procesamiento (CPU). La memoria 306, que puede incluir tanto memoria de sólo lectura (ROM) como memoria de acceso aleatorio (RAM), proporciona instrucciones y datos al procesador 304. Una parte de la memoria 306 también puede incluir una memoria de acceso aleatorio no volátil (NVRAM). El procesador 304 realiza habitualmente operaciones lógicas y aritméticas basadas en instrucciones de programa almacenadas dentro de la memoria 306. Las instrucciones en la memoria 306 pueden ser ejecutables para implementar los procedimientos descritos en el presente documento.

El dispositivo inalámbrico 302 también puede incluir un alojamiento 308 que puede incluir un transmisor 310 y un receptor 312 para permitir la transmisión y la recepción de datos entre el dispositivo inalámbrico 302 y una ubicación remota. El transmisor 310 y el receptor 312 pueden combinarse en un transceptor 314. Una única antena, o una pluralidad de antenas de transmisión 316, puede(n) fijarse al alojamiento 308 y acoplarse eléctricamente al transceptor 314. El dispositivo inalámbrico 302 también puede incluir múltiples transmisores, múltiples receptores y múltiples transceptores (no mostrados).

El dispositivo inalámbrico 302 también puede incluir un detector de señales 318 que puede usarse para detectar y cuantificar el nivel de señales recibidas por el transceptor 314. El detector de señales 318 puede detectar señales tales como energía total, energía por sub-portadora por símbolo, densidad espectral de potencia y otras señales. El dispositivo inalámbrico 302 también puede incluir un procesador de señales digitales (DSP) 320 para su uso en el procesamiento de señales.

Los diversos componentes del dispositivo inalámbrico 302 pueden acoplarse entre sí mediante un sistema de bus 322, que puede incluir un bus de potencia, un bus de señales de control y un bus de señales de estado, además de un bus de datos.

CABECERAS CORTAS DE MAC

La Modalidad de Contador (CTR) con el Protocolo de Encadenamiento de bloques Cifrados y Código de Autenticación de Mensajes (CBC-MAC) (CCMP) es un protocolo que se puede utilizar para proteger criptográficamente las MPDU de la norma 802.11. La protección se basa en una clave que se acuerda entre los dispositivos inalámbricos de comunicación. El tráfico grupal se protege usando una Clave Temporal Grupal (GTK), mientras que el tráfico de unidifusión se protege usando una Clave Pareada Transitoria (PTK), parte de la cual es una Clave Temporal (TK).

La figura 4A ilustra un ejemplo de un paquete 400A (por ejemplo, una MPDU) con una cabecera corta de MAC 410, una cabecera de CCMP 420, un Código de Integridad de Mensaje (MIC) 430 y una secuencia de verificación de trama (FCS) 440.

Como se ilustra, la cabecera corta de MAC 410 puede contener un campo de control de trama (FC) 412, la dirección de destino 414 y la dirección de origen 416 del paquete de datos, y un campo de control de secuencia 418. Como se ilustra, la cabecera de CCMP 420 puede tener un número de paquete (PN) y un octeto de identificador de clave 422 con un campo Ext IV y un campo de identificador de clave. Como se ilustra, el número de paquete es un número de 48 bits almacenado en 6 octetos (como se ilustra, los códigos de PN pueden ser transportados en los primeros dos octetos 426 y los últimos cuatro octetos 428 de la cabecera de CCMP 420) y se aumenta para cada paquete posterior.

Como se ilustra, el octeto de Identificador de Clave 422 puede contener el campo Ext IV (bit 5), el campo de Identificador de Clave (bits 6 a 7) y un sub-campo reservado (bits 0 a 4). Esta información en la cabecera de CCMP 420 puede utilizarse para cifrar la unidad de datos y el MIC 430, que protege la integridad y la autenticidad del paquete. La FCS 440, por otra parte, que se utiliza para la detección y corrección de errores, no se cifra habitualmente.

MECANISMO IMPLÍCITO DE CAMBIO DE CLAVES

Hay ciertos escenarios en los que una nueva GTK o PTK necesita ser acordada entre los dispositivos. Este procedimiento se denomina generalmente como cambio de claves. La GTK es habitualmente cambiada por un AP con bastante frecuencia, con fines de seguridad. Los cambios frecuentes de claves dan como resultado, en dispositivos que abandonan un Conjunto de Servicios Básicos (BSS), con el tiempo, la pérdida de su capacidad para decodificar el tráfico grupal desde el BSS. La PTK también se puede cambiar cuando el espacio de los Números de Paquete (PN) se agota, pero este es un suceso menos frecuente debido al gran tamaño del PN (6 octetos).

Con el fin de que el cambio de claves sea un suceso sin problemas, cada MPDU puede indicar una entre un cierto número de claves que se pueden utilizar en paralelo. Esto permite que pueda configurarse una nueva clave, mientras la vieja clave también pueda usarse para los paquetes sujetos a reintentos. La clave particular que se utiliza para proteger un paquete está indicada por el Identificador de Clave (Key ID). Como se muestra en la figura 4A, el Identificador de Clave está habitualmente incluido en la cabecera de MAC del paquete.

Ciertas normas (tales como la 802.11ah) pueden definir tramas con una cabecera corta de MAC, en la que el Identificador de Clave ya no está presente. La figura 4B ilustra una trama 400B de ese tipo, indicando con la "X" un campo omitido de Identificador de Clave. La falta de un campo de Identificador de Clave puede plantear un desafío con respecto a la selección y el cambio de claves (por ejemplo, según los dispositivos necesitan saber qué clave usar durante el cambio de claves).

En tales casos, puede haber una necesidad de que los dispositivos de transmisión y recepción establezcan qué claves están siendo utilizadas y permitan el establecimiento de nuevas claves, mediante un procedimiento de cambio de claves.

Los aspectos de la presente divulgación proporcionan técnicas que permiten a dispositivos, tanto transmisores como receptores, acordar un Identificador de Clave por defecto que pueda ser utilizado para la protección de las tramas con una cabecera corta de MAC, y que se use un procedimiento implícito de cambio de claves para conmutar a una nueva clave (reciente).

Por lo tanto, ciertos aspectos de la presente divulgación proporcionan técnicas que permiten a los dispositivos transmisores y receptores acordar un Identificador de Clave por defecto que se utiliza para la protección de las tramas con una cabecera corta de MAC, y que se use un procedimiento implícito de cambio de claves para conmutar a una nueva clave (reciente).

De acuerdo con ciertos aspectos, el procedimiento implícito de cambio de claves implica detener temporalmente el uso de tramas (400B) con una cabecera corta de MAC. Durante este tiempo, las tramas normales (por ejemplo, 400A) se envían con el Identificador de Clave actual. Se acuerdan entones una nueva clave y un nuevo Identificador de Clave (por ejemplo, utilizando establecimientos de comunicación de claves, nuevas o existentes). Una vez que se

han acordado la nueva clave y el nuevo Identificador de Clave, el Identificador de Clave por defecto para las tramas con una cabecera corta de MAC se convierte en el nuevo Identificador de Clave (activado por la negociación exitosa de una nueva clave y un nuevo Identificador de Clave), después de lo cual puede reanudarse el uso de tramas con una cabecera corta de MAC (sin Identificadores de Clave).

Un procedimiento implícito de cambio de claves de ese tipo para una PTK (tráfico de unidifusión) se puede ilustrar con el siguiente ejemplo. Antes de un procedimiento de cambio de claves, las tramas con una cabecera corta de MAC utilizan un Identificador de Clave por defecto para el tráfico de unidifusión (por ejemplo, el *Identificador de Clave 1).* En algún momento, el AP pretende cambiar la PTK. A partir de este momento, el AP puede dejar de usar tramas con cabeceras cortas de MAC y utilizar solamente tramas normales para el tráfico de unidifusión al destino específico, todavía con el *Identificador de Clave 1* (la PTK actual).

Durante el procedimiento de cambio de claves, el AP intercambia valores arbitrarios únicos con la STA para una nueva clave pareada; en este ejemplo, con el *Identificador de Clave 2.* De acuerdo con ciertos aspectos, el intercambio de valores arbitrarios únicos puede conmutar de forma implícita la clave pareada por defecto para cabeceras cortas de unidifusión, por el *Identificador de Clave 2.* Cuando el intercambio de valores arbitrarios únicos se ha realizado y la nueva PTK puede ser determinada por el AP y la STA, el AP conmuta a la nueva clave. La conmutación puede indicarse, ya sea mediante el uso de tramas normales de unidifusión con el *Identificador de Clave 2* o bien reanudando el uso de tramas con una cabecera corta de MAC (que ahora también utilizará el *Identificador de Clave 2).*

El procedimiento implícito de cambio de claves para la GTK (tráfico grupal) se ilustra en el siguiente ejemplo. En este ejemplo, una GTK por defecto para las tramas con una cabecera corta de MAC es el *Identificador de Clave 3*, antes de un procedimiento de cambio de claves. Una vez más, en algún momento, el AP pretende cambiar la GTK. A partir de este momento, el AP sólo utiliza tramas normales para el tráfico grupal, con el *Identificador de Clave 3* de la GTK (la GTK actual).

Durante el procedimiento de cambio de claves, el AP realiza establecimientos de comunicación para claves grupales con todas sus STA asociadas, para instalar la GTK con *Identificador de Clave 4* en las STA (por ejemplo, todas las estaciones objeto de las transmisiones grupales). Cada establecimiento de comunicación para claves grupales conmuta de forma implícita la clave grupal por defecto para las tramas con una cabecera corta de MAC, al nuevo *Identificador de Clave 4.*

Cuando se han realizado todos los establecimientos de comunicación para claves grupales, el AP conmuta a la nueva clave, ya sea mediante el uso de tramas grupales normales con *Identificador de Clave 4*, o bien mediante el uso de tramas grupales con una cabecera corta de MAC (que ahora también utilizará el *Identificador de Clave 4).*

La figura 5 es un diagrama de bloques de operaciones ejemplares 500 para comunicaciones inalámbricas por parte de un aparato de recepción, de acuerdo con aspectos de la presente divulgación. Las operaciones 500 pueden realizarse por un aparato, tal como una estación de recepción (RX-STA) implicada en una sesión con un punto de acceso (AP).

En 502, el aparato recibe paquetes cortos desde un dispositivo, careciendo dichos paquetes pequeños de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo. En 504, el aparato decodifica, usando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos.

En 506, el aparato participa en un procedimiento de cambio de claves con el dispositivo. En 508, el aparato decodifica, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

La figura 6 es un diagrama de bloques de operaciones ejemplares 600 para comunicaciones inalámbricas por parte de un aparato de transmisión, de acuerdo con aspectos de la presente divulgación. Las operaciones 600 pueden realizarse por un aparato de transmisión, tal como un punto de acceso implicado en una sesión con una estación de recepción.

En 602, el aparato codifica, usando un primer identificador de clave por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo. En 604, el aparato participa en un procedimiento de cambio de claves con el dispositivo. En 606, el aparato codifica, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves. En 608, el aparato transmite los primeros y segundos paquetes cortos.

Las diversas operaciones de los procedimientos descritos anteriormente pueden realizarse mediante cualquier medio adecuado capaz de realizar las funciones correspondientes. Los medios pueden incluir diversos componentes y/o módulos de hardware y/o software que incluyen, pero sin limitación, un circuito, un circuito integrado específico de la aplicación (ASIC) o un procesador. Generalmente, cuando hay operaciones ilustradas en figuras, estas

operaciones pueden tener componentes de medios y funciones homólogos correspondientes, con una numeración similar. Por ejemplo, las operaciones 500 y 600 ilustradas en las figuras 5 y 6 corresponden a los medios 500A y 600A ilustrados en las figuras 5A y 6A, respectivamente.

Por ejemplo, los medios de transmisión pueden comprender un transmisor (por ejemplo, la unidad transmisora 222) y/o una o más antenas 224 del punto de acceso 110 ilustrado en la figura 2, o el transmisor 310 y/o la antena o antenas 316 que se representan en la figura 3. Los medios de recepción pueden comprender un receptor (por ejemplo, la unidad receptora 222) y/o una o más antenas 224 del punto de acceso 110 ilustrado en la figura 2, o el receptor 312 y/o la antena o antenas 316 que se representan en la figura 3. Los medios de procesamiento, los medios de determinación, los medios de detección, los medios de exploración, los medios de selección o los medios de terminación de una operación pueden comprender un sistema de procesamiento, que puede incluir uno o más procesadores, tales como el procesador de datos de RX 242, el procesador de datos de TX 210 y/o el controlador 230 del punto de acceso 110 ilustrado en la figura 2, o el procesador 304 y/o el DSP 320 representado en la figura 3.

De acuerdo con ciertos aspectos, tales medios pueden implementarse por sistemas de procesamiento configurados para realizar las funciones correspondientes mediante la implementación de diversos algoritmos (por ejemplo, en hardware o mediante la ejecución de instrucciones de software) descritos anteriormente para la realización de la asociación rápida. Por ejemplo, los medios para recibir pueden incluir las unidades receptoras mostradas en las figuras 2 y 3, los medios para decodificar pueden implementarse por un sistema de procesamiento que realiza un algoritmo que recibe, como entrada, un paquete corto desde los medios de recepción y que decodifica el paquete corto usando un primer identificador de clave por defecto (previamente establecido), mientras que los medios para participar en un procedimiento de cambio de claves pueden implementarse por un sistema de procesamiento que realice un algoritmo (por ejemplo, el procesador de RX mostrado en la figura 2) para establecer un segundo Identificador de Clave por defecto para su uso posterior. De modo similar, los medios para codificar pueden ser implementados por un sistema de procesamiento (por ejemplo, uno de los procesadores que se muestran en las figuras 2 o 3) que realiza un algoritmo para codificar paquetes cortos utilizando un primer identificador de clave por defecto, y los medios para transmitir los paquetes cortos pueden ser implementados como cualquiera de las unidades transmisoras mostradas en las figuras 2 o 3.

Como se usa en el presente documento, el término "determinar" incluye una amplia variedad de acciones. Por ejemplo, "determinar" puede incluir calcular, computar, procesar, obtener, investigar, consultar (por ejemplo, consultar una tabla, una base de datos u otra estructura de datos), averiguar y similares. "Determinar" también puede incluir recibir (por ejemplo, recibir información), acceder (por ejemplo, acceder a datos en una memoria) y similares. "Determinar" también puede incluir resolver, seleccionar, elegir, establecer y similares.

Como se usa en el presente documento, una frase que hace referencia a "al menos uno de" una lista de elementos se refiere a cualquier combinación de tales elementos, incluyendo elementos individuales. Como ejemplo, "al menos uno de: *a, b* o *c*" pretende incluir: a, *b, c, a*-*b, a*-*c, b*-*c* y *a*-*b*-*c.*

Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con la presente divulgación pueden implementarse o realizarse con un procesador de propósito general, con un procesador de señales digitales (DSP), con un circuito integrado específico de la aplicación (ASIC), con una formación de compuertas programables en el terreno (FPGA) o con otro dispositivo de lógica programable (PLD), lógica de compuerta discreta o de transistor, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, micro-controlador o máquina de estados disponible en el mercado. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

Las etapas de un procedimiento o algoritmo descrito en relación con la presente divulgación pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo de software puede residir en cualquier forma de medio de almacenamiento conocido en la técnica. Algunos ejemplos de medios de almacenamiento que pueden usarse incluyen una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria flash, una memoria EPROM, una memoria EEPROM, registros, un disco duro, un disco extraíble, un CD-ROM, etc. Un módulo de software puede comprender una única instrucción o muchas instrucciones, y puede estar distribuido entre varios segmentos de código diferentes, entre diferentes programas y entre múltiples medios de almacenamiento. Un medio de almacenamiento puede estar acoplado al procesador de manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede ser una parte integrante del procesador.

Los procedimientos divulgados en el presente documento comprenden una o más etapas o acciones para realizar el procedimiento descrito. Las etapas de procedimiento y/o acciones pueden intercambiarse entre sí sin apartarse del alcance de las reivindicaciones. Dicho de otro modo, a no ser que se indique un orden específico de etapas o acciones, el orden y/o uso de etapas y/o acciones específicas pueden modificarse sin apartarse del alcance de las

reivindicaciones.

Las funciones descritas pueden implementarse en hardware, software, firmware o cualquier combinación de los mismos. Si se implementan en hardware, una configuración de hardware ejemplar puede comprender un sistema de procesamiento en un nodo inalámbrico. El sistema de procesamiento puede implementarse con una arquitectura de bus. El bus puede incluir cualquier número de buses y puentes de interconexión según la aplicación específica del sistema de procesamiento y las restricciones de diseño globales. El bus puede vincular entre sí varios circuitos, incluyendo un procesador, medios legibles por máquina y una interfaz de bus. La interfaz de bus puede usarse para conectar un adaptador de red, entre otras cosas, al sistema de procesamiento a través del bus. El adaptador de red puede usarse para implementar las funciones de procesamiento de señales de la capa PHY. En el caso de un terminal de usuario 120 (véase la figura 1), también puede conectarse una interfaz de usuario (por ejemplo, un teclado, una pantalla, un ratón, una palanca de control, etc.) al bus. El bus también puede vincular otros diversos circuitos tales como fuentes de temporización, periféricos, reguladores de voltaje, circuitos de gestión de potencia y similares, que son ampliamente conocidos en la técnica y, por lo tanto, no serán descritos en mayor detalle.

El procesador puede ser responsable de gestionar el bus y el procesamiento general, incluyendo la ejecución de software almacenado en los medios legibles por máquina. El procesador puede implementarse con uno o más procesadores de propósito general y/o de propósito especial. Los ejemplos incluyen microprocesadores, micro-controladores, procesadores DSP y otros sistemas de circuitos que pueden ejecutar software. El término 'software' deberá interpretarse en sentido amplio, como instrucciones, datos o cualquier combinación de los mismos, ya sea mencionados como software, firmware, middleware, micro-código, lenguaje de descripción de hardware o de otro modo. Los medios legibles por máquina pueden incluir, a modo de ejemplo, RAM (memoria de acceso aleatorio), memoria flash, ROM (memoria de sólo lectura), PROM (memoria programable de sólo lectura), EPROM (memoria programable borrable de sólo lectura), EEPROM (memoria programable de sólo lectura, eléctricamente borrable), registros, discos magnéticos, discos ópticos, discos duros o cualquier otro medio de almacenamiento adecuado o cualquier combinación de los mismos. Los medios legibles por máquina pueden realizarse en un producto de programa informático. El producto de programa informático puede comprender materiales de embalaje.

En una implementación en hardware, los medios legibles por máquina pueden formar parte del sistema de procesamiento, independientemente del procesador. Sin embargo, como apreciarán fácilmente los expertos en la técnica, los medios legibles por máquina, o cualquier parte de los mismos, pueden ser externos al sistema de procesamiento. A modo de ejemplo, los medios legibles por máquina pueden incluir una línea de transmisión, una onda portadora modulada mediante datos y/o un producto informático independiente del nodo inalámbrico, donde el procesador pueda acceder a todos ellos a través de la interfaz de bus. Como alternativa, o además, los medios legibles por máquina, o cualquier parte de los mismos, pueden integrarse en el procesador, tal como puede ser el caso con la memoria caché y/o los ficheros de registro generales.

El sistema de procesamiento puede configurarse como un sistema de procesamiento de propósito general con uno o más microprocesadores que proporcionan la funcionalidad del procesador y una memoria externa que proporciona al menos una parte de los medios legibles por máquina, todos ellos conectados entre sí con otro sistema de circuitos de soporte a través de una arquitectura de bus externa. Como alternativa, el sistema de procesamiento puede implementarse con un ASIC (circuito integrado específico de la aplicación), con el procesador, la interfaz de bus, la interfaz de usuario en el caso de un terminal de acceso, el sistema de circuitos de soporte y al menos una parte de los medios legibles por máquina integrados en un único chip, o con una o más FPGA (matrices de compuertas de campo programable), PLD (dispositivos de lógica programable), controladores, máquinas de estados, lógica de compuertas, componentes de hardware discretos o cualquier otro sistema de circuitos adecuado, o cualquier combinación de circuitos que pueda realizar la diversa funcionalidad descrita a lo largo de esta divulgación. Los expertos en la técnica reconocerán el mejor modo de implementar la funcionalidad descrita para el sistema de procesamiento en función de la aplicación particular y las restricciones de diseño global impuestas al sistema global.

Los medios legibles por máquina pueden comprender diversos módulos de software. Los módulos de software incluyen instrucciones que, cuando son ejecutadas por el procesador, hacen que el sistema de procesamiento lleve a cabo varias funciones. Los módulos de software pueden incluir un módulo de transmisión y un módulo de recepción. Cada módulo de software puede residir en un único dispositivo de almacenamiento o puede estar distribuido entre múltiples dispositivos de almacenamiento. A modo de ejemplo, un módulo de software puede cargarse en una RAM desde un disco duro cuando se produce un suceso de activación. Durante la ejecución del módulo de software, el procesador puede cargar parte de las instrucciones en caché para aumentar la velocidad de acceso. Una o más líneas de caché pueden cargarse entonces en un fichero de registro general para su ejecución mediante el procesador. Cuando se haga referencia posteriormente a la funcionalidad de un módulo de software, deberá entenderse que tal funcionalidad es implementada por el procesador cuando ejecuta instrucciones de ese módulo de software.

Si se implementan en software, las funciones pueden almacenarse o transmitirse como una o más instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informáticos como medios de comunicación, incluyendo cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible

al que pueda accederse mediante un ordenador. A modo de ejemplo, y no de manera limitativa, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Además, cualquier conexión puede denominarse de manera adecuada un medio legible por ordenador. Por ejemplo, si el software se transmite desde una sede de la Red, un servidor u otro origen remoto, usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos (IR), radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas tales como infrarrojos, radio y microondas se incluyen en la definición de medio. Los discos, como se usan en el presente documento, incluyen discos compactos (CD), discos de láser, discos ópticos, discos versátiles digitales (DVD), discos flexibles y discos Blu-ray®, donde algunos discos normalmente reproducen datos de manera magnética, mientras que otros discos reproducen los datos ópticamente con láser. Por lo tanto, en algunos aspectos, los medios legibles por ordenador pueden comprender medios legibles por ordenador no transitorios (por ejemplo, medios tangibles). Además, en otros aspectos, los medios legibles por ordenador pueden comprender medios transitorios legibles por ordenador (por ejemplo, una señal). Las combinaciones de lo anterior también deberían incluirse dentro del alcance de los medios legibles por ordenador.

Por lo tanto, determinados aspectos pueden comprender un producto de programa informático para realizar las operaciones presentadas en el presente documento. Por ejemplo, tal producto de programa informático puede comprender un medio legible por ordenador que tenga instrucciones almacenadas (y/o codificadas) en el mismo, siendo las instrucciones ejecutables por uno o más procesadores para realizar las operaciones descritas en el presente documento. En determinados aspectos, el producto de programa informático puede incluir material de embalaje.

Además, debería apreciarse que los módulos y/u otros medios adecuados para realizar los procedimientos y las técnicas descritos en el presente documento pueden descargarse y/u obtenerse de otro modo por medio de un terminal de usuario y/o una estación base, según corresponda. Por ejemplo, un dispositivo de este tipo puede estar acoplado a un servidor para facilitar la transferencia de medios para realizar los procedimientos descritos en el presente documento. Como alternativa, pueden proporcionarse diversos procedimientos descritos en el presente documento mediante medios de almacenamiento (por ejemplo, RAM, ROM, un medio de almacenamiento físico tal como un disco compacto (CD) o un disco flexible, etc.), de modo que un terminal de usuario y/o una estación base puedan obtener los diversos procedimientos al acoplar o al proporcionar los medios de almacenamiento al dispositivo. También puede utilizarse cualquier otra técnica adecuada para proporcionar los procedimientos y técnicas descritos en el presente documento a un dispositivo.

Debe entenderse que las reivindicaciones no están limitadas a la configuración y componentes precisos ilustrados anteriormente. Diversas modificaciones, cambios y variaciones pueden realizarse en la disposición, el funcionamiento y los detalles de los procedimientos y aparatos descritos anteriormente sin apartarse del alcance de las reivindicaciones.

A continuación se describen ejemplos adicionales para facilitar el entendimiento de la invención:

1. Un aparato para comunicaciones inalámbricas, que comprende:

un receptor configurado para recibir paquetes cortos desde un dispositivo, careciendo dichos paquetes cortos de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo; y

un decodificador configurado para:

decodificar, usando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos,

participar en un procedimiento de cambio de claves con el dispositivo, y

decodificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

2. El aparato del ejemplo 1, en el que, durante el procedimiento de cambio de claves, el aparato recibe paquetes adicionales desde el dispositivo, que incluyen un campo de identificador de clave.

3. El aparato del ejemplo 2, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

4. El aparato del ejemplo 2, en el que el decodificador está configurado además para determinar que el procedimiento de cambio de claves está completo después de recibir más paquetes cortos que carecen de un

campo de identificador de clave.

5. El aparato del ejemplo 1, en el que el decodificador está configurado además para determinar el segundo Identificador de Clave por defecto, en base a la recepción de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto.

6. Un aparato para comunicaciones inalámbricas, que comprende:

un codificador configurado para:

codificar, usando un primer identificador de clave por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo,

participar en un procedimiento de cambio de claves con el dispositivo y codificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves; y

un transmisor configurado para transmitir los primeros y segundos paquetes cortos.

7. El aparato del ejemplo 6, en el que, durante el procedimiento de cambio de claves, el aparato transmite paquetes al dispositivo, que incluyen un campo de identificador de clave.

8. El aparato del ejemplo 7, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

9. El aparato del ejemplo 7, en el que el aparato está configurado para indicar que el procedimiento de cambio de claves está completo, mediante la transmisión de los segundos paquetes cortos que carecen de un campo de identificador de clave.

10. El aparato del ejemplo 6, en el que el aparato está configurado para indicar el segundo Identificador de Clave por defecto, en base a la transmisión de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto.

11. El aparato según la reivindicación 6, en el que:

los primeros y segundos paquetes cortos se codifican utilizando una Clave Pareada Transitoria (PTK).

12. El aparato según la reivindicación 6, en el que:

los primeros y segundos paquetes cortos se codifican utilizando una Clave Grupal Temporal (GTK).

13. Un procedimiento para comunicaciones inalámbricas por parte de un aparato, que comprende:

recibir paquetes cortos desde un dispositivo, careciendo dichos paquetes cortos de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo;

decodificar, utilizando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos;

participar en un procedimiento de cambio de claves con el dispositivo; y

decodificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

14. El procedimiento del ejemplo 13, en el que, durante el procedimiento de cambio de claves, el aparato recibe paquetes adicionales desde el dispositivo, que incluyen un campo de identificador de clave.

15. El procedimiento del ejemplo 14, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

16. El procedimiento del ejemplo 14, que comprende además determinar que el procedimiento de cambio de claves está completo después de recibir más paquetes cortos que carecen de un campo de identificador de clave.

17. El procedimiento del ejemplo 13, que comprende además determinar el segundo Identificador de Clave por defecto, en base a la recepción de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto.

18. Un procedimiento para comunicaciones inalámbricas por parte de un aparato, que comprende:

codificar, usando un primer identificador de clave por defecto, primeros paquetes cortos que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo;

participar en un procedimiento de cambio de claves con el dispositivo;

codificar, utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves; y

transmitir los primeros y segundos paquetes cortos.

19. El procedimiento del ejemplo 18, en el que, durante el procedimiento de cambio de claves, el aparato transmite paquetes al dispositivo, que incluyen un campo de identificador de clave.

20. El procedimiento del ejemplo 19, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

21. El procedimiento del ejemplo 19, que comprende además indicar que el procedimiento de cambio de claves está completo, mediante la transmisión de los segundos paquetes cortos que carecen de un campo de identificador de clave.

22. El procedimiento del ejemplo 18, que comprende además indicar el segundo Identificador de Clave por defecto, en base a la transmisión de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto.

23. El procedimiento del ejemplo 18, en el que:

los primeros y segundos paquetes cortos se codifican utilizando una Clave Pareada Transitoria (PTK).

24. El procedimiento del ejemplo 18, en el que:

los primeros y segundos paquetes cortos se codifican utilizando una Clave Grupal Temporal (GTK).

REIVINDICACIONES

1. Un aparato para comunicaciones inalámbricas, que comprende:

un receptor (502A) configurado para recibir paquetes cortos (400B) desde un dispositivo, careciendo dichos paquetes cortos (400B) de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo; y

un decodificador configurado para:

decodificar (504A), utilizando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos 10,

participar (506A) en un procedimiento de cambio de claves con el dispositivo, en el que, durante el procedimiento de cambio de claves, el aparato recibe paquetes adicionales desde el dispositivo, que incluyen un campo de identificador de clave,

determinar un segundo Identificador de Clave por defecto, en base a la recepción de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto, y

decodificar (508A), utilizando el segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

2. El aparato de la reivindicación 1, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

3. El aparato de la reivindicación 1, en el que el decodificador está configurado además para determinar que el procedimiento de cambio de claves está completo después de recibir más paquetes cortos que carecen de un campo de identificador de clave.

4. Un aparato para comunicaciones inalámbricas, que comprende:

un codificador configurado para:

codificar (602A), utilizando un primer identificador de clave por defecto, primeros paquetes cortos (400B) que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo,

participar (604A) en un procedimiento de cambio de claves con el dispositivo, y codificar (606A), utilizando un segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves, en el que, durante el procedimiento de cambio de claves, el aparato transmite paquetes al dispositivo, que incluyen un campo de identificador de clave; y

un transmisor (608A) configurado para transmitir los primeros y segundos paquetes cortos, donde el aparato está configurado para indicar el segundo Identificador de Clave por defecto, en base a la transmisión de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto.

5. El aparato de la reivindicación 4, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

6. El aparato de la reivindicación 4, en el que el aparato está configurado para indicar que el procedimiento de cambio de claves está completo mediante la transmisión de los segundos paquetes cortos que carecen de un campo de identificador de clave.

7. Un procedimiento (500) para comunicaciones inalámbricas por parte de un aparato, que comprende:

recibir (502) paquetes cortos (400B) desde un dispositivo, careciendo dichos paquetes cortos (400B) de un campo de identificador de clave que identifique una clave acordada entre el aparato y el dispositivo;

decodificar (504), utilizando un primer identificador de clave por defecto, algunos de los paquetes cortos recibidos;

participar (506) en un procedimiento de cambio de claves con el dispositivo, en el que, durante el

procedimiento de cambio de claves, el aparato recibe paquetes adicionales desde el dispositivo, que incluyen un campo de identificador de clave;

determinar un segundo Identificador de Clave por defecto, en base a la recepción de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto; y

decodificar (508), utilizando el segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, algunos de los paquetes cortos recibidos después del procedimiento de cambio de claves.

8. El procedimiento de la reivindicación 7, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

9. El procedimiento de la reivindicación 7, que comprende además determinar que el procedimiento de cambio de claves está completo después de recibir más paquetes cortos que carecen de un campo de identificador de clave.

10. Un procedimiento (600) para comunicaciones inalámbricas por parte de un aparato, que comprende:

codificar (602), usando un primer identificador de clave por defecto, primeros paquetes cortos (400B) que carecen de un campo de identificador de clave que identifique una clave acordada entre el aparato y un dispositivo;

participar (604) en un procedimiento de cambio de claves con el dispositivo, en el que, durante el procedimiento de cambio de claves, el aparato transmite paquetes al dispositivo, que incluyen un campo de identificador de clave;

indicar un segundo Identificador de Clave por defecto, en base a la transmisión de un paquete que incluye un campo de identificador de clave fijado en el segundo Identificador de Clave por defecto;

codificar (606), utilizando el segundo Identificador de Clave por defecto, establecido durante el procedimiento de cambio de claves, segundos paquetes cortos que carecen del identificador de clave después del procedimiento de cambio de claves; y

transmitir (608) los primeros y segundos paquetes cortos.

11. El procedimiento de la reivindicación 10, en el que el campo de identificador de clave identifica el primer identificador de clave por defecto.

12. El procedimiento de la reivindicación 10, que comprende además indicar que el procedimiento de cambio de claves está completo mediante la transmisión de los segundos paquetes cortos que carecen de un campo de identificador de clave.

13. El procedimiento de la reivindicación 10, en el que:

los primeros y segundos paquetes cortos se codifican utilizando una Clave Pareada Transitoria, PTK.

14. El procedimiento de la reivindicación 10, en el que:

los primeros y segundos paquetes cortos se codifican utilizando una Clave Grupal Temporal, GTK.

15. Un programa informático que incluye instrucciones ejecutables para hacer que al menos un ordenador realice un procedimiento según una de las reivindicaciones 7 a 9, o 10 a 14, cuando se ejecuta.

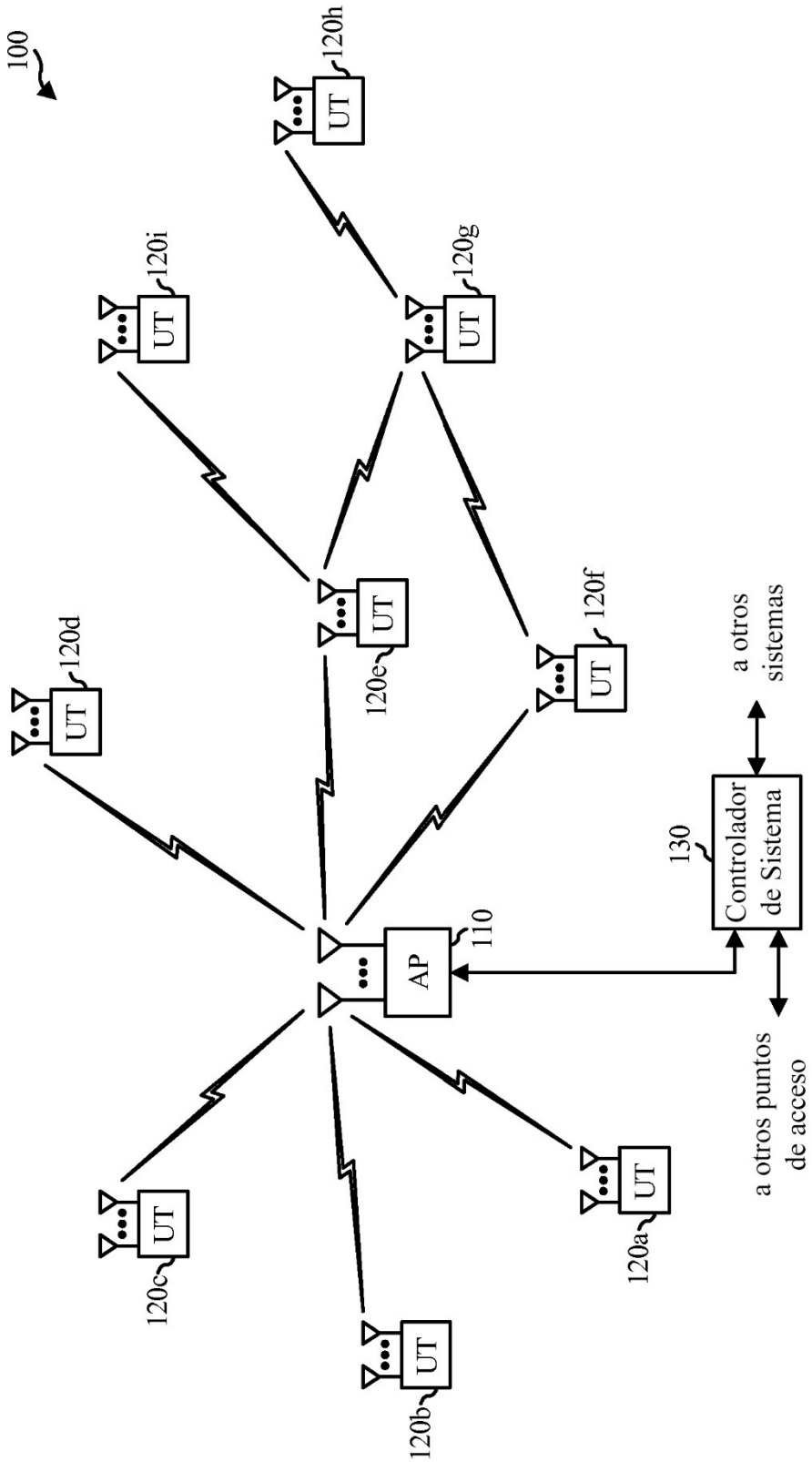
100
120h
UT
120i
UT
120g
UT
120d
UT
120e
UT
120f
UT
AP
110
130
Controlador de Sistema
a otros sistemas
a otros puntos de acceso
120c
UT
120b
UT
120a
UT

FIG. 1

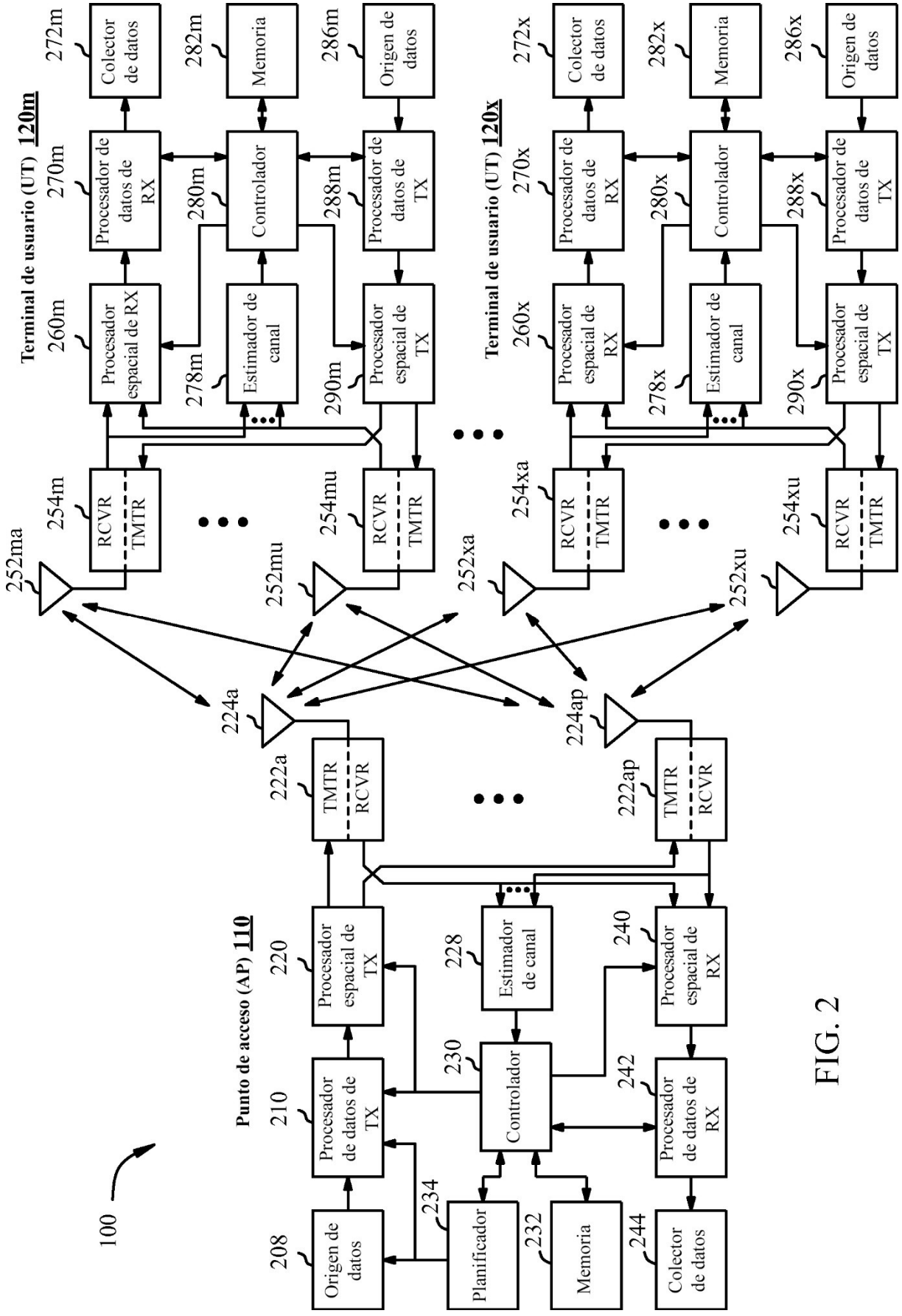
100
Punto de acceso (AP) 110
208 Origen de datos
210 Procesador de datos de TX
220 Procesador espacial de TX
222a TMTR RCVR
222ap TMTR RCVR
224a
224ap
228 Estimador de canal
230 Controlador
232 Memoria
234 Planificador
240 Procesador espacial de RX
242 Procesador de datos de RX
244 Colector de datos
252ma
252mu
252xa
252xu
254m RCVR TMTR
254mu RCVR TMTR
254xa RCVR TMTR
254xu RCVR TMTR
Terminal de usuario (UT) 120m
260m Procesador espacial de RX
270m Procesador de datos de RX
272m Colector de datos
278m Estimador de canal
280m Controlador
282m Memoria
286m Origen de datos
288m Procesador de datos de TX
290m Procesador espacial de TX
Terminal de usuario (UT) 120x
260x Procesador espacial de RX
270x Procesador de datos de RX
272x Colector de datos
278x Estimador de canal
280x Controlador
282x Memoria
286x Origen de datos
288x Procesador de datos de TX
290x Procesador espacial de TX

FIG. 2

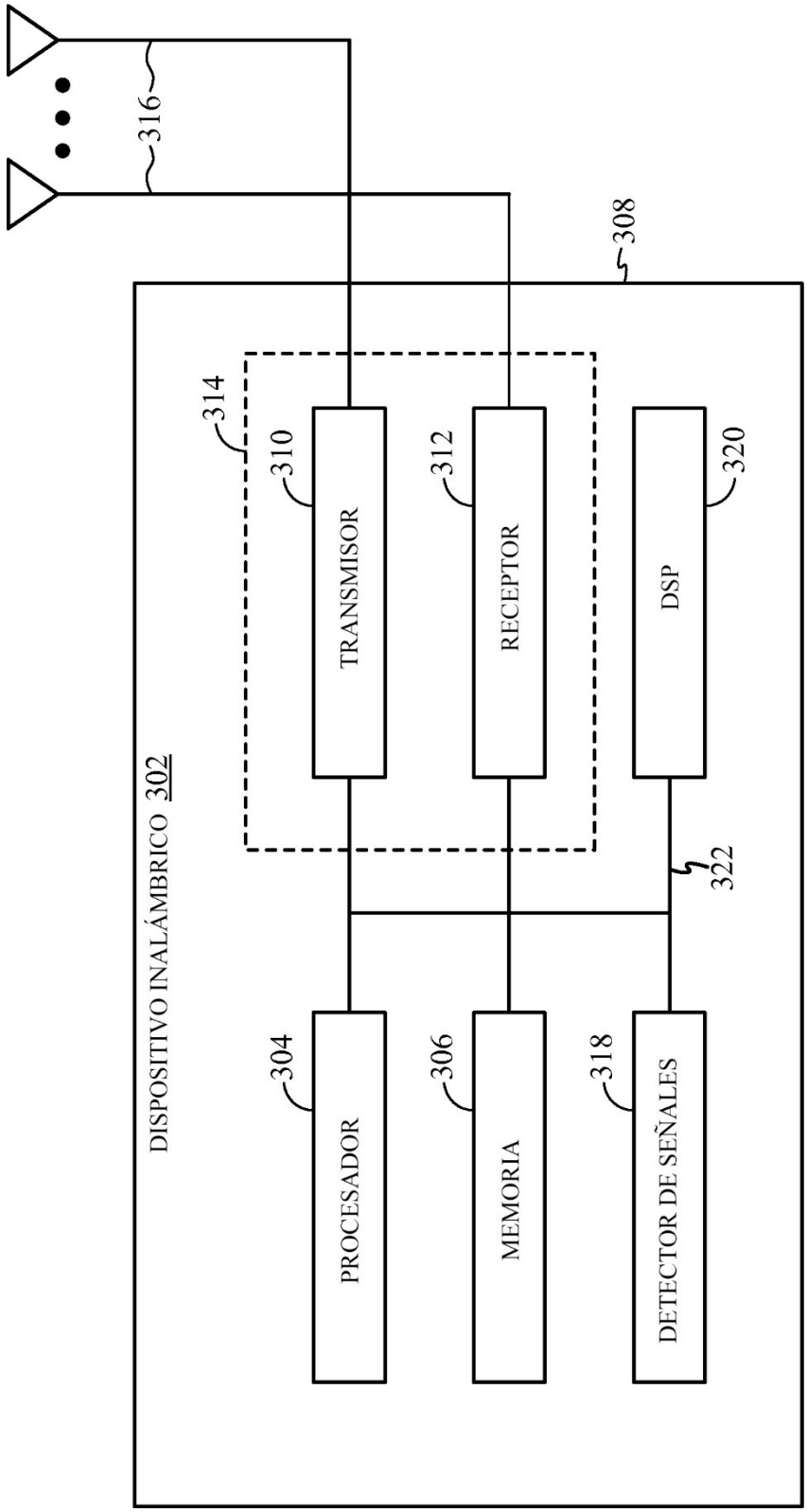
316
308
DISPOSITIVO INALÁMBRICO 302
314
310
TRANSMISOR
312
RECEPTOR
320
DSP
322
304
PROCESADOR
306
MEMORIA
318
DETECTOR DE SEÑALES

FIG. 3

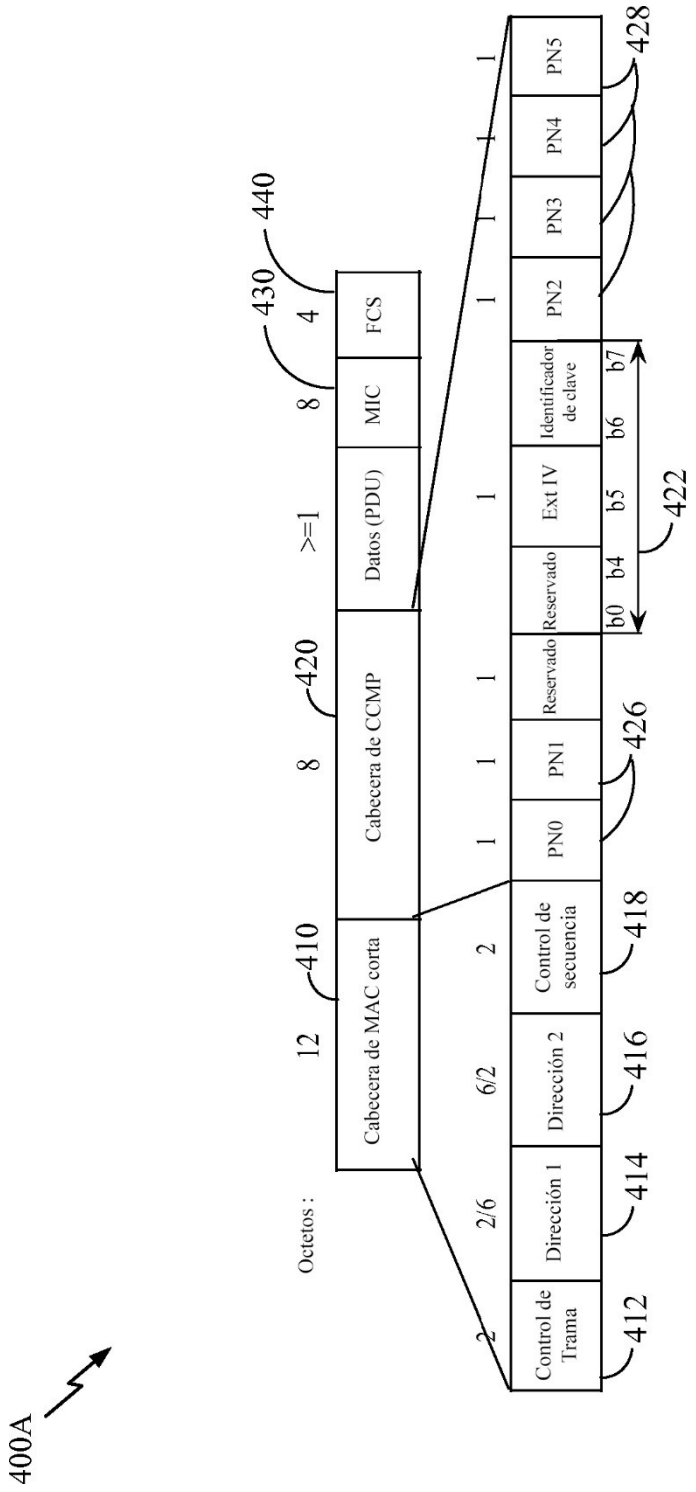
400A
Octetos :
12
2/6
6/2
2
1
1
1
1
1
1
1
1
1
1
8
>=1
8
4
Cabecera de MAC corta
Dirección 1
Dirección 2
Control de secuencia
PN0
PN1
Reservado
Reservado
Ext IV
Identificador de clave
PN2
PN3
PN4
PN5
Cabecera de CCMP
Datos (PDU)
MIC
FCS
b0
b4
b5
b6
b7
410
412
414
416
418
420
422
426
428
430
440

FIG. 4A

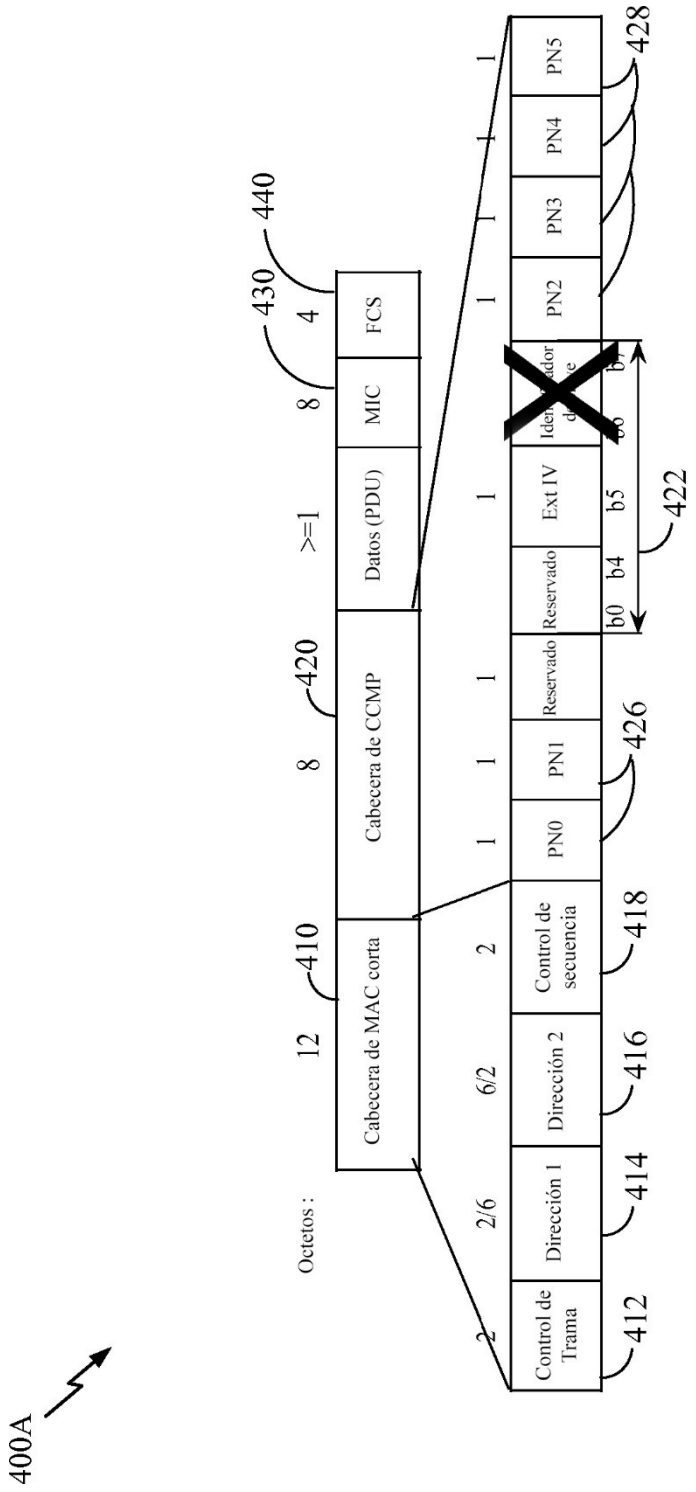
400A
Octetos :
12
2/6
6/2
2
1
1
1
1
1
1
1
1
1
1
1
1
8
>=1
8
4
2
Cabecera de MAC corta
Dirección 1
Dirección 2
Control de secuencia
PN0
PN1
Reservado
Reservado
Ext IV
Identificador de clave
PN2
PN3
PN4
PN5
Cabecera de CCMP
Datos (PDU)
MIC
FCS
Control de Trama
410
414
416
418
426
422
428
420
430
440
412
b0
b4
b5
b7

FIG. 4B

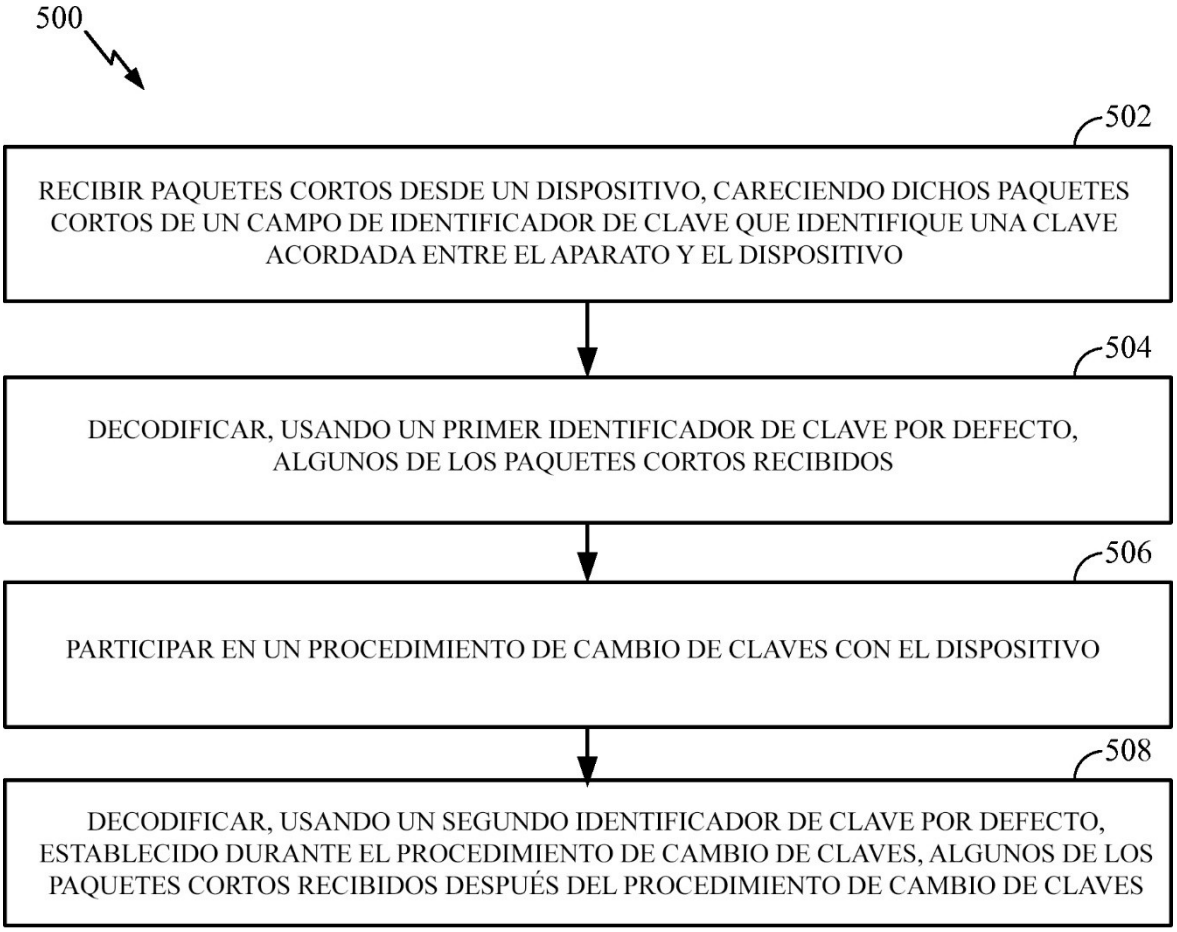
500
502
RECIBIR PAQUETES CORTOS DESDE UN DISPOSITIVO, CARECIENDO DICHOS PAQUETES CORTOS DE UN CAMPO DE IDENTIFICADOR DE CLAVE QUE IDENTIFIQUE UNA CLAVE ACORDADA ENTRE EL APARATO Y EL DISPOSITIVO
504
DECODIFICAR, USANDO UN PRIMER IDENTIFICADOR DE CLAVE POR DEFECTO, ALGUNOS DE LOS PAQUETES CORTOS RECIBIDOS
506
PARTICIPAR EN UN PROCEDIMIENTO DE CAMBIO DE CLAVES CON EL DISPOSITIVO
508
DECODIFICAR, USANDO UN SEGUNDO IDENTIFICADOR DE CLAVE POR DEFECTO, ESTABLECIDO DURANTE EL PROCEDIMIENTO DE CAMBIO DE CLAVES, ALGUNOS DE LOS PAQUETES CORTOS RECIBIDOS DESPUÉS DEL PROCEDIMIENTO DE CAMBIO DE CLAVES

FIG. 5

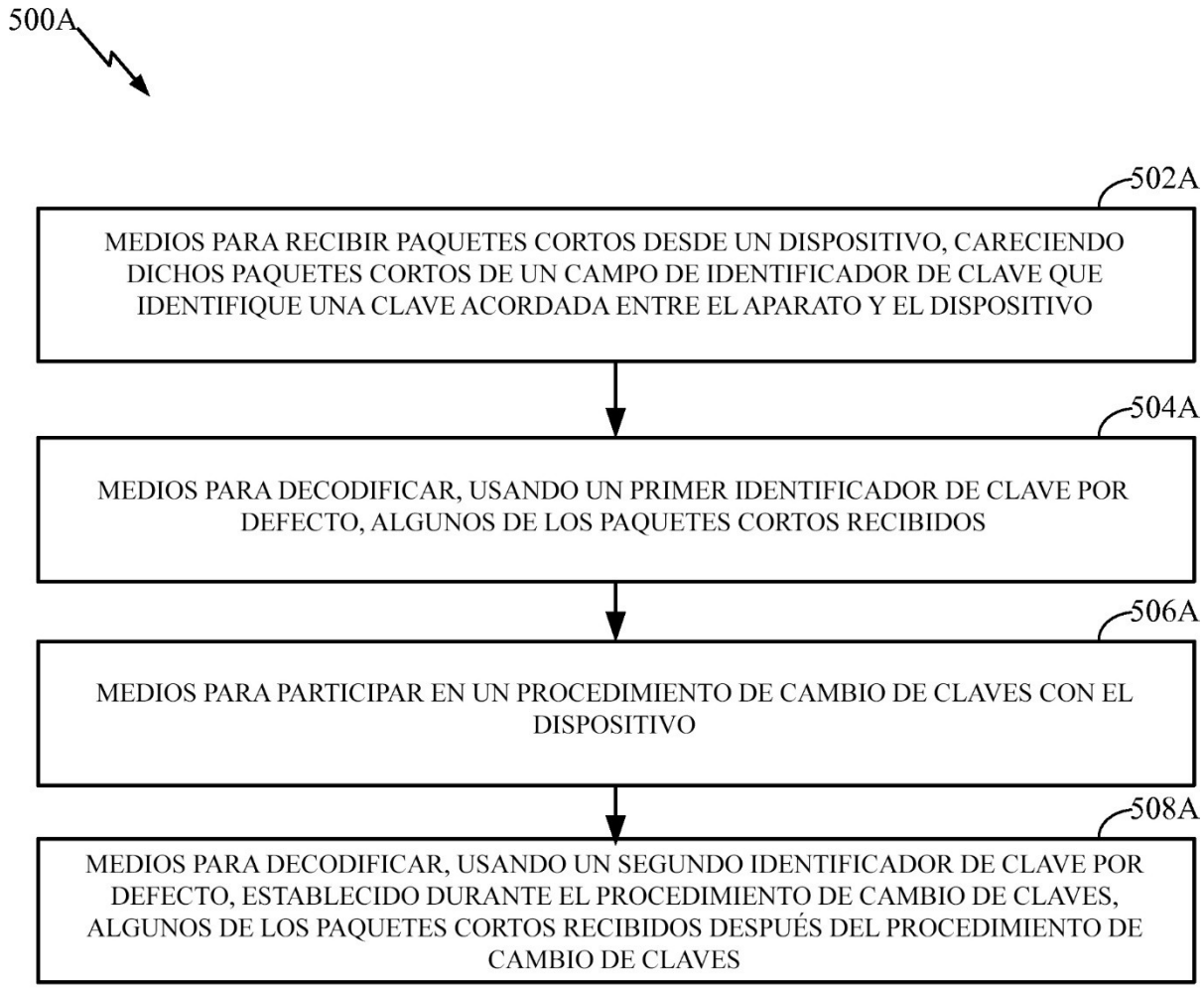
500A
502A
MEDIOS PARA RECIBIR PAQUETES CORTOS DESDE UN DISPOSITIVO, CARECIENDO DICHOS PAQUETES CORTOS DE UN CAMPO DE IDENTIFICADOR DE CLAVE QUE IDENTIFIQUE UNA CLAVE ACORDADA ENTRE EL APARATO Y EL DISPOSITIVO
504A
MEDIOS PARA DECODIFICAR, USANDO UN PRIMER IDENTIFICADOR DE CLAVE POR DEFECTO, ALGUNOS DE LOS PAQUETES CORTOS RECIBIDOS
506A
MEDIOS PARA PARTICIPAR EN UN PROCEDIMIENTO DE CAMBIO DE CLAVES CON EL DISPOSITIVO
508A
MEDIOS PARA DECODIFICAR, USANDO UN SEGUNDO IDENTIFICADOR DE CLAVE POR DEFECTO, ESTABLECIDO DURANTE EL PROCEDIMIENTO DE CAMBIO DE CLAVES, ALGUNOS DE LOS PAQUETES CORTOS RECIBIDOS DESPUÉS DEL PROCEDIMIENTO DE CAMBIO DE CLAVES

FIG. 5A

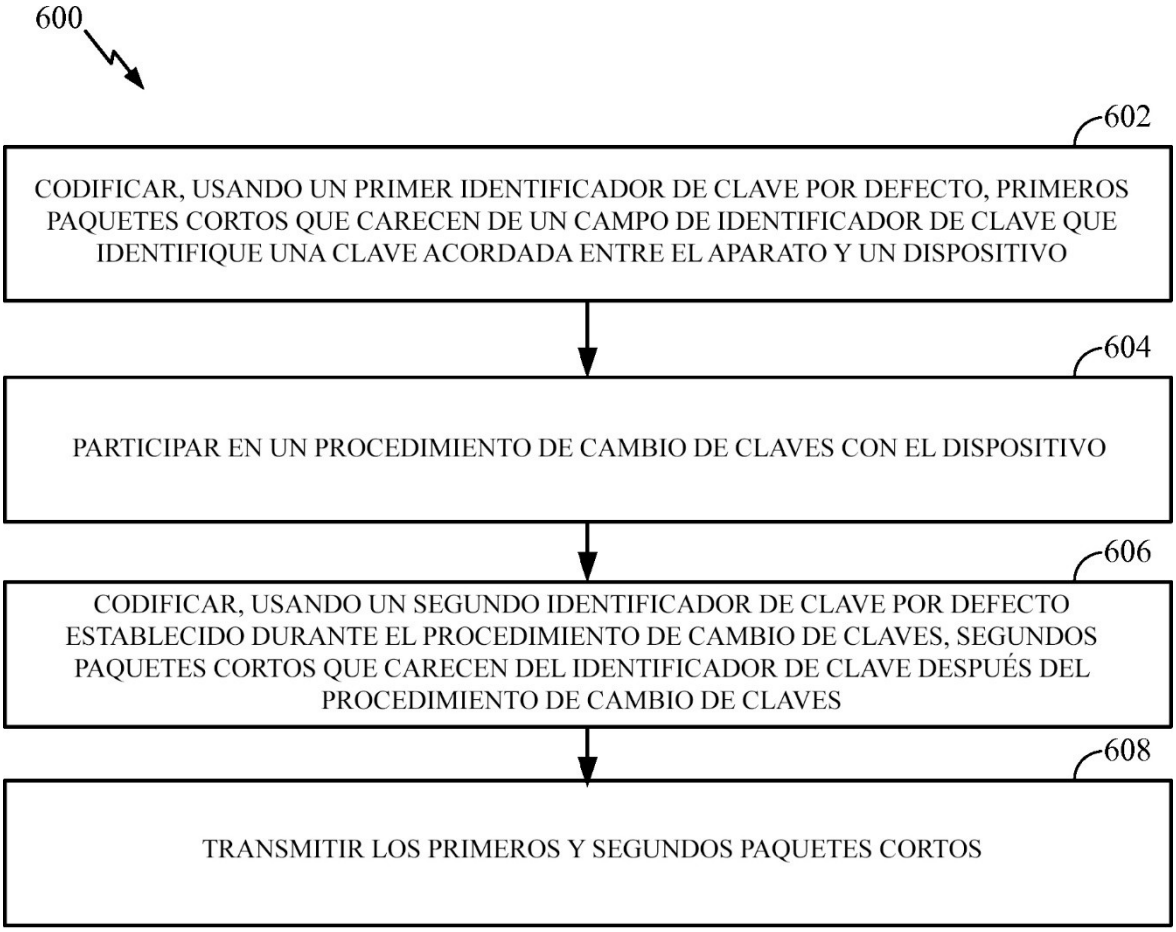
600
602
CODIFICAR, USANDO UN PRIMER IDENTIFICADOR DE CLAVE POR DEFECTO, PRIMEROS PAQUETES CORTOS QUE CARECEN DE UN CAMPO DE IDENTIFICADOR DE CLAVE QUE IDENTIFIQUE UNA CLAVE ACORDADA ENTRE EL APARATO Y UN DISPOSITIVO
604
PARTICIPAR EN UN PROCEDIMIENTO DE CAMBIO DE CLAVES CON EL DISPOSITIVO
606
CODIFICAR, USANDO UN SEGUNDO IDENTIFICADOR DE CLAVE POR DEFECTO ESTABLECIDO DURANTE EL PROCEDIMIENTO DE CAMBIO DE CLAVES, SEGUNDOS PAQUETES CORTOS QUE CARECEN DEL IDENTIFICADOR DE CLAVE DESPUÉS DEL PROCEDIMIENTO DE CAMBIO DE CLAVES
608
TRANSMITIR LOS PRIMEROS Y SEGUNDOS PAQUETES CORTOS

FIG. 6

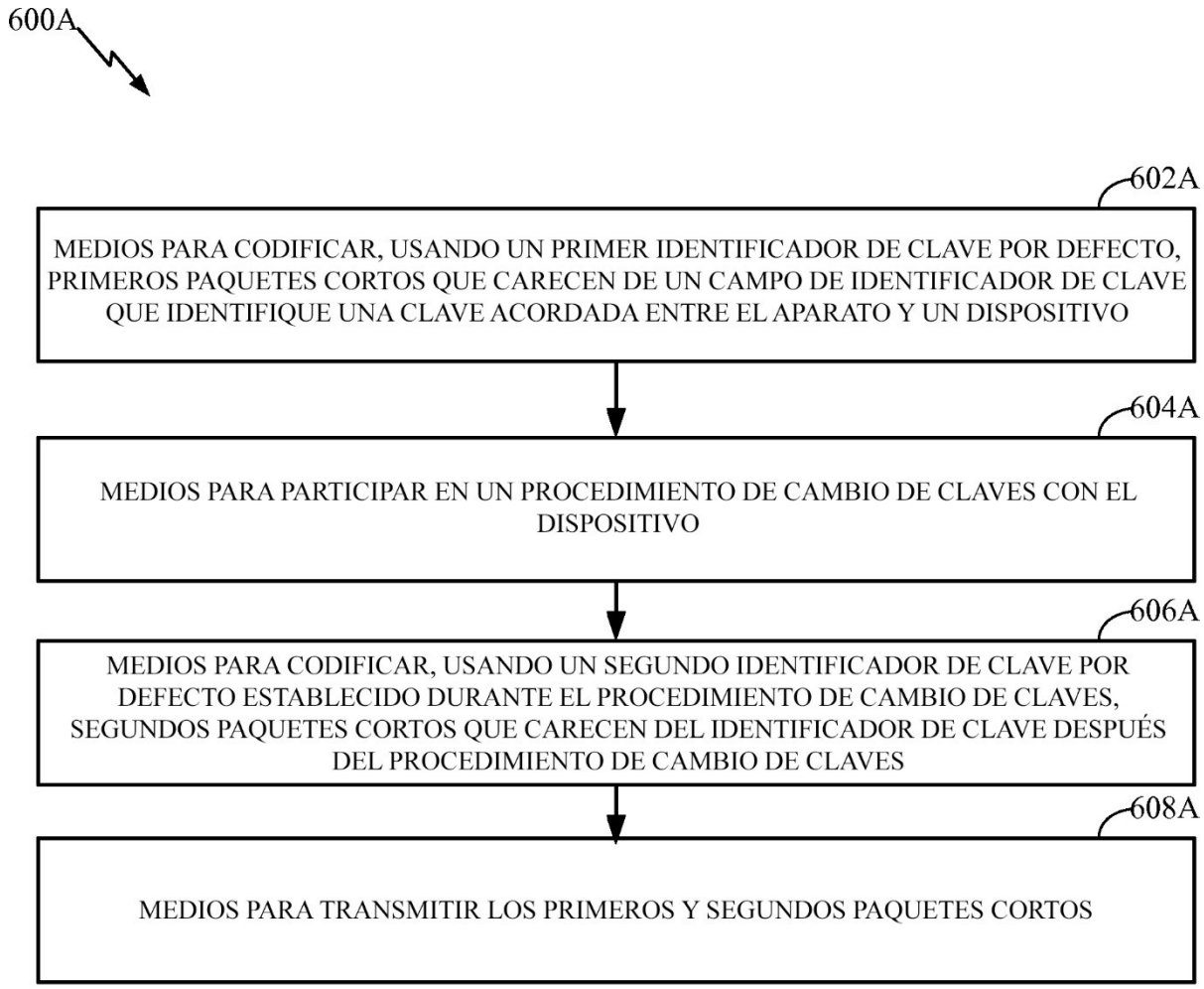
600A
602A
MEDIOS PARA CODIFICAR, USANDO UN PRIMER IDENTIFICADOR DE CLAVE POR DEFECTO, PRIMEROS PAQUETES CORTOS QUE CARECEN DE UN CAMPO DE IDENTIFICADOR DE CLAVE QUE IDENTIFIQUE UNA CLAVE ACORDADA ENTRE EL APARATO Y UN DISPOSITIVO
604A
MEDIOS PARA PARTICIPAR EN UN PROCEDIMIENTO DE CAMBIO DE CLAVES CON EL DISPOSITIVO
606A
MEDIOS PARA CODIFICAR, USANDO UN SEGUNDO IDENTIFICADOR DE CLAVE POR DEFECTO ESTABLECIDO DURANTE EL PROCEDIMIENTO DE CAMBIO DE CLAVES, SEGUNDOS PAQUETES CORTOS QUE CARECEN DEL IDENTIFICADOR DE CLAVE DESPUÉS DEL PROCEDIMIENTO DE CAMBIO DE CLAVES
608A
MEDIOS PARA TRANSMITIR LOS PRIMEROS Y SEGUNDOS PAQUETES CORTOS

FIG. 6A