(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 634 412**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 12/10 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.12.2013 PCT/US2013/074614**

(87) Fecha y número de publicación internacional: **19.06.2014 WO14093597**

(96) Fecha de presentación y número de la solicitud europea: **12.12.2013 E 13815894 (4)**

(97) Fecha y número de publicación de la concesión europea: **17.05.2017 EP 2932754**

(54) Título: **Seguridad para paquetes que usen un encabezado mac corto**

(30) Prioridad:

12.12.2012 US 201261736513 P
15.03.2013 US 201313840166

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.09.2017

(73) Titular/es:

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

(72) Inventor/es:

ASTERJADHI, ALFRED;
WENTINK, MAARTEN, MENZO y
MERLIN, SIMONE

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Seguridad para paquetes que usen un encabezado mac corto

Campo de la invención

Ciertos aspectos de la presente divulgación se refieren generalmente a comunicaciones inalámbricas y, más particularmente, a técnicas para activar la sobrecarga para paquetes que usen un encabezado mac corto

Antecedentes relevantes

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

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

El documento WO 2009/098572 A1 divulga que la eficiencia de la comunicación puede mejorarse usando encabezados comprimidos. En un modo de realización de ejemplo de dicha técnica anterior, se realiza un procedimiento mediante un dispositivo de transmisión para reducir el tamaño del encabezado. Se crea una asignación entre un identificador de canal lógico y un identificador de canal lógico comprimido. El identificador de canal lógico comprimido ocupa menos bits que el identificador de canal lógico. La asignación se transmite a un dispositivo receptor. Se formula un encabezado comprimido que incluye el identificador de canal lógico comprimido. Una comunicación que incluye el encabezado comprimido se transmite al dispositivo receptor. En otro modo de realización de ejemplo, un procedimiento se realiza mediante un dispositivo receptor para decodificar un encabezado que tenga un tamaño reducido. Se reciben una asignación y una comunicación que incluyen un encabezado comprimido. Se extrae un identificador de canal lógico comprimido del encabezado comprimido. Se recupera un identificador de canal lógico del identificador de canal lógico comprimido usando la asignación.

El documento WO 2012/159082 A2 describe sistemas, procedimientos y se describen en el presente documento dispositivos para comunicar paquetes que tengan una pluralidad de tipos. En algunos aspectos, los paquetes incluyen un encabezado MAC comprimido. En algunos aspectos, los paquetes incluyen una trama de reconocimiento. Los campos incluidos en un tipo de paquete particular pueden basarse en el tipo de información que haya de comunicarse al dispositivo receptor.

Todavía existe una necesidad de una forma más eficiente de manejar los encabezados.

La presente invención proporciona una solución de acuerdo con la materia objeto de las reivindicaciones independientes.

SUMARIO

Ciertos aspectos de la presente divulgación proporcionan un aparato de comunicación inalámbrica. El aparato incluye típicamente un sistema de procesamiento configurado generalmente para almacenar localmente una porción de un conjunto de información, en el aparato, recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información, y decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

Ciertos aspectos de la presente divulgación proporcionan un aparato de comunicación inalámbrica. El aparato incluye típicamente un sistema de procesamiento configurado para señalar, a una entidad receptora, una porción de un conjunto de información usada para codificar una porción de datos de un paquete y transmitir, a la entidad receptora, un paquete con el campo de datos codificado usando el conjunto de información, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

Ciertos aspectos de la presente divulgación proporcionan un aparato de comunicación inalámbrica. El aparato incluye típicamente medios para almacenar localmente una porción de un conjunto de información, en el aparato, medios para recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de

información, y medios para decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

Ciertos aspectos de la presente divulgación proporcionan un aparato de comunicación inalámbrica. El aparato incluye típicamente medios para señalar, a una entidad receptora, una porción de un conjunto de información usada para codificar una porción de datos de un paquete y medios para transmitir, a la entidad receptora, un paquete con el campo de datos codificado usando el conjunto de información, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

Ciertos aspectos de la presente divulgación proporcionan un procedimiento para comunicaciones inalámbricas por un aparato. El procedimiento incluye típicamente almacenar localmente una porción de un conjunto de información, en el aparato, recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información, y decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

Ciertos aspectos de la presente divulgación proporcionan un procedimiento para comunicaciones inalámbricas por un aparato. El procedimiento incluye típicamente señalizar, a una entidad receptora, una porción de un conjunto de información usada para codificar una porción de datos de un paquete y transmitir, a la entidad receptora, un paquete con el campo de datos codificado usando el conjunto de información, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

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 para almacenar localmente una porción de un conjunto de información, en el aparato, recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información, y decodificar el campo de datos usando la porción almacenada del conjunto de Información adicional contenido en el paquete.

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 para señalar, a una entidad receptora, una porción de un conjunto de información usado para codificar una porción de datos de un paquete y transmitir, a la entidad receptora, un paquete con el campo de datos codificado usando el conjunto de información, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

Ciertos aspectos de la presente divulgación proporcionan una estación para comunicaciones inalámbricas. La estación incluye típicamente un sistema de procesamiento configurado generalmente para almacenar localmente una porción de un conjunto de información, en la estación, recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información, y decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

Ciertos aspectos de la presente divulgación proporcionan un punto de acceso para comunicaciones inalámbricas. El punto de acceso incluye típicamente un sistema de procesamiento configurado para señalar, a una estación, una porción de un conjunto de información usada para codificar una porción de datos de un paquete y transmitir, a la estación, un paquete con el campo de datos codificado usando el conjunto de información, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos. La invención es como se define en las reivindicaciones adjuntas 1-15.

BREVE DESCRIPCIÓN DE LOS DIBUJOS:

De modo que la manera en la cual se mencionaron anteriormente las características de la presente divulgación pueda entenderse con detalle, se ofrece una descripción más particular, resumida brevemente anteriormente, con referencia a sus aspectos, algunos de los cuales se ilustran en los dibujos adjuntos. Sin embargo, cabe señalarse que los dibujos adjuntos ilustran solamente ciertos aspectos típicos de esta divulgación y, por lo tanto, no han de considerarse limitativos de su alcance, ya que la descripción puede admitir otros aspectos igualmente eficaces.

La FIG. 1 ilustra un diagrama de una red de comunicaciones inalámbricas de ejemplo, de acuerdo con ciertos aspectos de la presente divulgación.

La FIG. 2 ilustra un diagrama de bloques de un punto de acceso y terminales de usuario de ejemplo, de acuerdo con ciertos aspectos de la presente divulgación.

La FIG. 3 ilustra un diagrama de bloques de un dispositivo inalámbrico de ejemplo, de acuerdo con ciertos aspectos de la presente divulgación.

La FIG. 4 ilustra una estructura de paquetes de ejemplo que utiliza un encabezado MAC corto.

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

La FIG. 5A ilustra medios de ejemplo capaces de realizar las operaciones mostradas en la FIG. 5.

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

La FIG. 6A ilustra medios de ejemplo capaces de realizar las operaciones mostradas en la FIG. 6.

La FIG. 7 ilustra una estructura de paquetes de ejemplo con un encabezado CCMP comprimido, de acuerdo con aspectos de la presente divulgación.

La FIG. 7A ilustra un encabezado CCMP comprimido de ejemplo, de acuerdo con aspectos de la presente divulgación.

La FIG. 8 ilustra otra estructura de paquetes de ejemplo con un encabezado CCMP comprimido, de acuerdo con aspectos de la presente divulgación.

La FIG. 8A ilustra un encabezado CCMP comprimido de ejemplo, de acuerdo con aspectos de la presente divulgación.

La FIG. 9 ilustra una estructura de paquetes de ejemplo sin ningún encabezado CCMP, de acuerdo con aspectos de la presente divulgación.

DESCRIPCIÓN DETALLADA

Diversos aspectos de la divulgación se describen de aquí en adelante con más detalle con referencia a los dibujos adjuntos. Sin embargo, esta divulgación puede realizarse de muchas formas diferentes y no debería interpretarse como limitada a ninguna estructura ni función específica presentada a lo largo de esta divulgación. En cambio, estos aspectos se proporcionan de modo que esta divulgación será exhaustiva y completa y transmitirá por completo el alcance de la divulgación a los expertos en la técnica. En base a las enseñanzas en el presente documento, un experto en la técnica debería apreciar que el alcance de la divulgación pretende abarcar cualquier aspecto de la divulgación divulgado en el presente documento, ya sea implementado de forma independiente de o combinado 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 expuestos en el presente documento. Además, el alcance de la divulgación está prevista para abarcar dicho aparato o procedimiento, que se lleva a la práctica usando otra estructura, funcionalidad o estructura y funcionalidad, además de o diferente 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 por uno o más elementos de una reivindicación.

Aunque en el presente documento se describen aspectos particulares, muchas variaciones y permutaciones de estos aspectos quedan 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 previstos para ser ampliamente aplicables a tecnologías inalámbricas diferentes, configuraciones de sistema, redes y protocolos de transmisión, algunos de los cuales se ilustran a modo de ejemplo en las figuras y en la descripción siguiente de los aspectos preferidos. La descripción detallada y los dibujos son meramente ilustrativos de la divulgación en vez de limitativos, estando definido el alcance de la divulgación por las reivindicaciones adjuntas y por los equivalentes de las mismas.

UN SISTEMA DE COMUNICACIÓN INALÁMBRICA DE EJEMPLO

Las técnicas descritas en el presente documento pueden usarse para diversos sistemas de comunicación inalámbrica de banda ancha, incluyendo sistemas de comunicación que estén basados en un sistema de multiplexado ortogonal. Los ejemplos de dichos sistemas de comunicación incluyen sistemas de acceso múltiple por división espacial (SDMA), de acceso múltiple por división de tiempo (TDMA), sistemas de acceso múltiple por división ortogonal de frecuencia (OFDMA), sistemas de acceso múltiple por división de frecuencia de portadora única (SC-FDMA), etc. Un sistema SDMA puede utilizar direcciones suficientemente diferentes para transmitir de forma simultánea datos que pertenezcan a múltiples terminales de usuario. Un sistema TDMA puede permitir que múltiples terminales de usuario compartan el mismo canal de frecuencia, dividiendo la señal de transmisión en ranuras temporales diferentes, estando asignada cada ranura temporal a terminales de usuario diferentes. Un sistema OFDMA utiliza el multiplexado por división ortogonal de frecuencia (OFDM), que es una técnica de modulación que divide el ancho de banda global del sistema en múltiples subportadoras ortogonales. Estas subportadoras pueden denominarse también tonos, colectores, etc. Con el OFDM, cada subportadora puede modularse de forma independiente con datos. Un sistema SC-FDMA puede utilizar el FDMA entrelazado (IFDMA) para transmitir en

subportadoras que estén distribuidas a través del ancho de banda del sistema, el FDMA localizado (LFDMA) para transmitir en un bloque de subportadoras adyacentes o el FDMA mejorado (EFDMA) para transmitir en múltiples bloques de subportadoras adyacentes. En general, los símbolos de modulación se envían en el dominio de frecuencia con el OFDM y en el dominio de tiempo con el SC-FDMA.

Las enseñanzas en el presente documento pueden incorporarse en (por ejemplo, implementarse dentro de o realizarse por) una variedad de aparatos cableados o inalámbricos (por ejemplo, nodos). En algunos aspectos, un nodo inalámbrico implementado de acuerdo con 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 radioeléctrica (“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 router 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 con 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 con alguna otra terminología. En algunas implementaciones, un terminal de acceso puede comprender un teléfono móvil, un teléfono sin cables, un teléfono de protocolo de inicio de sesión ("SIP"), una estación de bucle local inalámbrico ("WLL"), un asistente digital personal ("PDA"), un dispositivo manual con capacidad que tenga conexión inalámbrica, una estación ("STA") o algún otro dispositivo de procesamiento adecuado conectado a un módem inalámbrico. Por consiguiente, uno o más aspectos enseñados en el presente documento pueden incorporarse a un teléfono (por ejemplo, un teléfono móvil o un smartphone), un ordenador (por ejemplo, un ordenador portátil), una tablet, 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 posicionamiento 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. Dicho nodo inalámbrico puede proporcionar, por ejemplo, conectividad para o a una red (por ejemplo, una red de área extensa tal como Internet o una red móvil) a través de un enlace de comunicación cableada o inalámbrica.

La FIG. 1 ilustra un sistema de acceso múltiple de múltiples entradas y múltiples salidas (MIMO) 100 con puntos de acceso y terminales de usuario. Por motivos de simplicidad, solamente se muestra un punto de acceso 110 en la FIG. 1. Un punto de acceso es generalmente una estación fija que se comunica con los terminales de usuario y que puede denominarse también estación base o con alguna otra terminología. Un terminal de usuario puede ser fijo o móvil y puede denominarse también estación móvil, dispositivo inalámbrico o con 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 puede comunicarse también entre pares con otro terminal de usuario. Un controlador de sistema 130 se acopla a y proporciona coordinación y control para los puntos de acceso.

Aunque porciones de la divulgación siguiente describirán terminales de usuario 120 capaces de comunicarse a través del acceso múltiple por división espacial (SDMA), para ciertos aspectos, los terminales de usuario 120 pueden incluir también algunos terminales de usuario que no den soporte al SDMA. Por lo tanto, para dichos aspectos, un AP 110 puede estar configurado para comunicarse con terminales de usuario, tanto SDMA como no SDMA. Este enfoque puede permitir de forma conveniente que versiones anteriores de terminales de usuario (estaciones "heredadas") permanezcan desplegadas en una empresa, ampliando su vida útil, permitiendo a la vez que se introduzcan nuevos terminales de usuario SDMA según se considere adecuado.

El sistema 100 emplea múltiples antenas de transmisión y múltiples antenas de recepción 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 el 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 TDMA, canales de código diferentes con CDMA, conjuntos disjuntos de subbandas 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 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 TDD, el enlace descendente y el enlace ascendente comparten la misma banda de frecuencia. Para un sistema FDD, el enlace descendente y el enlace ascendente usan bandas de frecuencia diferentes. El sistema MIMO 100 puede utilizar también una única portadora o múltiples portadoras para su transmisión. Cada terminal de usuario puede estar equipado con una única antena (por ejemplo, con el fin de mantener bajos los costes) o múltiples antenas (por ejemplo, donde pueda soportarse el coste adicional). El sistema 100 puede ser también un sistema TDMA si los terminales de usuario 120 comparten el mismo canal de frecuencia dividiendo la transmisión/recepción en ranuras temporales diferentes, estando cada ranura temporal asignada a un terminal de usuario 120 diferente.

La FIG. 2 ilustra un diagrama de bloques del punto de acceso 110 y dos terminales de usuario 120m y 120x en el sistema 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 transmisora para el enlace descendente y una entidad receptora para el enlace ascendente. Cada terminal de usuario 120 es una entidad transmisora para el enlace ascendente y una entidad receptora para el enlace descendente. Como se usa en el presente documento, una "entidad transmisora" es un aparato o dispositivo autónomo capaz de transmitir datos a través de un canal inalámbrico y una "entidad receptora" es un aparato o dispositivo autónomo capaz de recibir datos a través de un canal inalámbrico. En la descripción siguiente, el subíndice "*dn*" indica el enlace descendente, el subíndice "*up*" indica el enlace ascendente, se seleccionan N_{up} terminales de usuario para una transmisión simultánea en el enlace ascendente, se seleccionan N_{dn} terminales de usuario para una 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 en 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 una fuente de datos 286 y datos de control desde un controlador 280. El procesador de datos TX 288 procesa (por ejemplo, codifica, entrelaza y modula) los datos de tráfico para el terminal de usuario en base a los sistemas de codificación y modulación asociados con la velocidad seleccionada para el terminal de usuario y proporciona un flujo de símbolos de datos. Un procesador espacial 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 transmisora (TMTR) 254 recibe y procesa (por ejemplo, convierte a analógico, amplifica, filtra y aumenta de frecuencia) un flujo de símbolos de transmisión respectivo para generar una señal de enlace ascendente. $N_{ut,m}$ unidades transmisoras 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 una transmisión simultánea en el enlace ascendente. Cada uno de estos terminales de usuario realiza 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 unidad receptora (RCVR) 222 respectiva. Cada unidad receptora 222 realiza un procesamiento complementario al realizado por la unidad transmisora 254 y proporciona un flujo de símbolos recibidos. Un procesador espacial RX 240 realiza un procesamiento espacial de recepción en los N_{ap} flujos de símbolos recibidos desde las N_{ap} unidades receptoras 222 y proporciona N_{up} flujos recuperados de símbolos de datos de enlace ascendente. El procesamiento espacial de recepción se realiza de acuerdo con la inversión matricial de correlación de canal (CCMI), con el mínimo error cuadrático medio (MMSE), con la cancelación suave de interferencias (SIC) o con 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 terminal de usuario respectivo. Un procesador de datos RX 242 procesa (por ejemplo, demodula, desentrelaza y decodifica) cada flujo recuperado de símbolos de datos de enlace ascendente, de acuerdo con 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 otro procesamiento.

En el enlace descendente, en el punto de acceso 110, un procesador de datos TX 210 recibe datos de tráfico desde una fuente de datos 208 para N_{dn} terminales de usuario planificados para la transmisión de 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 canales de transporte diferentes. El procesador de datos TX 210 procesa (por ejemplo, codifica, entrelaza y modula) los datos de tráfico para cada terminal de usuario en base a la velocidad seleccionada para ese terminal de usuario. El procesador de datos TX 210 proporciona N_{dn} flujos de símbolos de datos de enlace descendente para los N_{dn} terminales de usuario. Un procesador espacial TX 220 realiza un procesamiento espacial (tal como una precodificación 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 transmisora 222 recibe y procesa un flujo de símbolos de transmisión respectivo para generar una señal de enlace descendente. N_{ap} unidades transmisoras 222 proporcionan N_{ap} señales de enlace descendente

para la 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 receptora 254 procesa una señal recibida desde una antena 252 asociada y proporciona un flujo de símbolos recibido. Un procesador espacial RX 260 realiza un procesamiento espacial receptor en los $N_{ut,m}$ flujos de símbolos recibidos desde $N_{ut,m}$ unidades receptoras 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 de acuerdo con la CCMI, con el MMSE o con alguna otra técnica. Un procesador de datos RX 270 procesa (por ejemplo, demodula, desentrelaza 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 SNR, varianza de ruido, etc. De manera similar, 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 típicamente la matriz de filtro espacial para el terminal de usuario en base a 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 en base a 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 retroalimentación (por ejemplo, los autovectores, los autovalores, 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 diversas unidades de procesamiento en el punto de acceso 110 y en el terminal de usuario 120, respectivamente.

La FIG. 3 ilustra diversos componentes que pueden utilizarse en un dispositivo inalámbrico 302 que puede emplearse dentro del sistema 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 controle el funcionamiento del dispositivo inalámbrico 302. El procesador 304 puede denominarse también unidad central de procesamiento (CPU). La memoria 306, que puede incluir tanto memoria de solo lectura (ROM) como memoria de acceso aleatorio (RAM) proporciona instrucciones y datos al procesador 304. Una porción de la memoria 306 puede incluir también memoria de acceso aleatorio no volátil (NVRAM). El procesador 304 realiza típicamente operaciones lógicas y aritméticas en base a 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 puede incluir también 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 transmisoras 316, puede(n) fijarse al alojamiento 308 y acoplarse de forma eléctrica al transceptor 314. El dispositivo inalámbrico 302 puede incluir también múltiples transmisores, múltiples receptores y múltiples transceptores (no mostrados).

El dispositivo inalámbrico 302 puede incluir también un detector de señales 318 que pueda 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 subportadora por símbolo, densidad espectral de potencia y otras señales. El dispositivo inalámbrico 302 puede incluir también un procesador de señales digitales (DSP) 320 para su uso en el procesamiento de señales.

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

SEGURIDAD DE EJEMPLO PARA PAQUETES CON ENCABEZADOS MAC CORTOS

El uso de estructuras de paquetes con encabezados MAC cortos (comprimidos relativos a los encabezados MAC completos) se ha aceptado en ciertas normas, tales como IEEE 802.11ah. El encabezado MAC corto definido en 802.11ah se reduce a 12 bytes a partir de los 34 bytes de un encabezado MAC normal. Un número reducido de bits en los encabezados MAC cortos permite la reducción de la sobrecarga y es especialmente beneficioso para los paquetes de datos cortos donde la sobrecarga representa un porcentaje mayor del tamaño general del paquete.

Las técnicas presentadas en el presente documento proporcionan técnicas para reducir la sobrecarga de paquetes cifrados, tales como los que usan encabezados MAC cortos. Las técnicas presentadas en el presente documento proporcionan diversas opciones para reducir la sobrecarga asociada con el cifrado por paquete. Estas técnicas pueden usarse por separado o, en algunos casos, combinarse para lograr mayores reducciones en la sobrecarga.

La FIG. 4 ilustra un ejemplo de un paquete 400 (en el ejemplo ilustrado, una MPDU) con un encabezado MAC corto 410, pero un encabezado CCMP completo 420. Como se ilustra, el encabezado MAC 420 que contiene la dirección de destino y de origen del paquete de datos y un encabezado CCMP con un número de paquete (PN), una Ext IV y un ID de clave. Como se ilustra, el número de paquete es un número de 48 bits almacenado en 6 octetos (como se ilustra, los códigos PN son los primeros dos octetos y los últimos cuatro octetos del encabezado CCMP 420) y se incrementan para cada paquete posterior. El octeto de ID de Clave 422 puede contener el Ext IV (bit 5), el ID de Clave (bits 6-7) y un subcampo reservado (bits 0-4).

Esta información en el encabezado CCMP se usa para cifrar la unidad de datos y el código de integridad de mensaje (MIC) que protege la integridad y la autenticidad del paquete. No se cifra a secuencia de verificación de trama (FCS) que se usa para la detección y la corrección de errores.

Las técnicas presentadas en el presente documento pueden ayudar a reducir la sobrecarga asociada con la transmisión de un encabezado CCMP. De acuerdo con ciertos aspectos, parte de la información CCMP (llevada convencionalmente en un encabezado CCMP completo) puede almacenarse en el receptor. Por ejemplo, si se almacenan los 4 bytes superiores del PN, el encabezado CCMP puede reducirse en 4 bytes. Además, o como alternativa, pueden extraerse campos innecesarios (reservados) (1 Byte). Otras técnicas discutidas a continuación pueden dar como resultado reducciones adicionales.

La FIG. 5 es un diagrama de bloques de operaciones 500 de ejemplo para comunicaciones inalámbricas por una entidad receptora, de acuerdo con aspectos de la presente divulgación. Las operaciones 500 pueden realizarse por un aparato, tal como una estación o un punto de acceso.

En 502, el aparato almacena una porción de una información de protocolo de modo de cifrado de contador (CCMP) localmente, en el aparato. En 504, el aparato recibe un paquete con un encabezado MAC, una indicación de un tipo del encabezado MAC y un campo de datos cifrado usando la información CCMP. En 506, el aparato descifra el campo de datos usando la porción almacenada de la información CCMP y la información adicional contenida en el paquete.

La FIG. 6 es un diagrama de bloques de operaciones 600 de ejemplo para comunicaciones inalámbricas por una entidad transmisora, de acuerdo con aspectos de la presente divulgación. Las operaciones 600 pueden realizarse por un aparato, tal como una estación o un punto de acceso.

En 602, el aparato señala una porción de una información de protocolo de modo de cifrado de contador (CCMP) a una entidad receptora, que vaya a almacenarse en la entidad receptora. En 604, el aparato transmite un paquete con un encabezado MAC, una indicación de un tipo del encabezado MAC y un campo de datos cifrado usando la información CCMP, en donde el paquete carece de parte de la información CCMP usada para cifrar el campo de datos.

La FIG. 7 ilustra un paquete 700 de ejemplo con un encabezado CCMP corto (comprimido) 720, de acuerdo con aspectos de la presente divulgación.

Como se ilustra, es posible realizar la compresión de encabezado CCMP definiendo una PN base (en el ejemplo ilustrado, BPN = PN2 | PN3 | PN4 | PN5). La BPN puede almacenarse en la entidad receptora y puede obtenerse a través del intercambio de tramas de gestión. De acuerdo con ciertos aspectos, puede enviarse una porción restante del encabezado CCMP con el paquete (por ejemplo, con los bits menos significativos de la PN enviada y la ID de clave, PN0 | PN1 | ID de clave). Esto puede denominarse PN de paquete (PPN).

A partir de esta información, junto con la información almacenada, puede reconstruirse la información de encabezado CCMP completa en el receptor. Por ejemplo, la PN completa puede reconstruirse a partir de la PPN (transmitida) y de la BPN (almacenada) como: PN = concatenar PPN | BPN. La BPN puede ser necesaria para actualizarse tras el vuelco PN0 | PN1. Se espera que un vuelco basado en 16 bits sea muy bajo para las aplicaciones 802.11ah y puede detectarse en el receptor (y la BPN actualizarse en consecuencia).

Como se muestra en la FIG. 7A, usando este enfoque, un encabezado CCMP se redujo de 8 Octetos a 3 Octetos ya que solamente PN0 | PN1 | Octetos de ID de Clave deben transmitirse junto con el paquete.

La FIG. 8 ilustra un paquete 800 de ejemplo con otro ejemplo de un encabezado CCMP corto 820, de acuerdo con aspectos de la presente divulgación.

Como se ilustra, es posible realizar una compresión de encabezado CCMP aún más eficiente. Esta compresión adicional puede ser posible, por ejemplo, permitiendo que un número de control de secuencia (SC) transmitido (en el encabezado MAC) actúe como PN0 | PN1. En otras palabras, PN0 | PN1 = SC (= Número de Secuencia (SN) | Número de Fragmento (FN)). En algunos casos, el número de paquete aumenta con etapas de 16 cuando la MSDU no está fragmentada. Como resultado, la PN puede reducirse de forma efectiva en 4 bits.

Como se ilustra en la FIG. 8A, este enfoque puede dar como resultado un encabezado CCMP que se reduzca a solamente 1 Octeto, ya que solamente el Octeto de ID de clave tiene que transmitirse con el paquete.

Como se ilustra en la FIG. 9, incluso puede ser posible enviar un paquete sin ningún encabezado CCMP en absoluto (como se indica por un encabezado CCMP vacío 920). Esta compresión adicional puede ser posible extrayendo el octeto de ID de Clave. Esto puede ser posible porque el valor de Ext IV (incluido en el octeto de ID de Clave) es siempre 1 para CCMP. Además, como la reencripción nunca puede producirse para el tráfico de unidifusión y el tráfico de grupo no usa encabezados MAC cortos, puede omitirse el ID de Clave también. Como resultado, el encabezado CCMP se elimina básicamente del encabezado MAC corto. En este caso, (los LSB de) el número de paquete puede determinarse a partir del número de control de secuencia SC, por ejemplo, como PN0 | PN1 = SC).

Como se describe en el presente documento, almacenando una porción de información CCMP (por ejemplo, PN2 I PN3 | PN4 | PN5) del encabezado CCMP como una PN de base en el receptor (por ejemplo, obtenida a través del intercambio de tramas de gestión), puede reducirse sustancialmente la sobrecarga del encabezado CCMP. De acuerdo con ciertos aspectos, un Octeto de un campo Rsvd del encabezado CCMP puede extraerse cuando se use con un encabezado MAC corto. Además, el campo ID de clave del encabezado CCMP puede almacenarse en el receptor (y obtenerse a través de un intercambio de tramas de gestión) cuando se use con un encabezado MAC corto. La reencripción puede lograrse mediante el uso temporal de tramas normales con un encabezado MAC normal y la clave actual, mientras se negocia una nueva clave. Cuando se ha negociado la nueva clave (y la ID de Clave), puede convertirse en la clave (e ID de Clave) que se usa para el encabezado MAC corto y puede retomarse el uso de encabezados MAC cortos.

De acuerdo con algunos, el campo de control de secuencia del encabezado MAC corto puede usarse como PN0 | PN1 del encabezado CCMP cuando se use con un encabezado MAC corto.

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 componente(s) y/o módulo(s) de hardware y/o software que incluyan, pero sin limitación, un circuito, un circuito integrado específico de la aplicación (ASIC) o un procesador. Generalmente, donde hayan operaciones ilustradas en figuras, esas operaciones pueden tener componentes de medios y funciones homólogos correspondientes, con una numeración similar. Por ejemplo, las operaciones 500 y 600 ilustradas en las FIGS. 5 y 6 corresponden a los medios 500A y 600A ilustrados en las FIGS. 5A y 6A, respectivamente.

Por ejemplo, los medios de transmisión pueden comprender un transmisor (por ejemplo, la unidad transmisora 222) y/o una(s) antena(s) 224 del punto de acceso 110 ilustrado en la FIG. 2 o el transmisor 310 y/o la antena(s) 316 representados en la FIG. 3. Los medios de recepción pueden comprender un receptor (por ejemplo, la unidad receptora 222) y/o una(s) antena(s) 224 del punto de acceso 110 ilustrado en la FIG. 2 o el receptor 312 y/o la(s) antena(s) 316 representada(s) en la FIG. 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 RX 242, el procesador de datos TX 210 y/o el controlador 230 del punto de acceso 110 ilustrado en la FIG. 2 o el procesador 304 y/o el DSP 320 representado en la FIG. 3.

Como se usa en el presente documento, el término "determinar" engloba una amplia variedad de acciones. Por ejemplo, "determinar" puede incluir calcular, computar, procesar, derivar, investigar, consultar (por ejemplo, consultar una tabla, una base de datos u otra estructura de datos), averiguar y similares. "Determinar" puede incluir también recibir (por ejemplo, recibir información), acceder (por ejemplo, acceder a datos en una memoria) y similares. "Determinar" puede incluir también 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 esos elementos, incluyendo elementos individuales. Como ejemplo, "al menos uno de: *a, b* o *c*" está previsto para abarcar a, *b, c, a-b, a-c, b-c* y *a-b-c.*

Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en conexión con la presente divulgación pueden implementarse o realizarse con un procesador de uso general, con un procesador de señales digitales (DSP), con un circuito integrado específico de la aplicación (ASIC), con una matriz de puertas programables por campo (FPGA) o con otro dispositivo de lógica programable (PLD), lógica de puertas discretas 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 uso general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier máquina de estados, microcontrolador, controlador o procesador disponible comercialmente. Un procesador puede implementarse también como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores en conjunción con un núcleo DSP o cualquier otra dicha configuración.

Las etapas de un procedimiento o algoritmo descrito en conexión 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 solo 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 distribuirse por varios segmentos de código diferentes, entre programas diferentes y a través de múltiples medios de almacenamiento. Un medio de almacenamiento puede estar acoplado al procesador de tal manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador.

Los procedimientos divulgados en el presente documento comprenden una o más etapas o acciones para conseguir el procedimiento descrito. Las etapas de procedimiento y/o las acciones pueden intercambiarse entre sí sin apartarse del alcance de las reivindicaciones. En otras palabras, a no ser que se especifique un orden específico de etapas o acciones, el orden y/o el 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 de ejemplo 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 dependiendo de la aplicación específica del sistema de procesamiento y de las restricciones de diseño globales. El bus puede vincular entre sí diversos 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 FIG. 1), puede conectarse también una interfaz de usuario (por ejemplo, un teclado, una pantalla, un ratón, una palanca de control, etc.) al bus. El bus puede vincular también otros diversos circuitos tales como fuentes de temporización, periféricos, reguladores de tensión, circuitos de gestión de energía y similares, que son ampliamente conocidos en la técnica y, por lo tanto, no se describirán con 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 uso general y/o de uso especial. Entre los ejemplos se incluyen microprocesadores, microcontroladores, procesadores DSP y otra circuitería que pueden ejecutar software. Software deberá interpretarse ampliamente como instrucciones, datos o cualquier combinación de los mismos, ya se denomine software, firmware, middleware, microcódigo, lenguaje de descripción de hardware o de otra forma. Los medios legibles por máquina pueden incluir, a modo de ejemplo, RAM (memoria de acceso aleatorio), memoria flash, ROM (memoria de solo lectura), PROM (memoria programable de solo lectura), EPROM (memoria programable de solo lectura y borrable), EEPROM (memoria programable de solo 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 de hardware, los medios legibles por máquina pueden formar parte del sistema de procesamiento independiente 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 por 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. De forma alternativa, o además, los medios legibles por máquina, o cualquier porción 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 uso general con uno o más microprocesadores que proporcionen la funcionalidad del procesador y una memoria externa que proporcione al menos una porción de los medios legibles por máquina, todos ellos conectados entre sí con otra circuitería de soporte, mediante una arquitectura de bus externa. De forma 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), la circuitería de soporte y al menos una porción de los medios legibles por máquina integrados en un único chip o con una o más FPGA (matrices de puertas programables por campo), PLD (dispositivos de lógica programable), controladores, máquinas de estados, lógica de puertas, componentes de hardware discretos o cualquier otra circuitería adecuada 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 dependiendo de la aplicación particular y de las restricciones de diseño globales impuestas al sistema global.

Los medios legibles por máquina pueden comprender diversos módulos de software. Los módulos de software incluyen instrucciones que, cuando se ejecutan por el procesador, hacen que el sistema de procesamiento realice

varias funciones. Los módulos de software pueden incluir un módulo de transmisión y un módulo receptor. 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 produzca un suceso de activación. Durante la ejecución del módulo de software, el procesador puede cargar parte de las instrucciones en la memoria caché para aumentar la velocidad de acceso. Una o más líneas de memoria caché pueden cargarse entonces en un fichero de registro general para su ejecución mediante el procesador. Cuando se haga referencia a continuación a la funcionalidad de un módulo de software, se entenderá que dicha funcionalidad se implementa por el procesador cuando ejecuta instrucciones de ese módulo de software.

Si se implementan en software, las funciones, como una o más instrucciones o código, pueden almacenarse en, o transmitirse 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 limitación, dichos medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otros dispositivos de 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 un código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. También, cualquier conexión se denomina de forma apropiada medio legible por ordenador. Por ejemplo, si el software se transmite desde una página web, un servidor u otra fuente remota 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, tal y como se usan en el presente documento, incluyen disco compacto (CD), disco láser, disco óptico, disco versátil digital (DVD), disco flexible y disco Blu-ray®, donde los discos reproducen usualmente datos de forma magnética o de forma óptica 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, para otros aspectos, los medios legibles por ordenador pueden comprender medios transitorios legibles por ordenador (por ejemplo, una señal). Las combinaciones de lo anterior deberían incluirse también dentro del alcance de los medios legibles por ordenador.

Por lo tanto, ciertos aspectos pueden comprender un producto de programa informático para realizar las operaciones presentadas en el presente documento. Por ejemplo, dicho 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. Para ciertos 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 otra forma por un terminal de usuario y/o una estación base según corresponda. Por ejemplo, dicho dispositivo puede acoplarse a un servidor para facilitar la transferencia de medios para realizar los procedimientos descritos en el presente documento. De forma 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 tal manera 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. Además, puede utilizarse cualquier otra técnica adecuada para proporcionar a un dispositivo los procedimientos y técnicas descritos en el presente documento.

Ha de entenderse que las reivindicaciones no se limitan a la configuración y a componentes precisos ilustrados anteriormente. Pueden realizarse diversas modificaciones, cambios y variaciones en la disposición, en el funcionamiento y en los detalles de los procedimientos y de los aparatos descritos anteriormente sin apartarse del alcance de las reivindicaciones.

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

1. Un aparato de comunicación inalámbrica, que comprende:

   un sistema de procesamiento configurado para almacenar localmente una porción de un conjunto de información, en el aparato;

   un receptor configurado para recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información; y

   un decodificador configurado para decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

2. El aparato del ejemplo 1, en donde el paquete comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes relativo a un encabezado MAC normal.

3. El aparato del ejemplo 1, en donde:

el conjunto de información usado para codificar el campo de datos comprende información de protocolo de modo de cifrado de contador (CCMP); y

el sistema de procesamiento está configurado para obtener la información CCMP usada para codificar el campo de datos de al menos uno de un encabezado CCMP del paquete o un encabezado CCMP de un paquete recibido anteriormente y usar la información CCMP obtenida para decodificar el campo de datos.

4. El aparato del ejemplo 3, en donde el sistema de procesamiento está configurado para:

obtener una primera porción de la información CCMP usada para codificar el campo de datos de un encabezado CCMP comprimido contenido en el paquete; y

obtener una segunda porción de la información CCMP usada para codificar el campo de datos de un encabezado CCMP completo, contenido en un paquete recibido anteriormente, que tiene al menos alguna información CCMP que no está contenida en el encabezado CCMP comprimido.

5. El aparato del ejemplo 3, en donde el sistema de procesamiento está configurado además para obtener la porción de la información CCMP a través del intercambio de tramas de gestión.

6. El aparato del ejemplo 3, en donde el sistema de procesamiento está configurado además para obtener la porción de la información CCMP a través de un paquete recibido anteriormente con un encabezado CCMP completo.

7. El aparato del ejemplo 3, en donde:

la porción almacenada de la información CCMP comprende una primera porción de un número de paquete usado para cifrar el campo de datos, en donde el número de paquete se incrementa con cada transmisión.

8. El aparato del ejemplo 7, en donde:

el paquete comprende un encabezado CCMP con una segunda porción del número de paquete.

9. El aparato del ejemplo 7, en donde el sistema de procesamiento está configurado para generar el número de paquete en base a la primera porción del número de paquete almacenado en el aparato y un número de secuencia contenido en un encabezado MAC.

10. El aparato de acuerdo con la reivindicación 7, en donde:

la primera porción del número de paquete almacenado en el aparato comprende bits más significativos del número de paquete; y

el sistema de procesamiento está configurado para detectar un vuelco en el número de paquete y actualizar los bits más significativos del número de paquete almacenado en el aparato en respuesta a la detección.

11. El sistema del ejemplo 3, en donde el sistema de procesamiento está configurado además para:

recibir un paquete posterior con una versión actualizada de la información CCMP; y actualizar la porción almacenada de la información CCMP.

12. El aparato del ejemplo 3, en donde:

el paquete comprende un encabezado CCMP que carece de Bytes reservados; y

el sistema de procesamiento decodifica el campo de datos usando la información contenida en el encabezado CCMP y la información almacenada.

13. El aparato del ejemplo 1, en donde:

el sistema de procesamiento decodifica el campo de datos usando un ID de clave almacenado.

14. El aparato del ejemplo 13, en donde el receptor está configurado para recibir el ID de clave almacenado a través de un intercambio de tramas de gestión o un encabezado CCMP completo.

15. Un aparato de comunicación inalámbrica, que comprende:

un sistema de procesamiento configurado para codificar un campo de datos usando un conjunto de información; y

un transmisor configurado para señalar, a otro aparato, una porción del conjunto de información y transmitir, al otro aparato, un paquete con el campo de datos codificado, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

16. El aparato del ejemplo 15, en donde el paquete comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes relativo a un encabezado MAC normal.

17. El aparato del ejemplo 15, en donde:

el conjunto de información usado para codificar el campo de datos comprende información de protocolo de modo de cifrado de contador (CCMP); y

el transmisor está configurado para proporcionar la información CCMP usada para codificar el campo de datos al otro aparato a través de al menos uno de un encabezado CCMP del paquete o un encabezado CCMP de un paquete transmitido anteriormente.

18. El aparato del ejemplo 17, en donde el transmisor está configurado para:

proporcionar una primera porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP comprimido contenido en el paquete; y

proporcionar una segunda porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP completo, contenido en un paquete recibido anteriormente, que tiene al menos parte de la información CCMP que no está contenida en el encabezado CCMP comprimido.

19. El aparato del ejemplo 17, en donde el transmisor está configurado además para señalar la porción de la información CCMP a través de un intercambio de tramas de gestión.

20. El aparato del ejemplo 17, en donde el transmisor está configurado además para señalar la porción de la información CCMP a través de un paquete transmitido anteriormente con un encabezado CCMP completo.

21. El aparato del ejemplo 15, en donde:

la porción señalada del conjunto de información comprende una primera porción de un número de paquete usado para codificar el campo de datos, en donde el número de paquete se incrementa con cada transmisión.

22. El aparato del ejemplo 21, en donde:

el paquete comprende un encabezado CCMP con una segunda porción del número de paquete.

23. El aparato del ejemplo 17, en donde el sistema de procesamiento está configurado además para:

transmitir un paquete posterior con una versión actualizada de la información CCMP.

24. El aparato del ejemplo 17, en donde:

el paquete comprende un encabezado CCMP que carece de Bytes reservados.

25. El aparato del ejemplo 15, en donde:

el sistema de procesamiento codifica el campo de datos usando un ID de clave.

26. El aparato del ejemplo 25, en donde el transmisor está configurado para transmitir el ID de clave al otro aparato a través de un intercambio de tramas de gestión o de un encabezado CCMP completo.

27. Un aparato para comunicaciones inalámbricas, que comprende:

medios para almacenar localmente una porción de un conjunto de información, en el aparato;
medios para recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información; y
medios para decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

28. El aparato del ejemplo 27, en donde el paquete comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes relativo a un encabezado MAC normal.

29. El aparato del ejemplo 27, en donde:

el conjunto de información usado para codificar el campo de datos comprende información de protocolo de modo de cifrado de contador (CCMP); y
el aparato comprende además medios para obtener la información CCMP usada para codificar el campo de datos de al menos uno de un encabezado CCMP del paquete o un encabezado CCMP de un paquete recibido anteriormente y usar la información CCMP obtenida para decodificar el campo de datos.

30. El aparato del ejemplo 29, en donde los medios de obtención están configurados para:

obtener una primera porción de la información CCMP usada para codificar el campo de datos a partir de un encabezado CCMP comprimido contenido en el paquete; y
obtener una segunda porción de la información CCMP usada para codificar el campo de datos de un encabezado CCMP completo, contenido en un paquete recibido anteriormente, que tiene al menos parte de la información CCMP que no está contenida en el encabezado CCMP comprimido.

31. El aparato del ejemplo 29, en donde los medios para obtener están configurados para obtener la porción de la información CCMP a través de un intercambio de tramas de gestión.

32. El aparato del ejemplo 29, en donde los medios para obtener están configurados para obtener la porción de la información CCMP a través de un paquete recibido anteriormente con un encabezado CCMP completo.

33. El aparato del ejemplo 29, en donde:

la porción almacenada de la información CCMP comprende una primera porción de un número de paquete usado para cifrar el campo de datos, en donde el número de paquete se incrementa con cada transmisión.

34. El aparato del ejemplo 33, en donde:

el paquete comprende un encabezado CCMP con una segunda porción del número de paquete.

35. El aparato del ejemplo 33, en donde los medios para decodificar están configurados para generar el número de paquete en base a la primera porción del número de paquete almacenado en el aparato y de un número de secuencia contenido en un encabezado MAC.

36. El aparato del ejemplo 33, en donde:

la primera porción del número de paquete almacenado en el aparato comprende bits más significativos del número de paquete; y
el sistema de procesamiento está configurado para detectar un vuelco en el número de paquete y actualizar los bits más significativos del número de paquete almacenado en el aparato en respuesta a la detección.

37. El aparato del ejemplo 29, en donde el aparato comprende además:

medios para recibir un paquete posterior con una versión actualizada de la información CCMP; y
medios para actualizar la porción almacenada de la información CCMP.

38. El aparato del ejemplo 29, en donde:

el paquete comprende un encabezado CCMP que carece de Bytes reservados; y
los medios de decodificación están configurados para decodificar el campo de datos usando información contenida en el encabezado CCMP y la información almacenada.

39. El aparato del ejemplo 27, en donde:

los medios para decodificar están configurados para decodificar el campo de datos usando un ID de clave

almacenado.

40. El aparato del ejemplo 39, que comprende además medios para recibir el ID de clave almacenado a través de un intercambio de tramas de gestión o de un encabezado CCMP completo.

41. Un aparato de comunicación inalámbrica, que comprende:

medios para codificar un campo de datos usando un conjunto de información; y

medios para señalar, a otro aparato, una porción del conjunto de información y transmitir, al otro aparato, un paquete con el campo de datos codificado, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

42. El aparato del ejemplo 41, en donde el paquete comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes relativo a un encabezado MAC normal.

43. El aparato del ejemplo 41, en donde:

el conjunto de información usado para codificar el campo de datos comprende información de protocolo de modo de cifrado de contador (CCMP); y
los medios de señalización están configurado para proporcionar la información CCMP usada para codificar el campo de datos al otro aparato a través de al menos uno de un encabezado CCMP del paquete o de un encabezado CCMP de un paquete transmitido anteriormente.

44. El aparato del ejemplo 43, en donde el procesador está configurado además para:

proporcionar una primera porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP comprimido contenido en el paquete; y
proporcionar una segunda porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP completo, contenido en un paquete recibido anteriormente, que tiene al menos parte de la información CCMP que no está contenida en el encabezado CCMP comprimido.

45. El aparato del ejemplo 43, en donde los medios de señalización están configurados además para señalar la porción de la información de CCMP a través de un intercambio de tramas de gestión.

46. El aparato del ejemplo 43, en donde los medios de señalización están configurados además para señalar la porción de la información CCMP a través de un paquete transmitido anteriormente con un encabezado CCMP completo.

47. El aparato del ejemplo 41, en donde:

la porción señalada del conjunto de información comprende una primera porción de un número de paquete usado para codificar el campo de datos, en donde el número de paquete se incrementa con cada transmisión.

48. El aparato del ejemplo 47, en donde:

el paquete comprende un encabezado CCMP con una segunda porción del número de paquete.

49. El aparato del ejemplo 43, que comprende además:

medios para transmitir un paquete posterior con una versión actualizada de información CCMP.

50. El aparato del ejemplo 43, en donde:

el paquete comprende un encabezado CCMP que carece de Bytes reservados.

51. El aparato del ejemplo 41, en donde:

los medios de codificación están configurados para codificar el campo de datos usando un ID de clave.

52. El aparato del ejemplo 51, en donde los medios de señalización están configurados para transmitir el ID de clave al otro aparato mediante un intercambio de tramas de gestión o de un encabezado CCMP completo.

53. Un procedimiento para comunicaciones inalámbricas por un aparato, que comprende:

almacenar localmente una porción de un conjunto de información, en el aparato;

recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información; y decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

54. El procedimiento del ejemplo 53, en donde el paquete comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes con respecto a un encabezado MAC normal.

55. El procedimiento del ejemplo 53, en donde:

el conjunto de información usado para codificar el campo de datos comprende información de protocolo de modo de cifrado de contador (CCMP); y

el procedimiento comprende además obtener la información CCMP usada para codificar el campo de datos de al menos uno de un encabezado CCMP del paquete o un encabezado CCMP de un paquete recibido anteriormente y usar la información CCMP obtenida para decodificar el campo de datos.

56. El procedimiento del ejemplo 55, en donde la obtención comprende:

obtener una primera porción de la información CCMP usada para codificar el campo de datos a partir de un encabezado CCMP comprimido contenido en el paquete; y

obtener una segunda porción de la información CCMP usada para codificar el campo de datos a partir de un encabezado CCMP completo, contenido en un paquete recibido anteriormente, que tiene al menos parte de la información CCMP que no está contenida en el encabezado CCMP comprimido.

57. El procedimiento del ejemplo 55, en donde la obtención comprende obtener la porción de la información de CCMP a través de un intercambio de tramas de gestión.

58. El procedimiento del ejemplo 55, en donde la obtención comprende obtener la porción de la información CCMP a través de un paquete recibido anteriormente con un encabezado CCMP completo.

59. El procedimiento del ejemplo 55, en donde:

la porción almacenada de la información CCMP comprende una primera porción de un número de paquete usado para cifrar el campo de datos, en donde el número de paquete se incrementa con cada transmisión.

60. El procedimiento del ejemplo 59, en donde:

el paquete comprende un encabezado CCMP con una segunda porción del número de paquete.

61. El procedimiento del ejemplo 59, que comprende además generar el número de paquetes en base a la primera porción del número de paquete almacenado en el aparato y un número de secuencia contenido en un encabezado MAC.

62. El procedimiento del ejemplo 59, en donde:

la primera porción del número de paquete almacenado en el aparato comprende bits más significativos del número de paquete; y
el procedimiento comprende además el defecto de un vuelco en el número de paquete y la actualización de los bits más significativos del número de paquete almacenado en el aparato en respuesta a la detección.

63. El procedimiento de la reivindicación 55, en donde el procedimiento comprende además:

recibir un paquete posterior con una versión actualizada de la información CCMP; y
actualizar la porción almacenada de la información CCMP.

64. El procedimiento del ejemplo 55, en donde:

el paquete comprende un encabezado CCMP que carece de Bytes reservados; y
la decodificación comprende decodificar el campo de datos usando información contenida en el encabezado CCMP y la información almacenada.

65. El procedimiento del ejemplo 53, en donde:

la decodificación comprende decodificar el campo de datos usando un ID de clave almacenado.

66. El procedimiento del ejemplo 65, que comprende además recibir el ID de clave almacenado a través de un intercambio de tramas de gestión o de un encabezado CCMP completo.

67. Un procedimiento para comunicaciones inalámbricas por un aparato, que comprende:

codificar un campo de datos usando un conjunto de información; y

señalar, a otro aparato, una porción del conjunto de información y transmitir, al otro aparato, un paquete con el campo de datos codificado, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

68. El procedimiento del ejemplo 67, en donde el paquete comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes con respecto a un encabezado MAC normal.

69. El procedimiento del ejemplo 67, en donde:

el conjunto de información usado para codificar el campo de datos comprende información de protocolo de modo de cifrado de contador (CCMP); y

la señalización comprende proporcionar la información CCMP usada para codificar el campo de datos al otro aparato a través de al menos uno de un encabezado CCMP del paquete o un encabezado CCMP de un paquete transmitido anteriormente.

70. El procedimiento del ejemplo 69, en donde la señalización comprende:

proporcionar una primera porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP comprimido contenido en el paquete; y

proporcionar una segunda porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP completo, contenido en un paquete recibido anteriormente, que tiene al menos parte de la información CCMP que no está contenida en el encabezado CCMP comprimido.

71. El procedimiento del ejemplo 69, en donde la señalización comprende señalar la porción de la información de CCMP a través de un intercambio de tramas de gestión.

72. El procedimiento del ejemplo 69, en donde la señalización comprende señalar la porción de la información CCMP a través de un paquete transmitido anteriormente con un encabezado CCMP completo.

73. El procedimiento del ejemplo 67, en donde:

la porción señalada del conjunto de información comprende una primera porción de un número de paquete usado para codificar el campo de datos, en donde el número de paquete se incrementa con cada transmisión.

74. El procedimiento del ejemplo 73, en donde:

el paquete comprende un encabezado CCMP con una segunda porción del número de paquete.

75. El procedimiento del ejemplo 69, que comprende además:

transmitir un paquete posterior con una versión actualizada de la información CCMP.

76. El procedimiento del ejemplo 69, en donde:

el paquete comprende un encabezado CCMP que carece de Bytes reservados.

77. El procedimiento del ejemplo 67, en donde:

la codificación comprende codificar el campo de datos usando un ID de clave.

78. El procedimiento del ejemplo 77, en donde la señalización comprende transmitir el ID de clave al otro aparato a través de un intercambio de tramas de gestión o de un encabezado CCMP completo.

79. 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 ejecutables para:

almacenar localmente una porción de un conjunto de información, en el aparato; recibir un paquete, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información; y

decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

80. 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 ejecutables para:

codificar un campo de datos usando un conjunto de información; señalar, a otro aparato, una porción del conjunto de información; y

transmitir al otro aparato un paquete con el campo de datos codificado, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

81. Una estación, que comprende:

al menos una antena;

un sistema de procesamiento configurado para almacenar localmente una porción de un conjunto de información, en la estación; un receptor configurado para recibir un paquete, a través de al menos una antena, comprendiendo dicho paquete un campo de datos codificado usando el conjunto de información; y

un decodificador configurado para decodificar el campo de datos usando la porción almacenada del conjunto de información e información adicional contenida en el paquete.

82. Un punto de acceso, que comprende:

al menos una antena;
un sistema de procesamiento configurado para codificar un campo de datos usando un conjunto de información; y
un transmisor configurado para señalar, a través de al menos una antena, a una estación, una porción del conjunto de información y transmitir, a la estación, un paquete con el campo de datos codificado, en donde el paquete carece de parte del conjunto de información usado para codificar el campo de datos.

REIVINDICACIONES

1. Un aparato (20a-120h, 120m, 302) de comunicación inalámbrica, que comprende:

medios (502A) para almacenar una primera porción de información de protocolo de modo de cifrado de contador, CCMP, obtenida a través de un paquete recibido anteriormente con un encabezado CCMP completo, localmente, en el aparato (120a-120h, 120m, 302);

medios (504A) para recibir un paquete (700, 800, 900), comprendiendo dicho paquete (700, 800, 900) un campo de datos codificado usando la información CCMP; y

medios (506A) para decodificar el campo de datos usando la primera porción almacenada de la información CCMP e información adicional contenida en el paquete (700, 800, 900); y

en donde el aparato (120a-120h, 120m, 302) comprende además medios para obtener una segunda porción de la información CCMP usada para codificar el campo de datos desde un encabezado CCMP comprimido (720) contenido en el paquete (700, 800, 900) y para obtener la primera porción almacenada de la información CCMP usada para codificar el campo de datos y en donde los medios (so6A) de decodificación están adaptados para usar las primera y segunda porciones obtenidas de la información CCMP para decodificar el campo de datos.

2. El aparato (120a-120h, 120m, 302) de la reivindicación 1, en donde el paquete (700, 800, 900) comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes con respecto a un encabezado MAC normal.

3. El aparato (120a-120h, 120m, 302) de la reivindicación 1, en donde:

la primera porción almacenada de la información CCMP comprende una primera porción de un número de paquete (700, 800, 900) usado para cifrar el campo de datos, en donde el número de paquete se incrementa con cada transmisión;

en particular en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP (720, 820, 920) con una segunda porción del número de paquetes; o

en particular en donde los medios de decodificación están configurados para generar el número de paquete en base a la primera porción del número de paquete almacenado en el aparato (120a-120h, 120m, 302) y un número de secuencia contenido en un encabezado MAC; o

en particular en donde:

la primera porción del número de paquete almacenado en el aparato (120a-120h, 120m, 302) comprende los bits más significativos del número de paquetes; y

el sistema de procesamiento está configurado para detectar un vuelco en el número de paquetes y actualizar los bits más significativos del número de paquetes almacenado en el aparato (120a-120h, 120m, 302) en respuesta a la detección.

4. El aparato de la reivindicación 1, en donde el aparato ((120a-120h, 120m, 302) comprende además:

medios para recibir un paquete (700, 800, 900) posterior con una versión actualizada de información CCMP; y

medios para actualizar la porción almacenada de la información CCMP; o

el aparato (120a-120h, 120m, 302) de la reivindicación 1, en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP (720, 820, 920) que carece de Bytes reservados; y

los medios (506A) de decodificación están configurados para decodificar el campo de datos usando la información contenida en el encabezado CCMP y la información almacenada.

5. Un aparato (110) de comunicación inalámbrica, que comprende:

medios para codificar un campo de datos usando la información de protocolo de modo de cifrado de contador, CCMP; y medios (602A) para señalar, a otro aparato (120a-120h, 120m, 302), una primera porción de la información CCMP y transmitir, al otro aparato (120a-120h, 120m, 302), un paquete (700, 800, 900) con el campo de datos codificado, en donde el paquete (700, 800, 900) carece de parte de la información CCMP usada para codificar el campo de datos, en donde:

los medios (602A) de señalización están configurados para proporcionar una segunda porción de la información CCMP usada para codificar el campo de datos al otro aparato (120a-120h, 120m, 302) en un encabezado CCMP comprimido (720) contenido en el paquete 700, 800, 900) y proporcionar la primera porción de la información CCMP usada para codificar el campo de datos al otro aparato (120a-120h, 120m, 302) en un encabezado CCMP completo, contenido en un paquete (700 , 800, 900) recibido anteriormente, que tiene al menos parte de la información CCMP que no está contenida en el encabezado CCMP comprimido (720).

6. El aparato (110) de la reivindicación 5, en donde el paquete (700, 800, 900) comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes relativo a un encabezado MAC normal.

7. El aparato (110) de la reivindicación 5, en donde:

la primera porción señalada de la información CCMP comprende una primera porción de un número de paquete usado para codificar el campo de datos, en donde el número de paquetes se incrementa con cada transmisión;

en particular en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP (720, 820, 920) con una segunda porción del número de paquetes; o

el aparato (no) de la reivindicación 5, que comprende además:

medios para transmitir un paquete (700, 800, 900) posterior con una versión actualizada de información CCMP.

8. El aparato (110) de la reivindicación 5, en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP (720, 820, 920) que carece de Bytes reservados.

9. Un procedimiento para comunicaciones inalámbricas por un aparato (120a-120h, 120m, 302), que comprende:

almacenar una primera porción de la información del protocolo de modo de cifrado de contador, CCMP, obtenida a través de un paquete recibido anteriormente con un encabezado CCMP completo, localmente, en el aparato (120a-120h, 120m, 302);

recibir un paquete (700, 800, 900), comprendiendo dicho paquete (700, 800, 900) un campo de datos codificado usando la información CCMP; y

decodificar el campo de datos usando la primera porción almacenada del conjunto de información e información adicional contenida en el paquete (700, 800, 900), en donde:

el procedimiento comprende además obtener una segunda porción de la información CCMP usada para codificar el campo de datos de un encabezado CCMP comprimido (720) contenido en el paquete (700, 800, 900) y obtener la primera porción almacenada de la información CCMP usada para codificar el campo de datos y usando las primera y segunda porciones obtenidas de la información CCMP para decodificar el campo de datos.

10. El procedimiento de la reivindicación 9, en donde el paquete (700, 800, 900) comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes con respecto a un encabezado MAC normal.

11. El procedimiento de la reivindicación 9, en donde:

la porción almacenada de la información CCMP comprende una primera porción de un número de paquetes usado para cifrar el campo de datos, en donde el número de paquetes se incrementa con cada

transmisión;

en particular en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP con una segunda porción del número de paquetes; o

en particular comprendiendo además generar el número de paquetes en base a la primera porción del número de paquete almacenado en el aparato (120a-120h, 120m, 302) y un número de secuencia contenido en un encabezado MAC; o

en particular en donde:

la primera porción del número de paquete almacenado en el aparato (120a-120h, 120m, 302) comprende los bits más significativos del número de paquetes; y

el procedimiento comprende además el defecto de un vuelco en el número de paquetes y la actualización de los bits más significativos del número de paquete almacenado en el aparato (120a-120h, 120m, 302) en respuesta a la detección; o

el procedimiento de la reivindicación 9, en donde el procedimiento comprende:

recibir un paquete (700, 800, 900) posterior con una versión actualizada de información CCMP; y

actualizar la porción almacenada de la información CCMP; o

el procedimiento de la reivindicación 9, en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP (720, 820, 920) que carece de Bytes reservados; y

la decodificación comprende decodificar el campo de datos usando información contenida en el encabezado CCMP (720, 820, 920) y la información almacenada.

12. Un procedimiento para comunicaciones inalámbricas por un aparato (110), que comprende:

codificar un campo de datos usando la información del protocolo de modo de cifrado de contador, CCMP; y

señalar, a otro aparato (120a-120h, 120m, 302), una primera porción de la información CCMP y transmitir, al otro aparato, un paquete (700, 800, 900) con el campo de datos codificado, en donde el paquete (700, 800, 900) carece de parte de la información CCMP usada para codificar el campo de datos, en donde:

la señalización comprende proporcionar una segunda porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP comprimido (720) contenido en el paquete (700, 800, 900) y la primera porción de la información CCMP usada para codificar el campo de datos al otro aparato en un encabezado CCMP completo, contenido en un paquete (700, 800, 900) recibido anteriormente, que tiene al menos alguna información CCMP que no está contenida en el encabezado CCMP comprimido (720).

13. El procedimiento de la reivindicación 12, en donde el paquete (700, 800, 900) comprende un encabezado MAC y una indicación de que el encabezado MAC comprende un encabezado MAC corto que tiene un número reducido de bytes con respecto a un encabezado MAC normal.

14. El procedimiento de la reivindicación 12, en donde:

la primera porción señalada de la información CCMP comprende una primera porción de un número de paquete usado para codificar el campo de datos, en donde el número de paquete se incrementa con cada transmisión;

en particular en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP con una segunda porción del número de paquete; o

el procedimiento de la reivindicación 12, que comprende además:

transmitir un paquete (700, 800, 900) posterior con una versión actualizada de información CCMP; o

el procedimiento de la reivindicación 12, en donde:

el paquete (700, 800, 900) comprende un encabezado CCMP (720, 820, 920) que carece de Bytes reservados; o

el procedimiento de la reivindicación 12, en donde:

la codificación comprende codificar el campo de datos usando un ID de clave;

en particular en donde la señalización comprende transmitir el ID de clave al otro aparato a través de un intercambio de tramas de gestión o de un encabezado CCMP completo.

15. Un programa informático que comprende un código para realizar las etapas del procedimiento de acuerdo con cualquiera de las reivindicaciones 9 a 14 cuando se ejecuten en un ordenador.

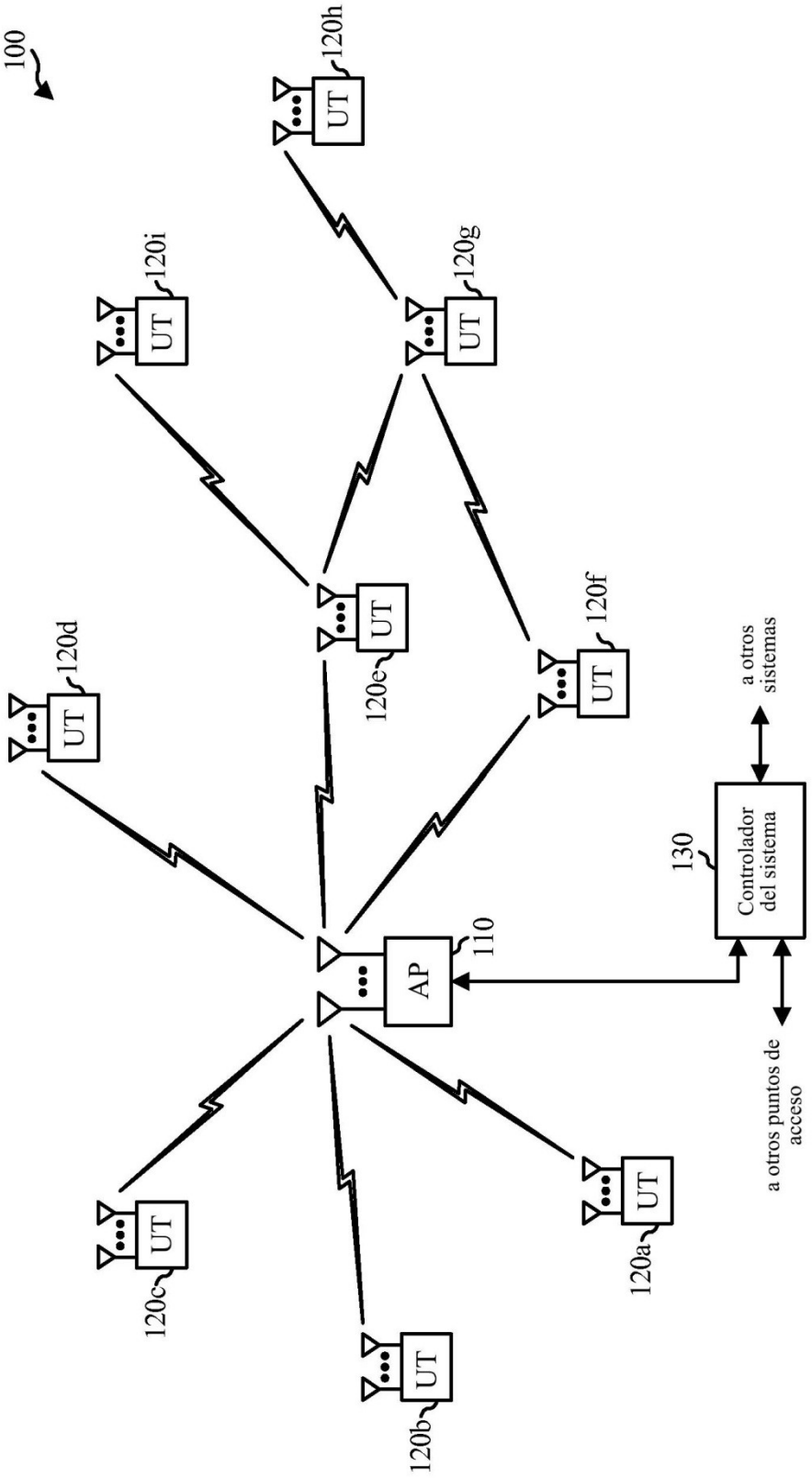

100
UT
120h
UT
120i
UT
120g
UT
120d
UT
120e
UT
120f
AP
110
130
Controlador del sistema
a otros sistemas
a otros puntos de acceso
UT
120c
UT
120b
UT
120a

FIG. 1

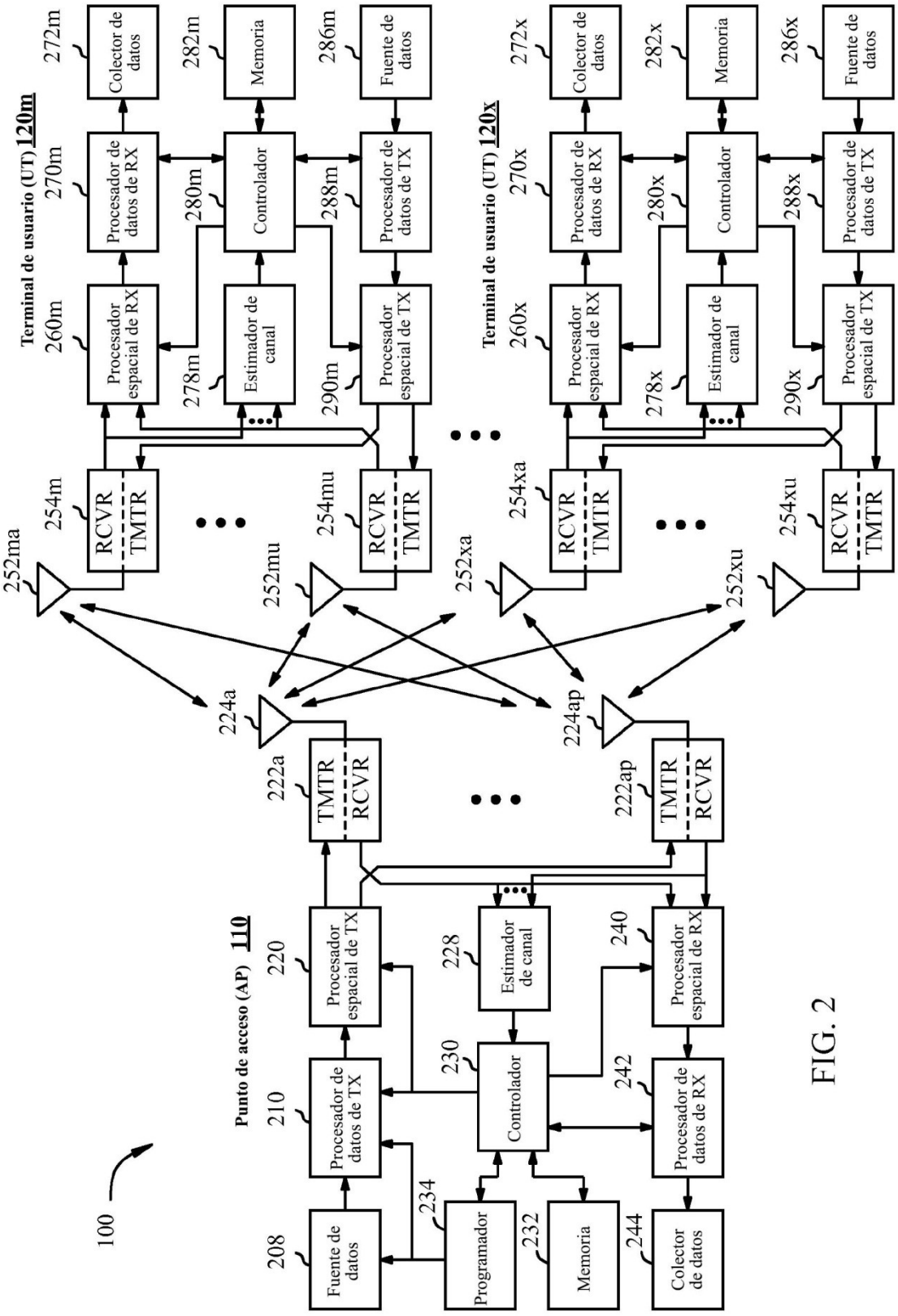

100
Punto de acceso (AP) 110
Fuente de datos 208
Procesador de datos de TX 210
Procesador espacial de TX 220
TMTR RCVR 222a
224a
Programador 234
Memoria 232
Controlador 230
Estimador de canal 228
Procesador espacial de RX 240
Procesador de datos de RX 242
Colector de datos 244
TMTR RCVR 222ap
224ap
252ma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

FIG. 2

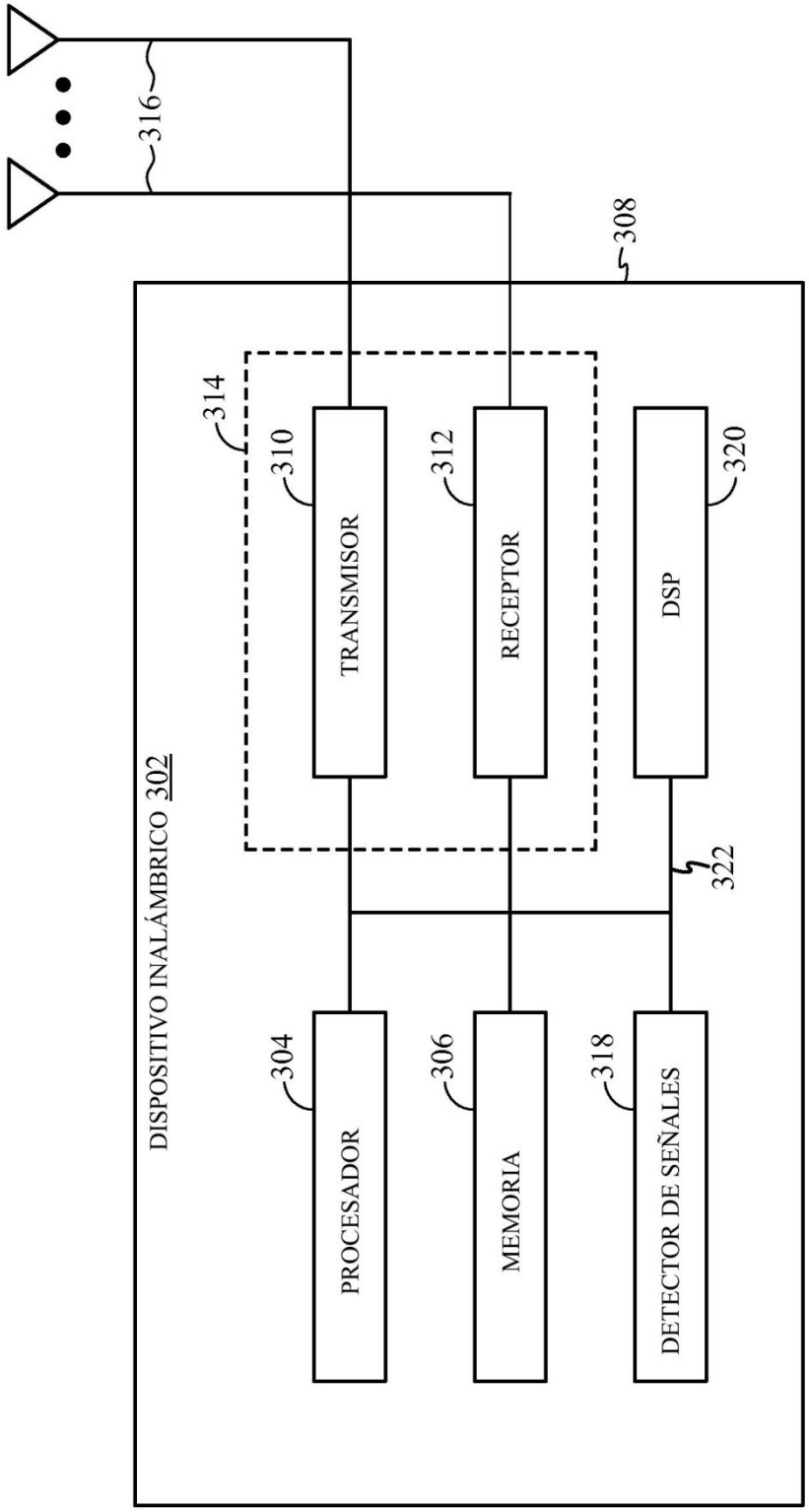

316
308
DISPOSITIVO INALÁMBRICO 302
314
310
TRANSMISOR
312
RECEPTOR
320
DSP
322
304
PROCESADOR
306
MEMORIA
318
DETECTOR DE SEÑALES

FIG. 3

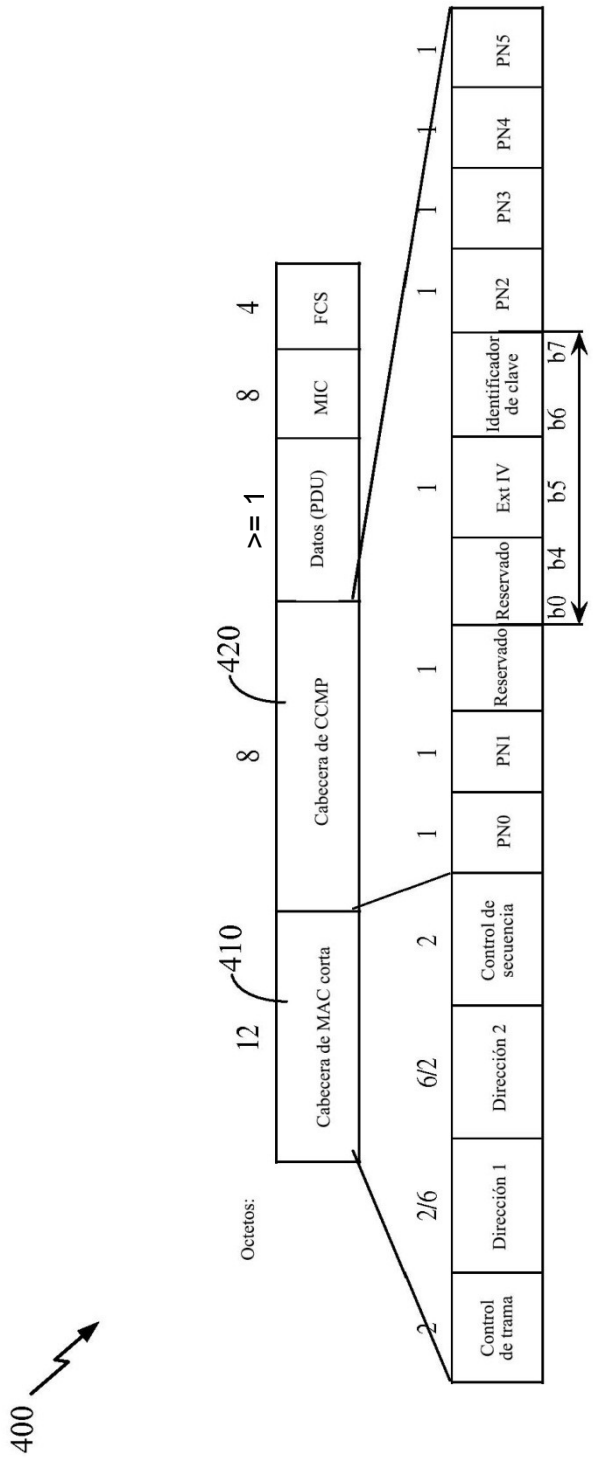

400
Octetos:
12
410
Cabecera de MAC corta
8
420
Cabecera de CCMP
>= 1
Datos (PDU)
8
MIC
4
FCS
2
Control de trama
2/6
Dirección 1
6/2
Dirección 2
2
Control de secuencia
1
PN0
1
PN1
1
Reservado
1
Reservado
1
Ext IV
1
Identificador de clave
1
PN2
1
PN3
1
PN4
1
PN5
b0
b4
b5
b6
b7

FIG. 4

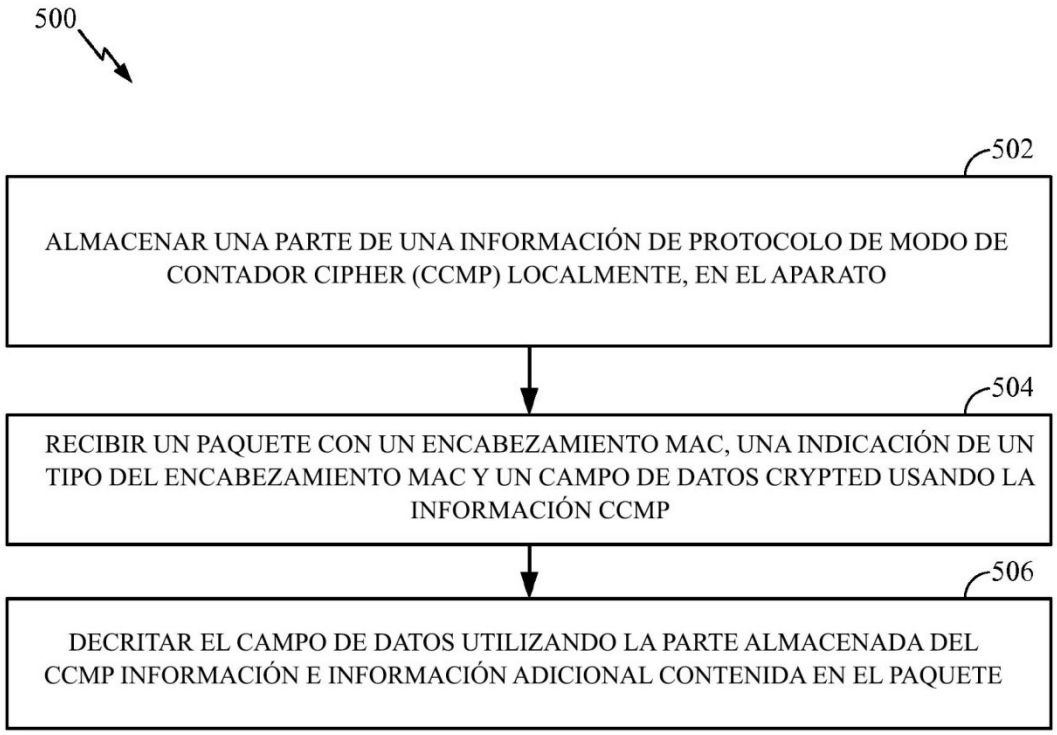

500
502
ALMACENAR UNA PARTE DE UNA INFORMACIÓN DE PROTOCOLO DE MODO DE CONTADOR CIPHER (CCMP) LOCALMENTE, EN EL APARATO
504
RECIBIR UN PAQUETE CON UN ENCABEZAMIENTO MAC, UNA INDICACIÓN DE UN TIPO DEL ENCABEZAMIENTO MAC Y UN CAMPO DE DATOS CRYPTED USANDO LA INFORMACIÓN CCMP
506
DECRITAR EL CAMPO DE DATOS UTILIZANDO LA PARTE ALMACENADA DEL CCMP INFORMACIÓN E INFORMACIÓN ADICIONAL CONTENIDA EN EL PAQUETE

FIG. 5

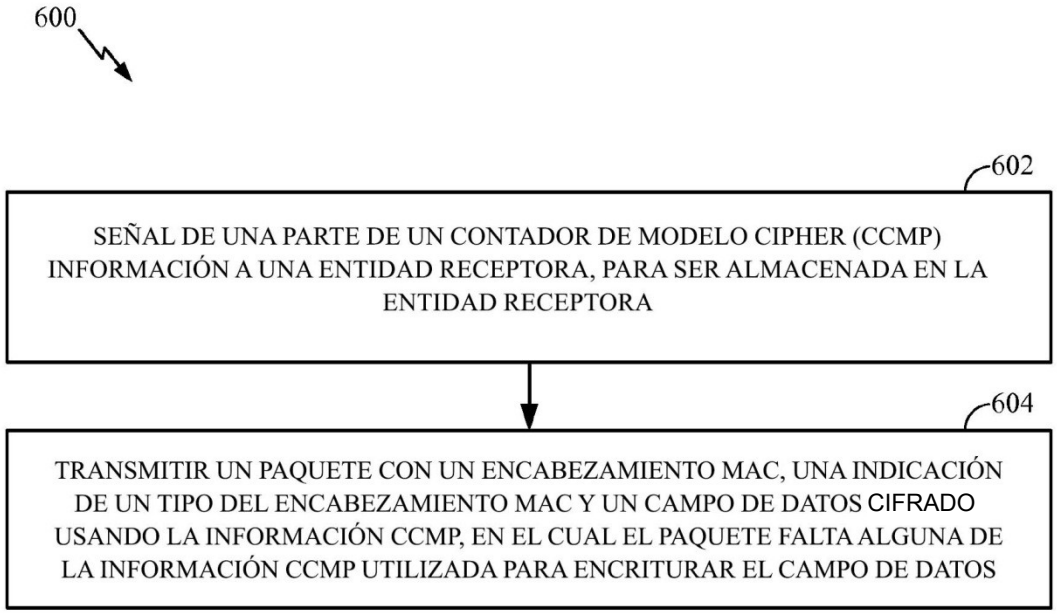

600
602
SEÑAL DE UNA PARTE DE UN CONTADOR DE MODELO CIPHER (CCMP) INFORMACIÓN A UNA ENTIDAD RECEPTORA, PARA SER ALMACENADA EN LA ENTIDAD RECEPTORA
604
TRANSMITIR UN PAQUETE CON UN ENCABEZAMIENTO MAC, UNA INDICACIÓN DE UN TIPO DEL ENCABEZAMIENTO MAC Y UN CAMPO DE DATOS CIFRADO USANDO LA INFORMACIÓN CCMP, EN EL CUAL EL PAQUETE FALTA ALGUNA DE LA INFORMACIÓN CCMP UTILIZADA PARA ENCRITURAR EL CAMPO DE DATOS

FIG. 6

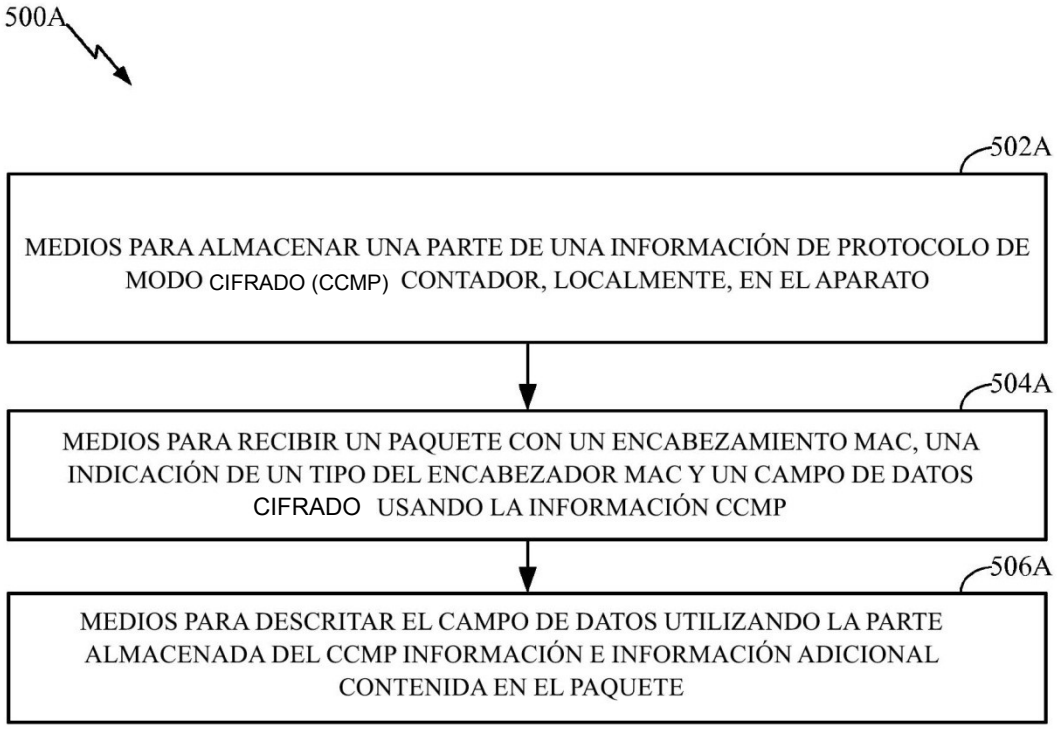

500A
502A
MEDIOS PARA ALMACENAR UNA PARTE DE UNA INFORMACIÓN DE PROTOCOLO DE MODO CIFRADO (CCMP) CONTADOR, LOCALMENTE, EN EL APARATO
504A
MEDIOS PARA RECIBIR UN PAQUETE CON UN ENCABEZAMIENTO MAC, UNA INDICACIÓN DE UN TIPO DEL ENCABEZADOR MAC Y UN CAMPO DE DATOS CIFRADO USANDO LA INFORMACIÓN CCMP
506A
MEDIOS PARA DESCRITAR EL CAMPO DE DATOS UTILIZANDO LA PARTE ALMACENADA DEL CCMP INFORMACIÓN E INFORMACIÓN ADICIONAL CONTENIDA EN EL PAQUETE

FIG. 5A

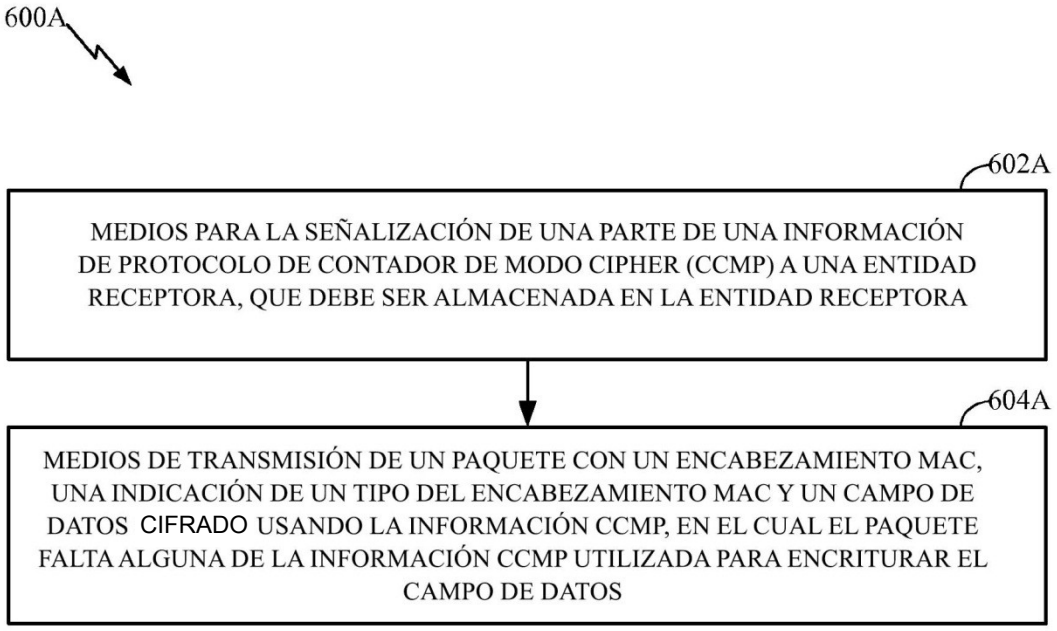
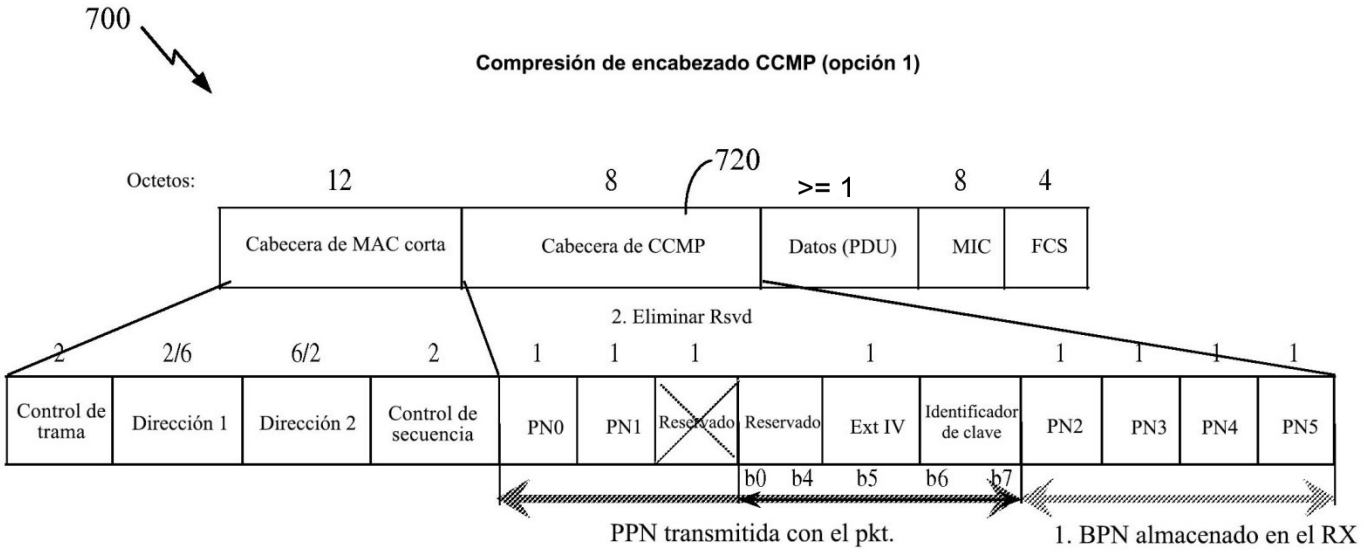

600A
602A
MEDIOS PARA LA SEÑALIZACIÓN DE UNA PARTE DE UNA INFORMACIÓN DE PROTOCOLO DE CONTADOR DE MODO CIPHER (CCMP) A UNA ENTIDAD RECEPTORA, QUE DEBE SER ALMACENADA EN LA ENTIDAD RECEPTORA
604A
MEDIOS DE TRANSMISIÓN DE UN PAQUETE CON UN ENCABEZAMIENTO MAC, UNA INDICACIÓN DE UN TIPO DEL ENCABEZAMIENTO MAC Y UN CAMPO DE DATOS CIFRADO USANDO LA INFORMACIÓN CCMP, EN EL CUAL EL PAQUETE FALTA ALGUNA DE LA INFORMACIÓN CCMP UTILIZADA PARA ENCRITURAR EL CAMPO DE DATOS

FIG. 6A

FIG. 7



- **Definir una PN base (BPN)**
  - BPN = PN2 | PN3 | PN4 | PN5
  - BPN se almacena en el RXer a través de intercambio de marco de gestión [6]
- **Transmite el resto del encabezado CCMP con el paquete**
  - PN0 | PN1 | Clave ID
  - Referido como paquete PN (PPN)
- **El encabezado CCMP completo se puede reconstruir en el receptor**
  - Concatenar PPN | BPN
- **BPN necesita ser actualizado en PNO |Vuelco PN1**
  - Se espera que un vuelco basado en 16 bits sea muy bajo para aplicaciones 11ah
- **El encabezado CCMP se reduce de 8 octetos a 3 octetos**
  - Sólo PN0 | PN1 | Key ID Los octetos necesitan ser transmitidos junto con el paquete

Encabezado CCMP corto (paso 1)

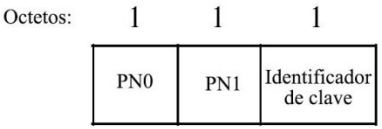


FIG. 7A

FIG. 8

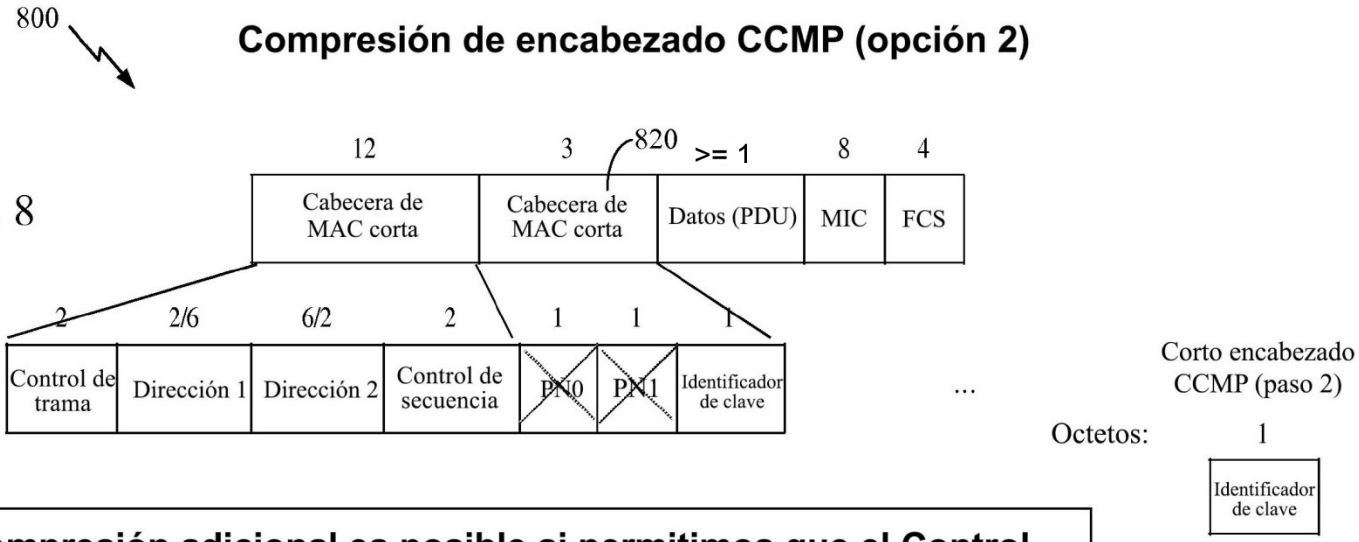
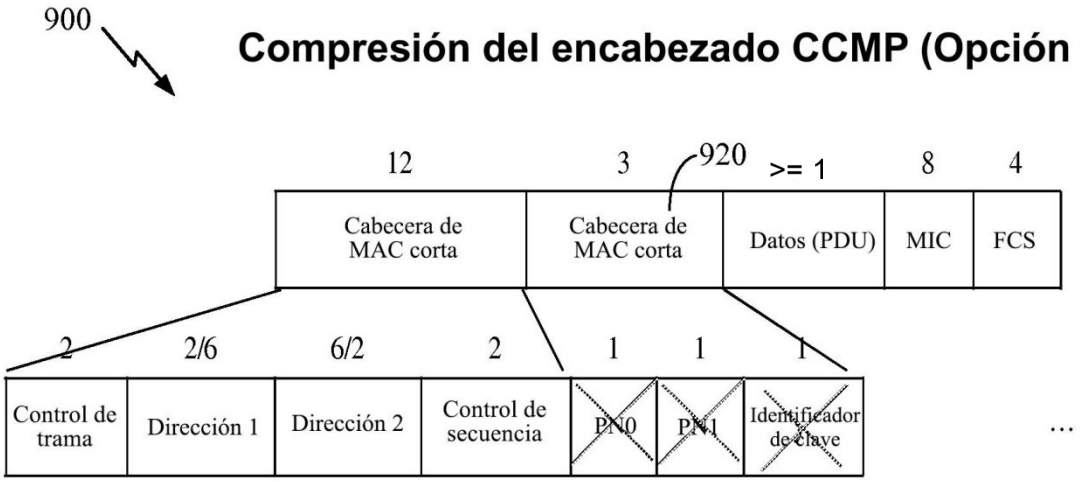


FIG. 8A

- **Una compresión adicional es posible si permitimos que el Control de Secuencia actúe como PN0 | PN1**
  - PN0 | PN1 = SC (= SN | FN)
  - El número de paquete aumenta con pasos de 16 cuando la MSDU no está fragmentada
  - Esto significa que la PN se reduce efectivamente en 4 bits
- **El encabezado CCMP se reduce a sólo 1 Octeto**
  - Sólo el octeto de identificación de clave necesita ser transmitido con el paquete

FIG. 9



- **Una compresión adicional es posible mediante la eliminación del octeto ID de clave**
  - La extensión IV es siempre 1 para CCMP
  - Reencripción nunca sucede para el tráfico de unidifusión y el tráfico de grupo no utiliza cortos encabezados de MAC, por lo que el identificador de clave se puede omitir también
- **El encabezado de CCMP se elimina básicamente del encabezado MAC corto**
  - PN0 | PN1 = SC