(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 755 836**

(51) Int. CI.:

H04W 64/00 (2009.01)
G01S 5/02 (2010.01)
G01S 5/14 (2006.01)
G01S 13/76 (2006.01)
G01S 13/87 (2006.01)
G01S 5/00 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.10.2016 PCT/US2016/057803**

(87) Fecha y número de publicación internacional: **26.05.2017 WO17087118**

(96) Fecha de presentación y número de la solicitud europea: **20.10.2016 E 16794788 (6)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 3378260**

(54) Título: **Medición de temporización fina segura**

(30) Prioridad:

20.11.2015 US 201562257932 P
27.05.2016 US 201615166646

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.04.2020

(73) Titular/es:

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

(72) Inventor/es:

VAMARAJU, SANTOSH y
ALDANA, CARLOS HORACIO

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Medición de temporización fina segura

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

[0001] Esta petición reivindica el beneficio y la prioridad de la Solicitud Provisional de los Estados Unidos n.º de serie 62/257 932 presentada el 20 de noviembre de 2015, y la Solicitud de Servicios Públicos de los Estados Unidos n.º de serie 15/166 646 presentada el 27 de mayo de 2016, ambas tituladas "SECURE FINE TIMING MEASUREMENT PROTOCOL [PROTOCOLO DE MEDICIÓN DE TEMPORIZACIÓN FINA SEGURA]" y ambas asignadas al cesionario del presente documento.

CAMPO DE LA INVENCIÓN

[0002] Los modos de realización del tema inventivo en general se relacionan con el campo de la comunicación inalámbrica y, más particularmente, con la determinación de la posición de un dispositivo móvil basándose en los protocolos de Medición de Temporización Fina (FTM).

ANTECEDENTES

[0003] Se pueden emplear diversas técnicas de localización para determinar la posición de un dispositivo de comunicación inalámbrica (por ejemplo, un dispositivo de red de área local inalámbrica (WLAN)), basándose en la recepción de señales de comunicación inalámbricas. Por ejemplo, las técnicas de posicionamiento pueden utilizar una o más sesiones de medición de temporización fina (FTM) entre un dispositivo móvil y uno o más puntos de acceso. Las técnicas de posicionamiento pueden utilizar el tiempo de llegada (TOA), el tiempo de ida y vuelta (RTT) de las señales de comunicación inalámbrica, el indicador de intensidad de la señal recibida (RSSI) o la diferencia horaria de llegada (TDOA) de las señales de comunicación inalámbrica para determinar la posición de un dispositivo de comunicación inalámbrica en una red de comunicación inalámbrica. Estos factores pueden usarse junto con las posiciones conocidas de una o más estaciones en la red inalámbrica para obtener la ubicación del dispositivo de comunicación inalámbrica. En general, las sesiones de FTM se transmiten sin cifrado y, por lo tanto, son susceptibles a ataques de intermediarios mediante los cuales una estación no autorizada puede supervisar la sesión y falsificar la información de dirección de una estación de respuesta. Como resultado, la estación no autorizada puede proporcionar información falsa de hora de llegada a la estación solicitante y, por lo tanto, afectar negativamente a los resultados de posicionamiento resultantes. El documento WO 2015/047234 A1 (INTEL CORP [US]; STEINER ITAI [IL]; SEGEV JONATHAN [IL]) 2 de abril de 2015 (02-04-2015) divulga un sistema transceptor inalámbrico para proporcionar un intercambio de medición de temporización fina (FTM) segura configurado para obtener un valor de token seguro inicial y para recibir un mensaje de respuesta de FTM que incluye un valor de respuesta de token seguro de una estación de respuesta.

SUMARIO

[0004] La invención se define en las reivindicaciones independientes. Se proporcionan características adicionales de la invención en las reivindicaciones dependientes. Los modos de realización y/o ejemplos divulgados en la siguiente descripción que no están cubiertos por las reivindicaciones adjuntas se considera que no forman parte de la presente invención.

[0005] Un ejemplo de un sistema de transceptor inalámbrico para proporcionar un intercambio de medición de temporización fina (FTM) segura de acuerdo con la divulgación incluye una memoria, al menos un procesador acoplado operativamente a la memoria y configurado para obtener un valor de token seguro inicial y un valor de respuesta de token seguro a través de una señal fuera de banda, generar un mensaje de petición de FTM que incluye el valor de token seguro inicial, un transmisor para enviar el mensaje de petición de FTM a una estación de respuesta y un receptor para recibir un mensaje de respuesta de FTM que incluye el valor de respuesta de token seguro de la estación de respuesta, de modo que al menos un procesador esté configurado para determinar un valor de tiempo de ida y vuelta (RTT) basado, al menos en parte, en el mensaje de respuesta de FTM.

[0006] Las implementaciones de dicho sistema transceptor inalámbrico pueden incluir una o más de las siguientes características. El mensaje de petición de FTM que incluye el valor de token seguro inicial puede incluir una trama de cabecera de Control de acceso a medios (MAC) con un elemento de información de token seguro. El mensaje de petición FTM que incluye el valor de token seguro inicial puede incluir un campo de parámetro FTM con un elemento de información de token seguro. El elemento de información de token seguro se puede agregar al campo de parámetro FTM. El valor de token seguro inicial y el valor de respuesta token seguro pueden ser valores iguales. El valor de token seguro inicial y el valor de respuesta token seguro pueden ser aleatorizados. El al menos un procesador puede configurarse adicionalmente para determinar una posición del sistema transceptor inalámbrico basándose, al menos en parte, en el valor RTT.

[0007] Un ejemplo de un procedimiento para participar en un intercambio de medición de temporización fina (FTM) segura de acuerdo con la divulgación incluye obtener una dirección de control de acceso a medios (MAC) de origen autentificado y una dirección MAC de destino autentificado, generar un mensaje de petición FTM que incluya la dirección MAC de origen autentificado y la dirección MAC de destino autentificado, enviar el mensaje de petición de FTM a una estación de respuesta, recibir un mensaje de respuesta de FTM que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado de la estación de respuesta, y determinar un valor de tiempo de ida y vuelta (RTT) basado al menos en parte en el mensaje de respuesta de FTM.

[0008] Las implementaciones de dicho procedimiento pueden incluir una o más de las características siguientes. Obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado puede incluir recibir la dirección MAC de origen autentificado y la dirección MAC de destino autentificado a través de un intercambio fuera de banda con un servidor de posición. Obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado puede incluir realizar una función de aleatorización en una dirección MAC de origen original y una dirección MAC de destino original. Al menos un elemento de información de campo de parámetro FTM puede ser una entrada a la función de aleatorización. El elemento de información de campo del parámetro FTM puede ser un campo de Función de sincronización de temporización parcial (PTSF). Una hora de salida (TOD) o una hora de llegada (TOA) del mensaje de respuesta de FTM puede usarse como entrada para la función de aleatorización. Se puede recibir un token seguro a través de un intercambio fuera de banda con un servidor de posición. Obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado puede incluir realizar una función de aleatorización en una dirección MAC de origen original y una dirección MAC de destino original, en el que el token seguro es una entrada a la función de aleatorización. La obtención de la dirección MAC de origen autentificado y la dirección MAC de destino autentificado puede incluir el intercambio de la dirección MAC en un elemento de información del proveedor.

[0009] Un ejemplo de un aparato para proporcionar un intercambio de medición de temporización fina (FTM) segura de acuerdo con la divulgación incluye medios para obtener un valor de token seguro inicial y un valor de respuesta de token seguro a través de una señal fuera de banda, medios para generar un mensaje de petición de FTM que incluye el valor de token seguro inicial, medios para enviar el mensaje de petición de FTM a una estación de respuesta, medios para recibir un mensaje de respuesta de FTM que incluye el valor de respuesta de token seguro de la estación de respuesta y medios para determinar un valor de tiempo de ida y vuelta (RTT) basado, al menos en parte, en el mensaje de respuesta de FTM.

[0010] Un ejemplo de un medio de almacenamiento legible por procesador no transitorio que comprende instrucciones para participar en un intercambio de medición de temporización fina (FTM) segura incluye un código para obtener una dirección de Control de acceso a medios (MAC) de origen autentificado y una dirección MAC de destino autentificado para generar un mensaje de petición FTM que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado, código para enviar el mensaje de petición FTM a una estación de respuesta, código para recibir un mensaje de respuesta de FTM que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado de la estación de respuesta y código para determinar un valor de tiempo de ida y vuelta (RTT) basado, al menos en parte, en el mensaje de respuesta de FTM.

[0011] Un ejemplo de un sistema de transceptor inalámbrico para participar en un intercambio de medición de temporización fina (FTM) segura incluye una memoria, al menos un procesador acoplado operativamente a la memoria y configurado para obtener una dirección de control de acceso a medios (MAC) de origen autentificado y una dirección MAC de destino autentificado, generar un mensaje de petición FTM que incluya la dirección MAC de origen autentificado y la dirección MAC de destino autentificado, enviar el mensaje de petición FTM a una estación de respuesta, recibir un mensaje de respuesta de FTM que incluya la dirección MAC de origen autentificado y la dirección MAC de destino autentificado de la estación de respuesta y determine un valor de tiempo de ida y vuelta (RTT) basado, al menos en parte, en el mensaje de respuesta de FTM.

[0012] Las implementaciones de dicho sistema transceptor inalámbrico pueden incluir una o más de las siguientes características. El al menos un procesador puede configurarse para obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado a través de un intercambio fuera de banda con un servidor de posición. El al menos un procesador puede estar configurado para realizar una función de aleatorización en una dirección MAC de origen original y una dirección MAC de destino original para obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado. Al menos un elemento de información de campo de parámetro FTM puede ser una entrada a la función de aleatorización. El al menos un elemento de información de campo de parámetro FTM puede ser un campo de Función de sincronización de temporización parcial (PTSF). Al menos uno de un Tiempo de Salida (TOD) o un Tiempo de Llegada (TOA) del mensaje de Respuesta FTM puede ser una entrada a la función de aleatorización. El al menos un procesador puede configurarse para obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado al recibir un token seguro a través de un intercambio fuera de banda con un servidor de posición y realizar una función de aleatorización en una dirección MAC de origen original y una dirección MAC de destino original, de modo que el token seguro sea una entrada a la función de aleatorización. El al menos un procesador está configurado para intercambiar una dirección MAC en un elemento de información del proveedor para obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado.

[0013] Los elementos y/o técnicas descritos en el presente documento pueden proporcionar una o más de las siguientes capacidades, así como otras capacidades no mencionadas. Dos estaciones pueden participar en una sesión de medición de temporización fina (FTM). Se puede incluir un token seguro en el mensaje de petición FTM inicial (iFTMR). La estación de respuesta puede incluir una respuesta de token seguro en el iFTM. Las estaciones de inicio y respuesta pueden autentificarse entre sí durante la sesión de FTM. El token seguro y la respuesta de token seguro pueden formar la base de una generación por trama de una nueva dirección de control de acceso a medios (MAC) de origen y una nueva dirección MAC de destino para las estaciones participantes. El token seguro y la respuesta de token seguro pueden formar la base de una generación de sesión por FTM de unas nuevas direcciones MAC de origen y destino para las estaciones participantes. Las direcciones MAC de origen y destino pueden aleatorizarse mediante procedimientos fuera de banda. Los tokens seguros se pueden reemplazar mediante el uso de combinaciones de valores FTM, como la función de sincronización de temporización parcial (PTSF), la hora de entrega (TOD) y la hora de llegada (TOA). En un ejemplo, algunas o todos las tramas en los mensajes FTM pueden estar cifradas. Se puede calcular un tiempo de ida y vuelta (RTT) basado en la sesión FTM. La información de posición puede obtenerse de la información RTT. La probabilidad de un ataque de intermediario puede reducirse. Además, puede ser posible que se logre un efecto mencionado anteriormente por medios distintos a los señalados, y un elemento/técnica señalado no necesariamente produce el efecto señalado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0014]

La FIG. 1A es un diagrama de bloques de ejemplo de una red de área local inalámbrica para proporcionar un protocolo FTM seguro.

La FIG. 1B es un diagrama de red de ejemplo de una red de comunicación de área local inalámbrica que incluye un servidor de posición.

La FIG. 2 es un diagrama conceptual del uso de múltiples sesiones seguras de FTM.

La FIG. 3 es un flujo de mensajes de ejemplo en una sesión FTM en la técnica anterior.

La FIG. 4 es un flujo de mensajes de ejemplo en una sesión segura de FTM.

La FIG. 5A es una trama MAC de ejemplo con un elemento de información de token seguro.

La FIG. 5B es una trama MAC de ejemplo con elementos de información de dirección segura.

La FIG. 6A es un ejemplo de trama MAC con dirección segura basada en un valor TSF parcial.

La FIG. 6B es un ejemplo de un elemento FTM con un token seguro.

La FIG. 7A es un diagrama de flujo de un proceso para intercambiar mensajes FTM incluyendo tokens seguros.

La FIG. 7B es un diagrama de flujo de un proceso para intercambiar mensajes FTM incluyendo direcciones de Control de acceso a medios (MAC) autentificadas.

La FIG. 8A es un diagrama de bloques de un dispositivo electrónico para su uso en el intercambio de mensajes FTM seguros.

La FIG. 8B es un diagrama de bloques de un transceptor inalámbrico a modo de ejemplo.

DESCRIPCIÓN DETALLADA

[0015] La siguiente descripción incluye sistemas, procedimientos, técnicas, secuencias de instrucciones y productos de programa informáticos a modo de ejemplo, que realizan las técnicas de la materia objeto de la presente invención. Sin embargo, debe entenderse que los modos de realización descritos pueden llevarse a la práctica sin estos detalles específicos. Por ejemplo, aunque los ejemplos utilizan tramas de mensajes de medición de temporización fina (FTM) según IEEE 802.11, los modos de realización no son tan limitados. En otros modos de realización, la información de posicionamiento puede proporcionarse mediante otras normas y dispositivos inalámbricos (por ejemplo, dispositivos de WiMAX). En otros ejemplos, para no oscurecer la descripción, no se han mostrado en detalle casos de instrucciones, protocolos, estructuras y técnicas ampliamente conocidos.

[0016] En las redes de comunicación inalámbrica, determinar la posición de un dispositivo electrónico con capacidades de comunicación inalámbrica (por ejemplo, dentro de un entorno interior o exterior) puede ser una característica deseada para los usuarios del dispositivo de comunicación (por ejemplo, usuarios de teléfonos móviles) y operadores de la red de comunicación inalámbrica. En algunos sistemas, las técnicas de tiempo de ida y vuelta

(RTT) pueden implementarse para determinar la posición del dispositivo de comunicación. En general, un dispositivo de comunicación puede transmitir un mensaje de petición a múltiples puntos de acceso y puede recibir un mensaje de respuesta de cada uno de los puntos de acceso. El rango entre el dispositivo de comunicación y cada uno de los puntos de acceso se puede determinar midiendo el tiempo de ida y vuelta entre los mensajes de petición y los mensajes de respuesta correspondientes. La posición del dispositivo de comunicación se puede determinar comparando la información RTT con las ubicaciones conocidas de los puntos de acceso. En algunos sistemas, las técnicas de diferencia de tiempo de llegada (TDOA) pueden implementarse para determinar la posición del dispositivo de comunicación. Por ejemplo, el dispositivo de comunicación puede determinar su posición basándose en la diferencia entre los rangos de cada uno de los puntos de acceso al dispositivo de comunicación. Un dispositivo de comunicación móvil puede iniciar operaciones de posicionamiento RTT (o las operaciones de posicionamiento TDOA) transmitiendo un mensaje de petición a uno o más puntos de acceso. El uso de un teléfono móvil y puntos de acceso se proporcionan para simplificar la explicación técnica y, por lo tanto, no son una limitación, ya que los mensajes de petición y la respuesta pueden enviarse entre puntos de acceso (es decir, sin un teléfono móvil). Los dispositivos de comunicación y los puntos de acceso pueden denominarse en general estaciones como una estación de inicio y una estación de respuesta.

[0017] En un ejemplo, un protocolo FTM (por ejemplo, 802.11mc D4.3 sección 10,24.6) puede permitir que dos estaciones intercambien tramas de medición de ida y vuelta (por ejemplo, tramas FTM). Una estación de inicio (por ejemplo, STA 1) calcula el tiempo de ida y vuelta registrando el TOA (es decir, t2) de la trama FTM de una estación de respuesta (por ejemplo, STA 2) y registrando el TOD de una trama de confirmación (ACK) de la trama FTM (es decir, t3). La STA 2 registra TOD de la trama FTM (es decir, t1) y el TOA del ACK recibido de STA 1 (es decir, t4). De este modo, el RTT se calcula como:

$$RTT = [(t4-t1) - (t3-t2)]$$

[0018] Este intercambio de trama puede ser propenso a un ataque de intermediario mediante suplantación y otros procedimientos que afectan la confianza de las estaciones que participan en el intercambio. Por ejemplo, una estación no autorizada puede supervisar el aire en busca de peticiones iFTM, y luego puede configurarse para enviar tramas FTM a una estación de inicio inocente falsificando la dirección de control de acceso a medios (MAC) de la estación de respuesta. La estación no autorizada puede enviar un mensaje ACK a las tramas FTM de las estaciones de respuesta, haciendo así que la estación de respuesta registre una hora falsa de llegada del ACK. Tales ataques de intermediario pueden afectar a la usabilidad general del protocolo FTM. Esto es particularmente relevante para aplicaciones de alta seguridad que se construyen sobre el protocolo FTM (por ejemplo, geo-cercado).

[0019] Los ataques de intermediario pueden eliminarse, o al menos obstaculizarse sustancialmente, mediante los procedimientos y aparatos descritos en el presente documento. En un ejemplo, el elemento de token seguro puede incluirse en un mensaje de petición de FTM inicial (iFTMR) y un elemento de respuesta de token seguro puede incluirse en la respuesta de FTM inicial (iFTM). Las estaciones participantes pueden autentificarse entre sí durante la sesión de FTM. La respuesta de token seguro y/o token seguro puede formar la base de una sesión FTM por trama y/o por seguridad (por ejemplo, basándose en un nivel de seguridad deseado). En un ejemplo, los tokens seguros pueden realizarse generando nuevas combinaciones de dirección MAC de origen y dirección MAC de destino para las estaciones participantes. Las estaciones participantes pueden implementar a través de hardware y/o software algoritmos de autentificación similares para autentificar (por ejemplo, reconocer, deducir) las combinaciones de direcciones MAC de origen autentificado y destino autentificado entre sí. Las estaciones participantes pueden usar la combinación de dirección MAC generada como las direcciones MAC de origen y destino de las tramas que transmiten. Por ejemplo, una estación de inicio puede programar su hardware para autentificar (por ejemplo, aceptar) mensajes FTM desde una dirección MAC de origen autentificado. Una estación de respuesta puede usar la dirección MAC de origen autentificado para transmitir un mensaje FTM a la dirección MAC de destino autentificado y programar su hardware para autentificar (por ejemplo, aceptar) tramas ACK de la dirección MAC de destino autentificado. La estación de inicio puede programar su hardware para enviar un mensaje ACK a los mensajes FTM recibidos de la dirección MAC de origen esperada. El uso de dicha combinación de direcciones MAC puede disminuir en gran medida la amenaza de un ataque de intermediario porque es poco probable que la estación no autorizada determine el origen y el destino de la sesión de FTM y, por lo tanto, no podrá hacerse pasar por ninguna de las estaciones.

[0020] En un modo de realización, la dirección MAC de origen autentificado y la dirección MAC de destino autentificado pueden ser aleatorizadas por procedimientos fuera de banda. Por ejemplo, se puede usar un factor de aleatorización o una función para generar direcciones MAC sobre la marcha. Las tramas FTM y ACK se pueden transmitir y recibir basándose en las direcciones MAC aleatorias correspondientes. En un modo de realización, los tokens seguros se pueden reemplazar mediante el uso de combinaciones de uno o más de los valores PTSF, TOD, TOA. Dichas combinaciones se pueden usar para deducir las direcciones MAC necesarias para autentificar las estaciones participantes. Entre los ejemplos de tales combinaciones se incluyen, entre otros, los siguientes:

M' = Secure_token XOR M (XOR también se puede reemplazar por AND)

M' = PTSF XOR (LSB(16) de M) (XOR también se puede reemplazar por AND)

M' = PTSF XOR (LSB (16) de M) XOR TOD XOR TOA (XOR también se puede reemplazar por AND)

[0021] Donde M' es la dirección MAC autentificada generada a partir de la dirección MAC original M.

[0022] Con referencia a la FIG. 1A, se muestra un diagrama de bloques de ejemplo de una red de comunicación inalámbrica 100 para proporcionar un protocolo FTM seguro. La red de comunicación inalámbrica 100 incluye cuatro puntos de acceso 102, 104, 106 y 104 y una estación cliente 120. Los puntos de acceso 102, 104, 106, 108 pueden ser puntos de acceso WLAN avanzados capaces de determinar sus propias posiciones (por ejemplo, un punto de acceso de auto localización). Los puntos de acceso pueden configurarse para comunicarse con uno o más puntos de acceso en la red de comunicación inalámbrica 100 (por ejemplo, dentro del rango de comunicación entre sí). En algunas implementaciones, los puntos de acceso pueden organizarse de modo que un punto de acceso pueda designarse como un punto de acceso principal, y los otros puntos de acceso pueden designarse como puntos de acceso objetivo. La estación cliente 120 puede ser cualquier dispositivo electrónico adecuado (por ejemplo, un ordenador tipo notebook, una tablet, un ordenador tipo netbook, un teléfono móvil, una consola de juegos, un asistente digital personal (PDA), una etiqueta de inventario, etc.) con capacidades de comunicación WLAN. Además, en la FIG. 1A, la estación cliente 120 está dentro del rango de comunicación de uno o más puntos de acceso 102, 104, 106, 108.

[0023] La estación cliente 120 puede participar en un intercambio fuera de banda u otro intercambio negociado previamente con uno o más puntos de acceso. Por ejemplo, la estación cliente 120 y el punto de acceso de confianza 108 pueden ser parte de un grupo de confianza formado a través de un servicio en la nube (por ejemplo, Google AP, iCloud). La estación cliente 120 y el punto de acceso de confianza 108 están configurados para establecer un intercambio fuera de banda 110. El contenido del intercambio fuera de banda 110 puede incluir tokens seguros, factores y funciones de aleatorización u otra información de seguridad para permitir intercambios de FTM seguros. En un ejemplo, los intercambios de FTM pueden estar cifrados y la información de seguridad recibida a través del intercambio fuera de banda 110 puede incluir claves públicas y/o privadas correspondientes. Al recibir la información de seguridad, la estación cliente 120 puede configurarse para iniciar una o más sesiones de FTM con los puntos de acceso 102, 104, 106, 108. Por ejemplo, una primera sesión FTM 112 puede ocurrir entre la estación cliente 120 y el punto de acceso fiable 108. La estación cliente 120 puede determinar la información de posición (por ejemplo, información RTT y/o TDOA) basándose en la primera sesión FTM 112. La estación cliente 120 puede iniciar posteriormente una segunda sesión FTM 114 con un segundo punto de acceso (por ejemplo, el punto de acceso 102) basándose en la información segura incluida en el intercambio fuera de banda 110. La segunda sesión 114 de FTM no necesita estar precedida por otro intercambio fuera de banda con el segundo punto de acceso 102. A continuación, la estación cliente 120 puede determinar la información de posición (por ejemplo, información RTT y/o TDOA) basándose en la segunda sesión 114 de FTM. Se pueden producir sesiones FTM adicionales basándose en la información de seguridad recibida durante el intercambio fuera de banda 110. La estación cliente 120 puede iniciar una tercera sesión FTM 116 con un tercer punto de acceso (por ejemplo, punto de acceso 104) y una cuarta sesión FTM 118 con un cuarto punto de acceso (por ejemplo, punto de acceso 106).

[0024] En algunas implementaciones, la estación cliente 120 puede usar la información de posición del punto de acceso (por ejemplo, latitud, longitud, altitud), en combinación con la información de temporización TDOA y/o la información de temporización RTT para construir una "ecuación de posicionamiento" en términos del rango entre la estación cliente 120 y cada uno de los puntos predeterminados de acceso 102, 104, 106, 108. Por ejemplo, al determinar la información de posición del punto de acceso, la información de temporización TDOA y la información de temporización RTT asociada con tres puntos de acceso objetivo, la estación cliente 120 puede resolver tres ecuaciones de posicionamiento para determinar una posición tridimensional de la estación cliente 120. Se observa que en otras implementaciones, la estación cliente 120 puede determinar una posición basándose en la información de posición del punto de acceso, la información de temporización TDOA y la información de temporización RTT asociada con cualquier número adecuado de puntos de acceso. Por ejemplo, una posición puede basarse en dos ecuaciones de posicionamiento independientes a partir de la información de posición del punto de acceso, la información de temporización TDOA y la información de temporización RTT asociada con dos puntos de acceso objetivo para determinar una posición bidimensional de la estación cliente 120.

[0025] Con referencia a la FIG. 1B, se muestra un diagrama de red de ejemplo de una red de área local inalámbrica que incluye un servidor de posición. La red 150 incluye puntos de acceso 102, 104, 106, 108, un servidor de posición 152 y una ruta de comunicación 154. El servidor de posición 152 es un dispositivo informático que incluye al menos un procesador y una memoria y está configurado para ejecutar instrucciones ejecutables por ordenador. Por ejemplo, un servidor de posición 152 comprende un sistema informático que incluye un procesador, memoria no transitoria, unidades de disco, una pantalla, un teclado, un ratón. El procesador es preferentemente un dispositivo inteligente, por ejemplo, una unidad central de procesamiento (CPU) de ordenador personal como las fabricadas por Intel® Corporation o AMD®, un microcontrolador, un circuito integrado específico de aplicación (ASIC), etc. La memoria incluye memoria de acceso aleatorio (RAM) y memoria de solo lectura (ROM). Las unidades de disco incluyen una unidad de disco duro, una unidad de CD-ROM y/o una unidad zip, y pueden incluir otras formas de unidades. La pantalla es una pantalla de cristal líquido (LCD) (por ejemplo, una pantalla de transistor de película delgada (TFT)), aunque otras formas de pantallas son aceptables, por ejemplo, un tubo de rayos catódicos (CRT). El teclado y el ratón proporcionan mecanismos de entrada de datos para un usuario. El servidor de posición 152 almacena (por ejemplo, en la memoria) código de software ejecutable por el procesador legible por el procesador que contiene instrucciones

para controlar el procesador para realizar las funciones descritas en el presente documento. Las funciones pueden ayudar en la implementación de proporcionar un protocolo FTM seguro. El software se puede cargar en la memoria descargándolo a través de una conexión de red, cargado desde un disco, etc. Además, el software puede no ser directamente ejecutable, por ejemplo, requiriendo compilación antes de la ejecución. Los puntos de acceso 102, 104, 106, 108 están configurados para comunicarse con el servidor de posición 152 para intercambiar información de posición a través de la ruta de comunicación 154. La ruta de comunicación 154 puede ser una red de área amplia (WAN) y puede incluir Internet. El servidor de posición 152 puede incluir una estructura de datos (por ejemplo, base de datos relacional, archivos planos) para almacenar tokens seguros, factores y funciones de aleatorización u otra información de seguridad para permitir intercambios de FTM seguros. En un ejemplo, el servidor de posición 152 puede incluir información de estación adicional tal como información de posición (por ejemplo, lat./long., X/y), información RTT, información SIFS y otra información asociada con una estación (por ejemplo, SSID, dirección MAC, valor de incertidumbre, área de cobertura, etc.). Un punto de acceso (por ejemplo, 102, 104, 106, 108) puede comunicarse con el servidor de posición 152 y puede recuperar, por ejemplo, información de seguridad, información SIFS e información RTT para usar en soluciones de posicionamiento de estación cliente. La configuración del servidor de posición 152 como servidor remoto es solo a modo de ejemplo y no una limitación. En un modo de realización, el servidor de posición 152 puede estar conectado directamente a un punto de acceso, o la funcionalidad puede estar incluida en un punto de acceso. Se puede usar más de un servidor de posición. El servidor de posición 152 puede incluir una o más bases de datos que contienen información de seguridad asociada con otras estaciones en redes adicionales. En un ejemplo, el servidor de posición 152 se compone de múltiples unidades de servidor.

[0026] Con referencia a la FIG. 2, se muestra un diagrama conceptual 200 del uso de múltiples intercambios de mensajes FTM seguros. El diagrama conceptual 200 incluye tres puntos de acceso (por ejemplo, AP1, AP2, AP3) y un dispositivo móvil (por ejemplo, STA1). En un ejemplo, el dispositivo móvil puede iniciar un intercambio 202 fuera de banda con API conectándose con el grupo de confianza 204 y recibiendo información de seguridad 206. La información de seguridad puede incluir elementos como tokens seguros, factores o funciones de aleatorización, tablas de búsqueda (por ejemplo, para correlacionar direcciones MAC reales y autentificadas), claves criptográficas u otra información para permitir intercambios de FTM seguros. La información de seguridad puede persistir en el servidor de posición 152 y puede ser accesible a través de la ruta de comunicación 154. STA1 puede utilizar la información de seguridad para iniciar una primera sesión segura de FTM 208 con API. STA 1 también puede usar la información de seguridad 206 para iniciar una segunda sesión segura FTM 210 con AP2, y una tercera sesión segura FTM 212 con AP3. El orden para la primera, segunda y tercera sesiones seguras de FTM es solo a modo de ejemplo. En un ejemplo, el orden de las sesiones seguras de FTM puede basarse en otra información de red, como transmisiones de balizas de estación o una consulta y respuesta del Protocolo de consulta de red de acceso (ANQP) (por ejemplo, un informe de contiguo ordenado).

[0027] Con referencia a la FIG. 3, se muestra un ejemplo de un diagrama conceptual de una sesión de medición de temporización fina (FTM) 300. El enfoque general incluye una estación de inicio 302 y una estación de respuesta 304. La estación de inicio 302 y la estación de respuesta 304 pueden ser cualquiera de la estación cliente 120 y los puntos de acceso 102, 104, 106, 108. Como distinción general, un punto de acceso puede servir a múltiples estaciones, pero los términos que se usan en el presente documento no son tan limitados. Las operaciones relevantes descritas en el presente documento pueden realizarse tanto en estaciones como en puntos de acceso. La sesión FTM puede permitir que la estación de inicio 302 obtenga su alcance con la estación de respuesta 304. La estación de inicio 302 puede realizar este procedimiento con otras estaciones múltiples (por ejemplo, puntos de acceso) para obtener su ubicación. Una sesión FTM es una instancia de un procedimiento de medición de temporización fina entre la estación de inicio 302 y la estación de respuesta 304, y puede incluir la programación asociada y los parámetros operativos de esa instancia. Una sesión FTM en general se compone de una negociación, un intercambio de mediciones y una terminación. Un punto de acceso puede participar en múltiples sesiones simultáneas de FTM. Las sesiones FTM simultáneas pueden ocurrir con estaciones de respuesta que son miembros de diferentes conjuntos de servicios básicos (BSS) y posiblemente diferentes conjuntos de servicios extendidos (ESS), o posiblemente fuera de un BSS, con cada sesión utilizando su propia programación, canal y parámetros operativos. Es posible que se requiera una estación de respuesta para establecer sesiones de FTM superpuestas con una gran cantidad de estaciones de inicio (por ejemplo, un punto de acceso que proporcione mediciones a varias estaciones de clientes diferentes en el estadio, un centro comercial o una tienda). En un ejemplo, una estación cliente puede tener múltiples sesiones de FTM en curso en el mismo canal o en canales diferentes con diferentes puntos de acceso de respuesta, mientras está asociada a un punto de acceso particular para el intercambio de datos o señalización. En un ejemplo, la estación cliente no está asociada con ningún punto de acceso. Para soportar las restricciones de ambos puntos de acceso, durante la negociación, la estación de inicio 302 inicialmente solicita una asignación de ventana de tiempo periódica preferente. La estación de respuesta 304 responde posteriormente aceptando o anulando la petición de asignación basándose en su disponibilidad y capacidad de recursos. Dado que algunas de las actividades 302 de la estación de inicio pueden no ser deterministas y tener mayor prioridad que la sesión FTM (por ejemplo, la interacción de transferencia de datos con un AP asociado), un conflicto puede evitar que la estación de inicio 302 esté disponible al comienzo de una instancia de ráfaga determinada por la estación de respuesta 304. En tal ejemplo, la estación de inicio 302 puede establecer sesiones con la estación de respuesta 304 y otra estación en diferentes canales. La periodicidad de cada ráfaga de las sesiones puede ser diferente y las compensaciones de reloj de cada estación pueden diferir. Por lo tanto, con el tiempo, pueden ocurrir algunos conflictos temporales. Para superar esto, durante cada instancia de ráfaga, la estación de inicio puede indicar su disponibilidad transmitiendo una trama de activación en forma de una trama de

petición de medición de temporización fina. Durante cada instancia de ráfaga, la estación de respuesta transmite una o más tramas de medición de temporización fina como se negoció.

[0028] Con referencia a la FIG. 4, con referencia adicional a la FIG. 3, se muestra un flujo de mensajes en una sesión segura de FTM 400. Una estación de inicio 402 puede proporcionar un mensaje de petición de asociación 406 a una estación de respuesta 404. En un ejemplo, la estación de inicio 402 puede enviar un mensaje de petición de sonda a una estación de respuesta 404. La petición de asociación 406 puede incluir la dirección MAC original (M1) asignada a la estación de inicio 402 y la dirección MAC original (M2) asignada a la estación de respuesta 404. En un ejemplo, al recibir el mensaje de petición de asociación 406, la estación de respuesta 404 puede configurarse para generar una dirección MAC de origen autentificado (M1') y una dirección MAC de destino autentificado (M2'). En un ejemplo, generar las direcciones MAC autentificadas incluye recibir información de seguridad de un servidor de posición u otro origen fuera de banda. La estación de respuesta 404 está configurada para proporcionar un mensaje de respuesta de asociación 408 (o un mensaje de respuesta de sonda) basado en las direcciones MAC originales (por ejemplo, M1 y M2). El mensaje de respuesta de asociación 408 puede incluir una indicación (por ejemplo, indicador, elemento de información) para indicar que la estación de respuesta está configurada para participar en una sesión FTM segura.

[0029] La estación de inicio 402, al recibir la respuesta de asociación 408 (o una respuesta de sonda), puede configurarse para obtener o generar la dirección MAC de origen autentificado (M1') y la dirección MAC de destino autentificado (M2'). Las direcciones MAC autentificadas pueden incluir tokens seguros. Las direcciones MAC originales pueden aleatorizarse basándose en elementos de hardware y/o software que operan en ambas estaciones (por ejemplo, obtenidas de un origen fuera de banda). En un modo de realización, los tokens seguros se pueden reemplazar o aumentar mediante el uso de combinaciones de uno o más de los valores PTSF, TOD, TOA. También pueden usarse otros elementos de información y operaciones lógicas (por ejemplo, M1'= PTSF XOR (LSB (16) de M1) XOR TOD XOR TOA y otras funciones como se describió anteriormente). La dirección MAC autentificada puede basarse en tablas de consulta o en otras funciones criptográficas negociadas previamente (por ejemplo, funciones de hash). La estación de inicio 402 está configurada para iniciar una sesión FTM segura enviando un mensaje 410 de iFTMR que incluye la dirección MAC de origen autentificado (M1') y la dirección MAC de destino autentificado (M2'). La estación de respuesta 404 proporciona un mensaje de confirmación (Ack) 412 utilizando las direcciones MAC autentificadas (por ejemplo, M1', M2'). La estación de respuesta 404 puede proporcionar un mensaje iFTM 414 y la estación de inicio 402 puede proporcionar la confirmación 416 correspondiente utilizando las direcciones MAC autentificadas. Los valores de RTT pueden calcularse como se describió previamente utilizando los valores para t1, t2, t3 y t4.

[0030] Con referencia a la FIG. 5A, se muestra una trama MAC 500 de ejemplo con un elemento de información de token seguro (IE). La trama MAC 500 en general puede cumplir con los estándares de la industria (por ejemplo, IEEE 802.11 REVmc, sección 8,2), con la adición de un token seguro IE 502. El token seguro IE puede ser un indicador (por ejemplo, bit) que indica que una estación está utilizando direcciones MAC autentificadas. El token seguro IE 502 puede incluir un código (por ejemplo, 2, 4, 8 bits) para indicar una o más funciones para generar y/o descodificar direcciones MAC autentificadas. Es decir, las estaciones pueden incluir hardware y software para generar y descodificar direcciones MAC autentificadas mediante múltiples procesos diferentes y el token seguro IE 502 indica cuál de los múltiples procesos puede usarse. En un ejemplo, el token seguro IE 502 puede representar un identificador seguro único (por ejemplo, 128, 256 bits) que puede ser autentificado por las estaciones de inicio y respuesta.

[0031] Con referencia a la FIG. 5B, se muestra una trama MAC 550 de ejemplo con elementos de información de dirección segura. Los elementos de dirección originales incluyen el elemento de dirección original 1 552 (por ejemplo, M1) y el elemento de dirección original 2 554 (por ejemplo, M2). Las direcciones seguras correspondientes (por ejemplo, direcciones autentificadas) pueden obtenerse basándose en uno o más factores de aleatorización u otras funciones. Por ejemplo, una primera función 556 puede usarse para transformar el elemento de dirección 1 552 en el elemento de dirección segura 1 562 (por ejemplo, M1'). De manera similar, se puede usar una segunda función 558 para transformar el elemento 554 de dirección 2 en el elemento 564 de dirección segura 2 (por ejemplo, M2'). La primera función 556 y la segunda función 558 pueden ser las mismas o diferentes funciones. En un modo de realización, la selección de las funciones primera y segunda puede basarse en el valor del token seguro IE 502. La primera y segunda función 556, 558 pueden incluirse en la información de seguridad obtenida de un procedimiento fuera de banda u otro procedimiento prenegociado. Una lista no limitativa de funciones de ejemplo incluye:

Función 1: M' = Secure_token XOR M

Función 2: M' = Secure_token AND M

Función 3: M' = PTSF XOR (LSB(16) of M)

Función 4: M' = PTSF AND (LSB(16) of M)

Función 5: M' = PTSF XOR (LSB(16) of M) XOR TOD XOR TOA

Función 6: M' = PTSF AND (LSB(16) of M) XOR TOD XOR TOA

Función 7: M' = PTSF AND (LSB(16) of M) AND TOD XOR TOA

Función 8: M' = PTSF AND (LSB(16) of M) AND TOD AND TOA

Función 9: M '= PTSF XOR (LSB (16) de M) XOR TOD Y TOA

Función 10: M' = PTSF XOR (LSB(16) of M) AND TOD XOR TOA

[0032] La lista de funciones es solo a modo de ejemplo, y no una limitación. Se pueden usar otras funciones. En un ejemplo, se pueden usar tablas de búsqueda o funciones de hash aleatorias para generar las direcciones MAC autentificadas. En un modo de realización, las tablas de búsqueda pueden incluir funciones hash criptográficas (por ejemplo, SHA-1) correspondientes a las direcciones MAC originales. Las tablas y funciones de búsqueda se pueden proporcionar a las estaciones a través de intercambios fuera de banda entre un servidor y las estaciones para preservar su integridad/confidencialidad.

[0033] Con referencia a la FIG. 6A, se muestra un ejemplo de la trama MAC 610 con direcciones seguras basadas en un valor de TSF parcial. El valor de temporizador TSF parcial 602 se incluye en un elemento 600 de Parámetros de medición de temporización fina (por ejemplo, IEEE 802.11 REVmc, Fig. 8-570). Se pueden usar una o más funciones 604 para generar una o más direcciones seguras. En un ejemplo, la una o más funciones 604 pueden utilizar el valor del temporizador TSF parcial 602 como una variable para calcular la dirección segura 1 606 y la dirección segura 2 608. Por ejemplo, un procesador de ordenador puede implementar las Funciones 3 a 10 descritas anteriormente para utilizar el valor de temporizador TSF parcial 602 (por ejemplo, PTSF) para calcular una dirección MAC segura (por ejemplo, autentificada).

[0034] Con referencia a la FIG. 6B, se muestra un elemento de parámetro de medición de temporización fina 650 con un token seguro. En general, el elemento del parámetro de medición de temporización fina 650 se basa en los estándares de la industria (por ejemplo, IEEE 802.11 REVmc, Fig. 8-570) con la adición de un elemento de información de token seguro. En un ejemplo, el elemento de información segura 652 puede utilizar un elemento de Reserva en elementos de parámetros FTM existentes (es decir, usar un elemento de información existente en lugar de agregar un elemento de información adicional al estándar). En otro ejemplo, se puede añadir/agregar un elemento de información de token seguro 654 a la trama estándar de la industria (como se muestra en líneas discontinuas). En un ejemplo, se pueden usar tanto el elemento de información de reserva existente como el elemento de información adjunto.

[0035] En funcionamiento, en referencia a la FIG. 7A, con referencia adicional a la FIG. 4, un proceso 700 para intercambiar mensajes FTM que incluye tokens seguros incluye las etapas mostradas. El proceso 700 es, sin embargo, solo un ejemplo y no es limitativo. El proceso 700 puede alterarse, por ejemplo, agregando, quitando o reorganizando etapas.

[0036] En la etapa 702, una estación de iniciación 402 está configurada para obtener un valor de token seguro inicial y un valor de respuesta de token seguro a través de una señal fuera de banda. La estación de inicio puede establecer un intercambio fuera de banda u otro intercambio negociado previamente con un servidor de posición 152. Por ejemplo, la estación de inicio 402 y otra estación (por ejemplo, el punto de acceso de confianza 108) pueden formar parte de un grupo de confianza formado a través de un servicio en la nube (por ejemplo, Google AP, iCloud). La estación de inicio 402 y la otra estación pueden configurarse para establecer un intercambio fuera de banda 110 basado en procedimientos de cifrado (por ejemplo, intercambiando datos cifrados). El contenido del intercambio fuera de banda 110 puede incluir el valor de token seguro inicial y el valor de respuesta de token seguro, factores y funciones de aleatorización u otra información de seguridad para permitir intercambios de FTM seguros. El valor de token seguro inicial y el valor de respuesta de token seguro pueden almacenarse en la memoria en la estación de inicio 402 e incorporarse en o con el IE de parámetros de FTM. En otro modo de realización, la estación de inicio puede obtener el valor de token seguro inicial y el valor de respuesta de token seguro intercambiando tramas cifradas 802.11. En un modo de realización, el valor de token seguro inicial y el valor de respuesta de token seguro se pueden aleatorizar. El factor de aleatorización de token seguro se puede intercambiar a través del proveedor IE en el iFTMR, FTM.

[0037] En la etapa 704, la estación de inicio 402 está configurada para generar un mensaje de petición de medición de temporización fina (FTM) que incluye el valor de token seguro inicial. El elemento de petición FTM puede corresponder al elemento del parámetro de medición de temporización fina 650 (por ejemplo, IEEE 802.11 REVmc, Fig. 8-570) con la adición de un valor de token seguro inicial en un elemento de información de token seguro 652. En un modo de realización, se puede agregar un elemento de información de token seguro 654 a la trama estándar de la industria.

[0038] En la etapa 706, la estación de inicio 402 está configurada para enviar el mensaje de petición de FTM a una estación de respuesta. En un ejemplo, la estación de inicio 402 está configurada para iniciar una sesión FTM segura enviando un mensaje 410 de iFTMR que incluye la dirección MAC de origen autentificado (M1'). La dirección MAC de origen autentificado incluye el valor de token seguro inicial. La estación de respuesta puede proporcionar un mensaje de confirmación (Ack) 412 utilizando las direcciones MAC autentificadas (por ejemplo, incluyendo el valor de token seguro inicial).

[0039] En la etapa 708, la estación de inicio 402 está configurada para recibir un mensaje de respuesta de FTM que incluye el valor de respuesta de token seguro de la estación de respuesta. En un ejemplo, la estación de respuesta 404 puede proporcionar un mensaje iFTM 414 que incluye el valor de respuesta de token seguro. En un ejemplo, el elemento de respuesta de FTM puede corresponder al elemento del parámetro de medición de temporización fina 650 (por ejemplo, IEEE 802.11 REVmc, Fig. 8-570) con la adición del valor de respuesta de token seguro en un elemento de información de token seguro. Como se analizó, el elemento de información de token seguro 654 se puede agregar como elemento de información adicional a la trama estándar de la industria. La estación de inicio 402 puede proporcionar la confirmación correspondiente 416 usando el valor de token de seguridad inicial.

[0040] En la etapa 710, la estación de inicio 402 está configurada para determinar un valor de tiempo de ida y vuelta (RTT) basado, al menos en parte, en la Respuesta FTM. En un ejemplo, la estación de inicio 402 calcula el tiempo de ida y vuelta registrando el TOA (es decir, t2) del mensaje de respuesta de FTM recibido de una estación de respuesta 404 y registrando el TOD de una trama de confirmación (ACK) del mensaje de respuesta de FTM (es decir, t3). La estación de respuesta 404 registra TOD del mensaje de respuesta de FTM (es decir, t1) y el TOA del mensaje de respuesta de FTM recibido de la estación de inicio (es decir, t4). El RTT se calcula así como RTT = [(t4-t1) - (t3-t2)]. El valor RTT puede usarse para determinar una distancia entre las estaciones de inicio y de respuesta, y posteriormente para el posicionamiento de las estaciones.

[0041] En funcionamiento, en referencia a la FIG. 7B, con referencia adicional a la FIG. 4, un proceso 730 para intercambiar mensajes FTM que incluye direcciones MAC autentificadas incluye las etapas mostradas. El proceso 730 es, sin embargo, solo un ejemplo y no es limitativo. El proceso 730 puede alterarse, por ejemplo, agregando, quitando o reorganizando etapas.

[0042] En la etapa 732, una estación de inicio 402 está configurada para obtener una dirección de control de acceso a medios (MAC) de origen autentificado y una dirección MAC de destino autentificado. En un ejemplo, la dirección de control de acceso a medios (MAC) de origen autentificado y la dirección MAC de destino autentificado pueden realizarse generando nuevas combinaciones de dirección MAC de origen y dirección MAC de destino para la estación de inicio 402 y la estación de respuesta 404 (es decir, el estaciones participantes). Las estaciones participantes pueden implementar a través de hardware y/o software algoritmos de autentificación similares para autentificar (por ejemplo, reconocer, deducir) las combinaciones de direcciones MAC de origen autentificado y destino autentificado entre sí. En un modo de realización, la dirección MAC de origen autentificado y la dirección MAC de destino autentificado pueden ser aleatorizadas por procedimientos fuera de banda. Por ejemplo, se puede usar un factor de aleatorización o una función para generar direcciones MAC sobre la marcha. En un modo de realización, los tokens seguros se pueden usar solos o en combinaciones de uno o más elementos de información (por ejemplo, valores PTSF, TOD, TOA) para modificar la dirección MAC original (por ejemplo, dirección 1 552, dirección 2 554) para obtener la dirección de control de acceso a medios (MAC) de origen autentificado y la dirección MAC de destino autentificado (por ejemplo, elemento de dirección segura 1, 562, elemento de dirección segura 2, 564). Las estaciones participantes pueden usar la combinación de dirección MAC generada como las direcciones MAC de origen y destino de las tramas que transmiten.

[0043] En la etapa 734, la estación de inicio 402 está configurada para generar un mensaje de petición de medición de temporización fina (FTM) que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado. El elemento de petición FTM puede corresponder al elemento del parámetro de medición de temporización fina 650 (por ejemplo, IEEE 802.11 REVmc, Fig. 8-570) con la dirección MAC de origen autentificado y la dirección MAC de destino autentificado incluida en la Dirección 1 552 y la Dirección 2 554. En un ejemplo, la dirección MAC de origen autentificado y la dirección MAC de destino autentificado pueden ser el resultado de las funciones 556, 558 (es decir, la dirección segura 1 562 y la dirección segura 2 564) en la FIG. 5B. En un ejemplo, la dirección MAC de origen autentificado y la dirección MAC de destino autentificado pueden ser el resultado de la función 604 (es decir, la dirección segura 1606 y la dirección segura 2 608) en la FIG. 6A. Se pueden usar otras funciones o tablas de búsqueda para generar la dirección MAC de origen autentificado y la dirección MAC de destino autentificado.

[0044] En la etapa 736, la estación de inicio 402 está configurada para enviar el mensaje de petición de FTM a una estación de respuesta. En un ejemplo, la estación de inicio 402 está configurada para iniciar una sesión FTM segura enviando un mensaje 410 de iFTMR que incluye la dirección MAC de origen autentificado (M1') y la dirección MAC de destino autentificado (M2'). En un ejemplo, el mensaje de petición de FTM incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado en la cabecera de la dirección MAC. La estación de respuesta puede proporcionar un mensaje de confirmación (Ack) 412 utilizando las direcciones MAC autentificadas.

[0045] En la etapa 738, la estación de inicio 402 está configurada para recibir un mensaje de respuesta de FTM que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado de la estación de respuesta. En un ejemplo, la estación de respuesta 404 puede proporcionar un mensaje iFTM 414 que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado en la cabecera de la dirección MAC. La estación de inicio 402 puede proporcionar la confirmación 416 correspondiente utilizando la dirección MAC de origen autentificado y la dirección MAC de destino autentificado en la cabecera de la dirección MAC.

[0046] En la etapa 740, la estación de inicio 402 está configurada para determinar un valor de tiempo de ida y vuelta (RTT) basado, al menos en parte, en la Respuesta FTM. En un ejemplo, la estación de inicio 402 calcula el tiempo de ida y vuelta registrando el TOA (es decir, t2) del mensaje de respuesta de FTM recibido de una estación de respuesta 404 y registrando el TOD de una trama de confirmación (ACK) del mensaje de respuesta de FTM (es decir, t3). La estación de respuesta 404 registra TOD del mensaje de respuesta de FTM (es decir, t1) y el TOA del mensaje de respuesta de FTM recibido de la estación de inicio (es decir, t4). El RTT se calcula así como RTT = [(t4-t1) - (t3-t2)]. El valor RTT puede usarse para determinar una distancia entre las estaciones de inicio y de respuesta, y posteriormente para el posicionamiento de las estaciones.

[0047] Los modos de realización pueden adoptar la forma de un modo de realización enteramente de hardware, un modo de realización enteramente de software (incluyendo firmware, software residente, microcódigo, etc.) o un modo de realización que combina aspectos de software y hardware que pueden denominarse todos, de manera genérica, como un "aparato", "circuito", "módulo" o "sistema" en el presente documento. Además, los modos de realización de la materia inventiva en cuestión pueden adoptar la forma de un producto de programa informático, realizado en cualquier medio de expresión tangible que tenga código de programa utilizable por ordenador incluido en el medio. Los modos de realización descritos pueden proporcionarse como un producto de programa informático, o software, que puede incluir un medio legible por máquina que tiene instrucciones almacenadas en el mismo, que pueden usarse para programar un sistema informático (u otro(s) dispositivo(s) electrónico(s)) para ejecutar (por ejemplo, llevar a cabo) un proceso de acuerdo con los modos de realización, esté descrito actualmente o no, ya que cada variación concebible no está enumerada en el presente documento. Un medio legible por máquina incluye cualquier mecanismo para almacenar o transmitir información en una forma (por ejemplo, software, aplicación de procesamiento) legible por una máquina (por ejemplo, un ordenador). Un medio legible por máquina puede ser un medio de almacenamiento legible por procesador no transitorio, un medio de almacenamiento legible por máquina, o un medio de señales legible por máquina. Un medio de almacenamiento legible por máquina puede incluir, por ejemplo, pero no se limita a, un medio de almacenamiento magnético (por ejemplo, disquete); un medio de almacenamiento óptico (por ejemplo, CD-ROM); un medio de almacenamiento magneto-óptico; una memoria de solo lectura (ROM); una memoria de acceso aleatorio (RAM); una memoria programable borrable (por ejemplo, EPROM y EEPROM); una memoria flash; u otros tipos de medio tangible adecuado para almacenar instrucciones electrónicas. Un medio de señales legibles por máquina puede incluir una señal de datos propagada con un código de programa legible por ordenador, realizado en el mismo, por ejemplo, una señal eléctrica, óptica, acústica u otra forma de señal propagada (por ejemplo, ondas portadoras, señales infrarrojas, señales digitales, etc.). El código de programa realizado en un medio de señales legible por máquina puede transmitirse usando cualquier medio adecuado, incluyendo, pero sin limitarse a, un medio cableado, un medio inalámbrico, de cables de fibra óptica, RF o cualquier otro medio de comunicaciones.

[0048] El código de programa informático para llevar a cabo las operaciones de los modos de realización puede escribirse en cualquier combinación de uno o más lenguajes de programación, incluyendo un lenguaje de programación orientado a objetos, tal como Java, Smalltalk, C++ o similares, y lenguajes de programación de procedimientos convencionales, tales como el lenguaje de programación "C" o lenguajes de programación similares. El código de programa puede ejecutarse completamente en el ordenador de un usuario, parcialmente en el ordenador del usuario, como un paquete de software autónomo, parcialmente en el ordenador del usuario y parcialmente en un ordenador remoto, o completamente en el ordenador o servidor remoto. En el último escenario, el ordenador remoto puede estar conectado al ordenador del usuario a través de cualquier tipo de red, incluyendo una red de área local (LAN), una red de área personal (PAN) o una red de área extensa (WAN), o la conexión puede realizarse con un ordenador externo (por ejemplo, a través de Internet, usando un proveedor de servicios de Internet).

[0049] Con referencia a la FIG. 8A es un diagrama de bloques de un modo de realización de un dispositivo electrónico 800 para su uso en el intercambio de mensajes FTM seguros. En algunas implementaciones, el dispositivo electrónico 800 puede ser una estación cliente 120 incorporada en un dispositivo como un ordenador portátil, una tablet, una netbook, un teléfono móvil, un teléfono inteligente, una consola de juegos, un asistente digital personal (PDA) o una etiqueta de inventario. El dispositivo electrónico 800 pueden ser otros sistemas electrónicos tales como un dispositivo Home Node B (HNB) con un transceptor inalámbrico y capacidades de posicionamiento (por ejemplo, un tipo de punto de acceso). El dispositivo electrónico 800 incluye una unidad procesadora 802 (que incluye posiblemente múltiples procesadores, múltiples núcleos, múltiples nodos y/o que implementa múltiples hilos, etc.). El dispositivo electrónico 800 incluye una unidad de memoria 806. La unidad de memoria 806 puede ser una memoria de sistema (por ejemplo, una o más entre una memoria caché, una SRAM, una DRAM, una RAM sin condensadores, una RAM con dos transistores, una eDRAM, una EDO RAM, una DDR RAM, una EEPROM, una NRAM, una RRAM, una SONOS, una PRAM, etc.) o una cualquiera o más de las posibles modos de realización, ya descritos anteriormente, de medios legibles por máquina. El dispositivo electrónico 800 incluye además un bus 810 (por ejemplo, PCI, ISA, PCI-Express, HyperTransport.RTM, InfiniBand.RTM., NuBus, AHB, AXI, etc.) e interfaces de red 804 que incluyen al menos una entre una interfaz de red inalámbrica (por ejemplo, una interfaz de WLAN, una interfaz Bluetooth.RTM., una interfaz WiMAX, una interfaz ZigBee.RTM, una interfaz de USB inalámbrica, etc.) y una interfaz de red cableada (por ejemplo, una interfaz de Ethernet, etc.).

[0050] El dispositivo electrónico 800 incluye además una unidad de comunicación 808. La unidad de comunicación 808 comprende una unidad de posicionamiento 812, un receptor 814, un transmisor 816 y una o más antenas 818. El transmisor 816, las antenas 818 y el receptor 814 forman un módulo de comunicación inalámbrica (siendo el transmisor

816 y el receptor 814 un transceptor 820). El transmisor 816 y el receptor 814 están configurados para comunicarse bidireccionalmente con una o más estaciones cliente y otros puntos de acceso a través de una antena 818 correspondiente. En algunos modos de realización, el dispositivo electrónico 800 puede configurarse como una estación WLAN con capacidades de determinación de posicionamiento (por ejemplo, un tipo de punto de acceso). La unidad de posicionamiento 812 puede utilizar la información de sesión FTM segura intercambiada con los puntos de acceso para determinar la información de temporización RSS y/o TDOA asociada con los puntos de acceso. La unidad de posicionamiento 812 puede determinar la posición del dispositivo electrónico 800 basándose, al menos en parte, en la información de temporización TDOA y la información de posición AP, como se describió anteriormente. En un ejemplo, el dispositivo electrónico 800 incluye un módulo de generación de tokens 822 configurado para obtener tokens seguros (por ejemplo, a través de intercambios fuera de banda) y generar la dirección MAC de origen autentificado y la dirección MAC de destino autentificado como se describe. Un módulo de autentificación 824 puede configurarse para autentificar (por ejemplo, verificar) tokens seguros y direcciones MAC recibidas en un intercambio FTM seguro. Por ejemplo, el módulo de autentificación 824 puede incluir algoritmos de autentificación u otros elementos de software para comparar la dirección MAC con los valores de la tabla de búsqueda, o para revertir los procesos de generación de tokens como se indica en las Funciones 1-10 anteriores. Además, en este modo de realización, los puntos de acceso pueden usar sus capacidades de procesamiento para ejecutar sus respectivas operaciones descritas anteriormente. Cualquiera de estas funcionalidades puede implementarse parcial (o totalmente) en hardware y/o en la unidad de procesador 802. Por ejemplo, la funcionalidad puede implementarse con un circuito integrado específico de la aplicación, en la lógica implementada en la unidad de procesador 802, en un coprocesador en un dispositivo periférico o tarjeta, etc. Además, los modos de realización pueden incluir menos componentes o componentes adicionales no ilustrados en la FIG. 8A (por ejemplo, pantalla, tarjetas de vídeo, tarjetas de audio, interfaces de red adicionales, dispositivos periféricos, etc.). La unidad de procesador 802. la unidad de memoria 806 y las interfaces de red 804 están acopladas al bus 810. Aunque se ilustra como acoplada al bus 810, la unidad de memoria 806 puede estar acoplada a la unidad de procesador 802.

[0051] Con referencia a la FIG. 8B, un ejemplo de un sistema transceptor inalámbrico tal como una estación 850 comprende un sistema informático que incluye un procesador 851, memoria 852 que incluye software 854, un transmisor 856, antenas 858 y un receptor 860. Los puntos de acceso 102, 104, 106, 108 pueden configurarse como la estación 850 de la FIG. 8B. El transmisor 856, las antenas 858 y el receptor 860 forman un módulo de comunicación inalámbrica (siendo el transmisor 856 y el receptor 860 un transceptor 862). El transmisor 856 está conectado a una de las antenas 858 y el receptor 860 está conectado a otra de las antenas 858. Otras estaciones de ejemplo pueden tener diferentes configuraciones, por ejemplo, con una sola antena 858 y/o con múltiples transmisores 856 y/o múltiples receptores 860. El transmisor 856 y el receptor 860 están configurados de modo que la estación 850 pueda comunicarse bidireccionalmente con la estación cliente 120 a través de las antenas 858. El procesador 851 es preferentemente un dispositivo de hardware inteligente, por ejemplo, una unidad central de procesamiento (CPU) como las fabricadas por ARM®, Intel® Corporation o AMD®, un microcontrolador, un circuito integrado específico de aplicación (ASIC), etc. el procesador 851 podría comprender múltiples entidades físicas separadas que pueden distribuirse en la estación 850. La memoria 852 incluye una memoria de acceso aleatorio (RAM) y una memoria de solo lectura (ROM). La memoria 852 es un medio de almacenamiento legible por procesador que almacena el software 854 que es legible por procesador, el código de software ejecutable por procesador que contiene instrucciones legibles por procesador que están configuradas para, cuando se ejecutan, hacer que el procesador 851 realice varias funciones descritas en el presente documento (aunque la descripción puede referirse solo al procesador 851 que realiza las funciones). De forma alternativa, el software 854 puede no ejecutarse directamente mediante el procesador 851 sino configurarse para hacer que el procesador 851, por ejemplo, al compilarse y ejecutarse, realice las funciones. En un ejemplo, la estación 850 incluye un módulo de generación de tokens 864 configurado para obtener tokens seguros (por ejemplo, a través de intercambios fuera de banda) y generar la dirección MAC de origen autentificado y la dirección MAC de destino autentificado como se describe. Un módulo de autentificación 866 puede configurarse para autentificar (por ejemplo, verificar) tokens seguros y direcciones MAC recibidas en un intercambio FTM seguro. Por ejemplo, el módulo de autentificación 866 puede incluir algoritmos de autentificación o elementos de software para comparar la dirección MAC con los valores de la tabla de búsqueda o para revertir los procesos de generación de tokens como se indica en las Funciones 1-10 anteriores.

[0052] Aunque los modos de realización se describen con referencia a varias implementaciones y usos, se entenderá que estos modos de realización son ilustrativos y que el alcance de la materia objeto de la invención no está limitado a los mismos. En general, pueden implementarse técnicas para posicionamiento con informes contiguos de protocolos de consulta de red de acceso, como se describe en el presente documento, con utilidades compatibles con cualquier sistema de hardware, o sistemas de hardware. Muchas variaciones, modificaciones, adiciones y mejoras son posibles.

[0053] Pueden proporcionarse varias instancias de componentes, operaciones o estructuras descritos en el presente documento como una única instancia. Finalmente, los límites entre varios componentes, operaciones y almacenes de datos son en cierto modo arbitrarios, y las operaciones particulares se ilustran en el contexto de configuraciones ilustrativas específicas. Pueden concebirse otras asignaciones de funcionalidad, las cuales pueden quedar dentro del alcance de la materia objeto de la invención. En general, las estructuras y la funcionalidad presentadas como componentes independientes en las configuraciones a modo de ejemplo pueden implementarse como una estructura o componente combinados. De manera similar, las estructuras y la funcionalidad presentadas como un único

componente pueden implementarse como componentes individuales. Estas y otras variaciones, modificaciones, adiciones y mejoras pueden quedar dentro del alcance de la materia objeto de la invención.

[0054] Como se usa en el presente documento, incluidas las reivindicaciones, a menos que se indique lo contrario, una declaración de que una función u operación está "basada en" un elemento o condición significa que la función u operación se basa en el elemento o condición indicada y puede basarse en uno o más elementos y/o condiciones además del elemento o condición indicada.

[0055] Además, se puede divulgar más de una invención.

REIVINDICACIONES

1. Un aparato (402) para proporcionar un intercambio de medición de temporización fina, FTM, segura que comprende:

medios para obtener un valor de token seguro inicial y una función de respuesta de token seguro mediante una señal fuera de banda, en el que la función de respuesta de token seguro está asociada con el valor de token seguro inicial;

medios para generar un mensaje de petición FTM que incluye el valor de token seguro inicial;

medios para enviar el mensaje de petición de FTM a una estación de respuesta;

medios para recibir un mensaje de respuesta de FTM que incluye un valor de respuesta de token seguro desde la estación de respuesta, en el que el valor de respuesta de token seguro es el resultado de realizar la función de respuesta de token seguro en un campo de función de sincronización de temporización parcial, PTSF, en el mensaje de respuesta de FTM; y

medios para determinar un valor de tiempo de ida y vuelta, RTT, basado al menos en parte en el mensaje de respuesta de FTM.

2. El aparato de acuerdo de la reivindicación 1, en el que el mensaje de petición de FTM que incluye el valor de token seguro inicial incluye una trama de cabecera de control de acceso a medios, MAC, con un elemento de información de token seguro.

3. El aparato de la reivindicación 1, en el que el mensaje de petición de FTM que incluye el valor de token seguro inicial incluye un campo de parámetro FTM con un elemento de información de token seguro.

4. El aparato de la reivindicación 3, en el que el elemento de información de token seguro se agrega al campo de parámetro FTM.

5. El aparato de la reivindicación 1, en el que el valor de respuesta de token seguro es el resultado de realizar la función de respuesta de token seguro en el campo de función de sincronización de temporización parcial, PTSF, y un campo de hora de llegada, TOA, en el mensaje de respuesta de FTM.

6. El aparato de la reivindicación 1, en el que el valor de respuesta de token seguro es el resultado de realizar la función de respuesta de token seguro en el campo de función de sincronización de temporización parcial, PTSF, y un campo de hora de salida, TOD, en el mensaje de respuesta de FTM.

7. El aparato de la reivindicación 1 que comprende además medios para determinar una posición basada al menos en parte en el valor RTT.

8. Un sistema transceptor inalámbrico (800) para proporcionar un intercambio de medición de temporización fina, FTM, segura que comprende:

una memoria (806); y,

un aparato de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que:

los medios para obtener el valor de token seguro inicial y una función de respuesta de token seguro, los medios para generar el mensaje de petición FTM y los medios para determinar el valor del tiempo de ida y vuelta, RTT, comprenden un procesador;

los medios para enviar el mensaje de petición de FTM comprenden un transmisor (816); y

los medios para recibir el mensaje de respuesta de FTM comprenden un receptor (814).

9. Un procedimiento para participar en un intercambio de medición de temporización fina, FTM, segura que comprende:

obtener una dirección control de acceso a medios, MAC, de origen autentificado, y una dirección MAC de destino autentificado realizando una función de aleatorización en una dirección MAC de origen original y una dirección MAC de destino original, en el que al menos un elemento de información de campo de parámetro FTM es una entrada para la función de aleatorización;

generar un mensaje de petición FTM que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado;

enviar el mensaje de petición de FTM a una estación de respuesta;

recibir un mensaje de respuesta de FTM que incluye la dirección MAC de origen autentificado y la dirección MAC de destino autentificado de la estación de respuesta; y

determinar un valor de tiempo de ida y vuelta, RTT, basado al menos en parte en el mensaje de respuesta de FTM.

10. El procedimiento según la reivindicación 9, en el que obtener la dirección MAC de origen autentificado y la dirección MAC de destino autentificado comprende recibir la función de aleatorización a través de un intercambio fuera de banda con un servidor de posición.

11. El procedimiento según la reivindicación 9, en el que el al menos un elemento de información de campo de parámetro FTM es un campo de función de sincronización de temporización parcial, PTSF.

12. El procedimiento según la reivindicación 9, en el que al menos uno de un Tiempo de salida, TOD o un Tiempo de llegada, TOA, del mensaje de Respuesta FTM es una entrada a la función de aleatorización.

13. El procedimiento según la reivindicación 9, que comprende además recibir un token seguro a través de un intercambio fuera de banda con un servidor de posición, en el que el token seguro es una entrada a la función de aleatorización.

14. Un medio de almacenamiento legible por procesador no transitorio que comprende instrucciones para participar en un intercambio de medición de temporización fina, FTM, segura de acuerdo con el procedimiento de cualquiera de las reivindicaciones 9 a 13.

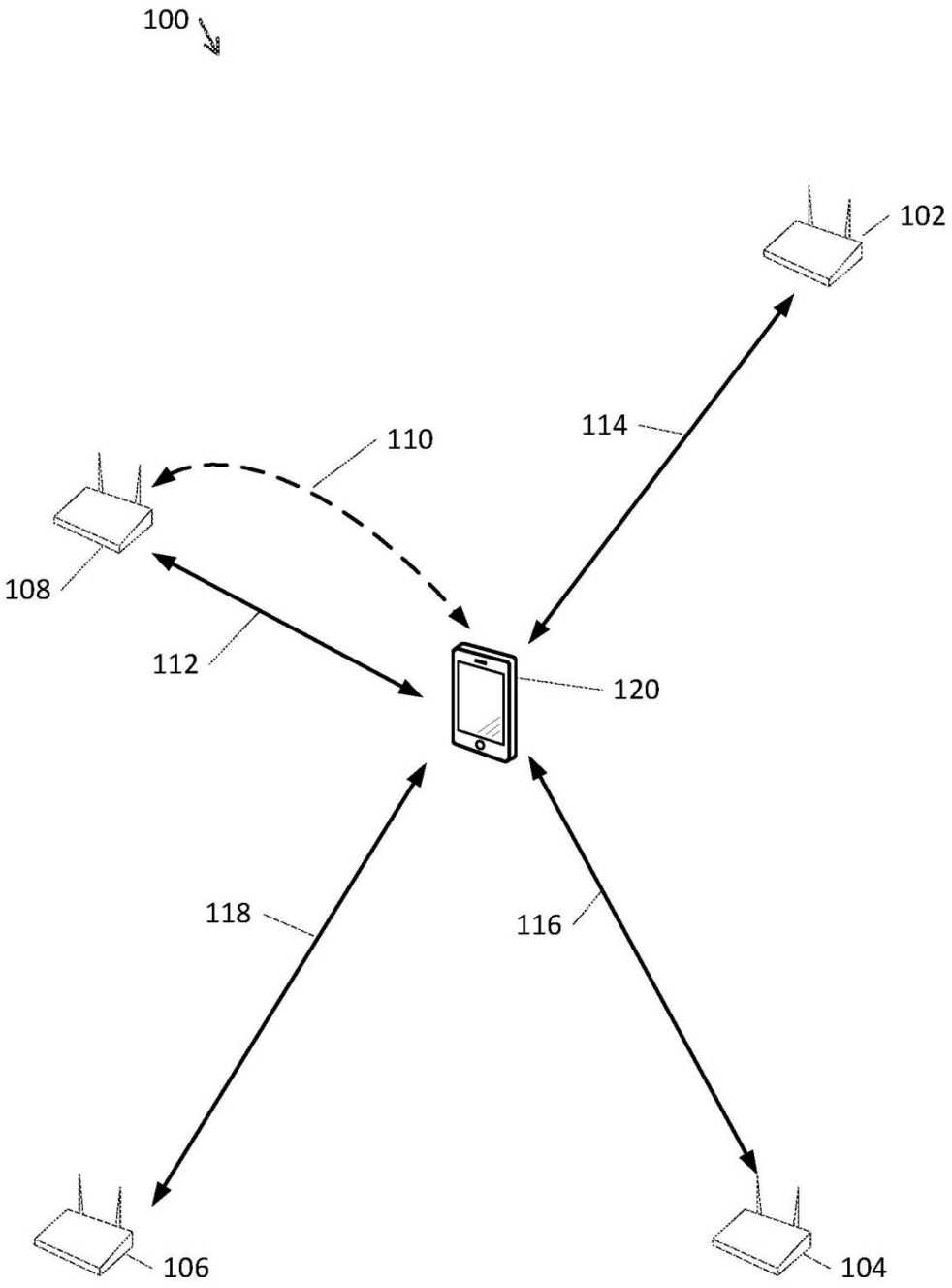


FIG. 1A

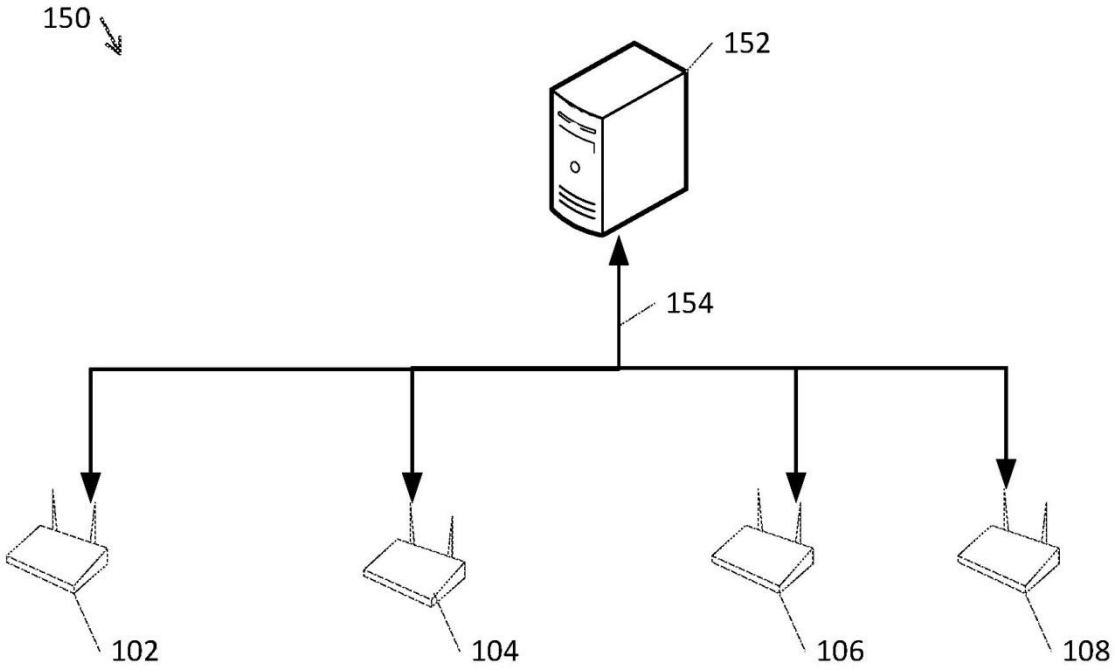


FIG. 1B

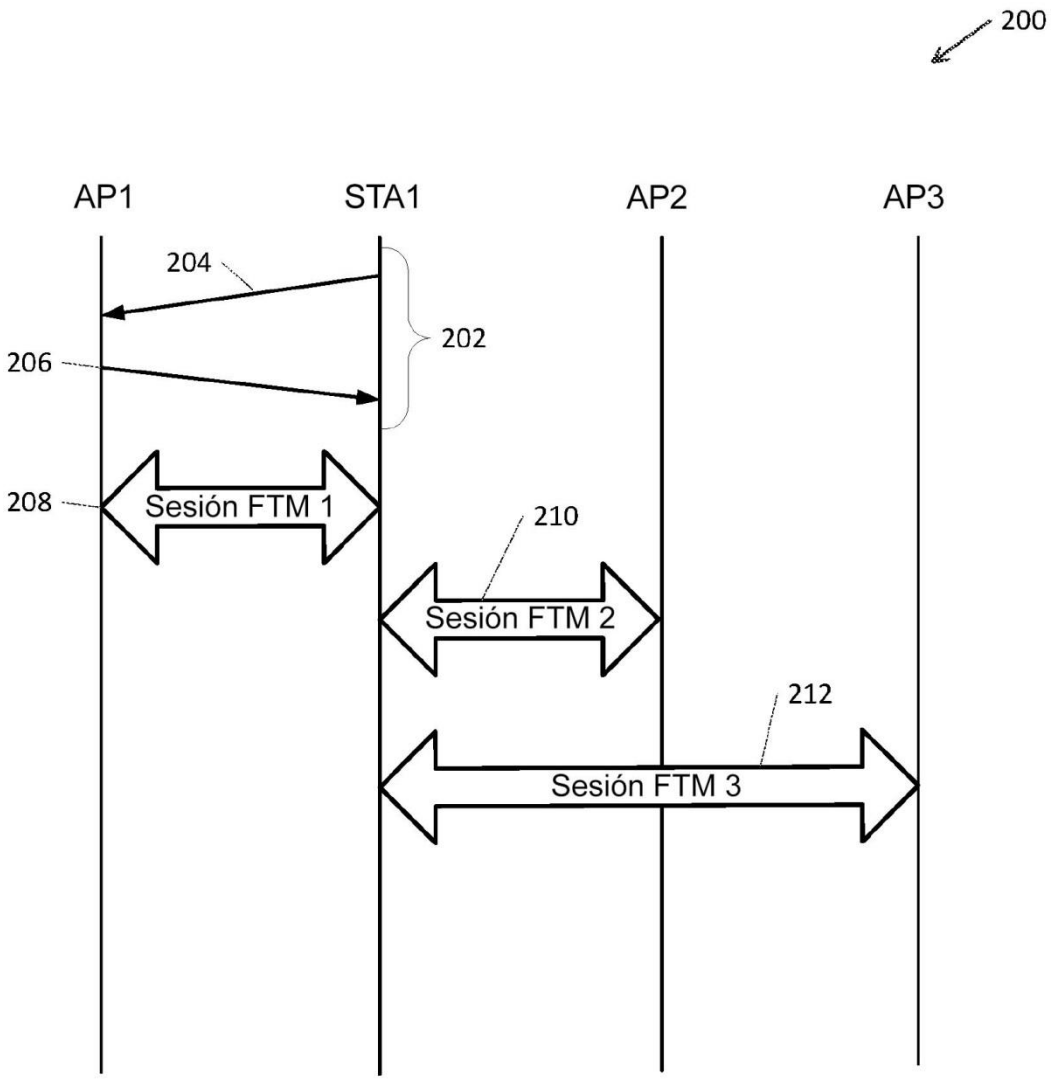
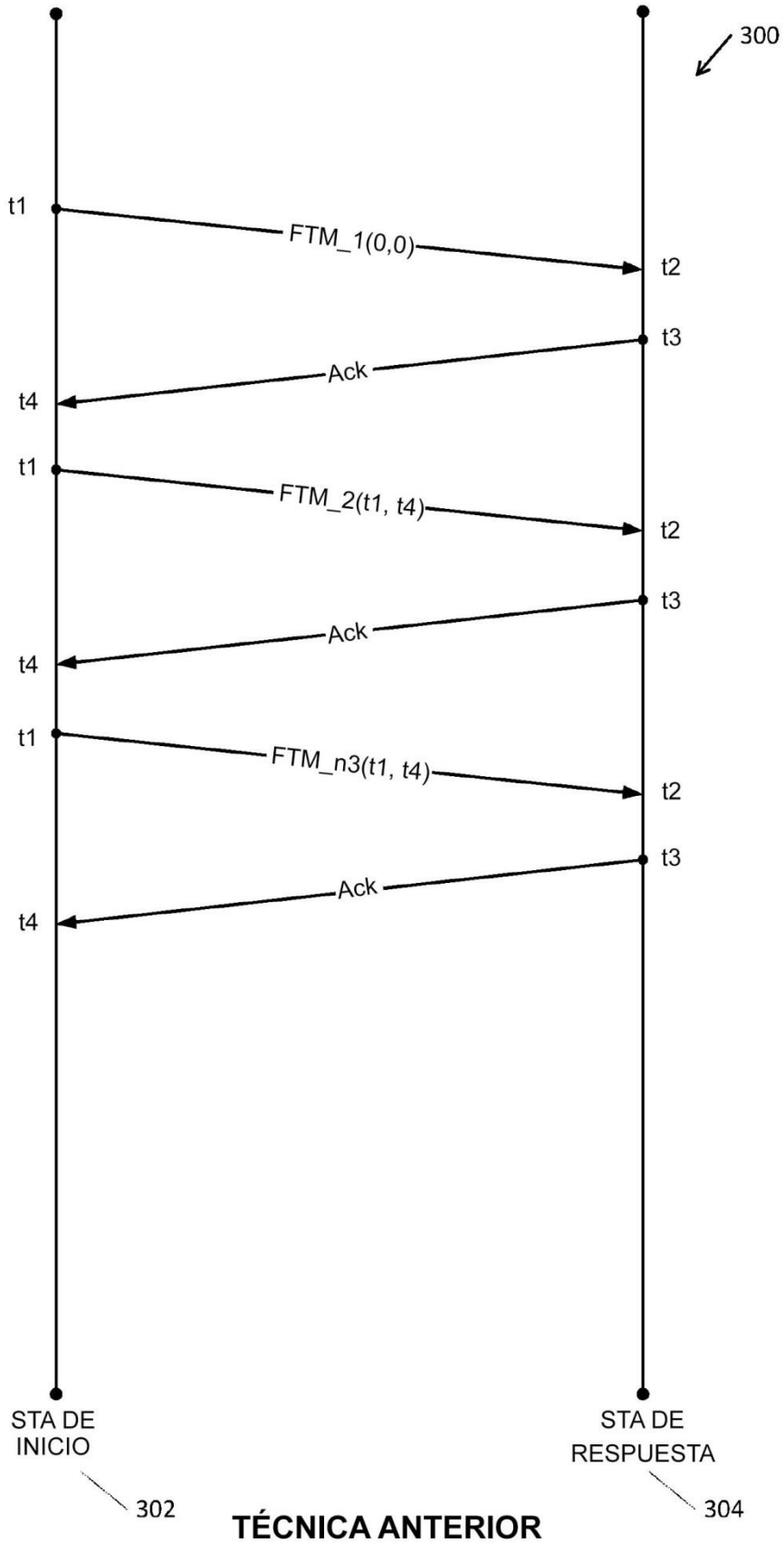

200
AP1
STA1
AP2
AP3
204
202
206
208
Sesión FTM 1
210
Sesión FTM 2
212
Sesión FTM 3

FIG. 2



TÉCNICA ANTERIOR

FIG. 3

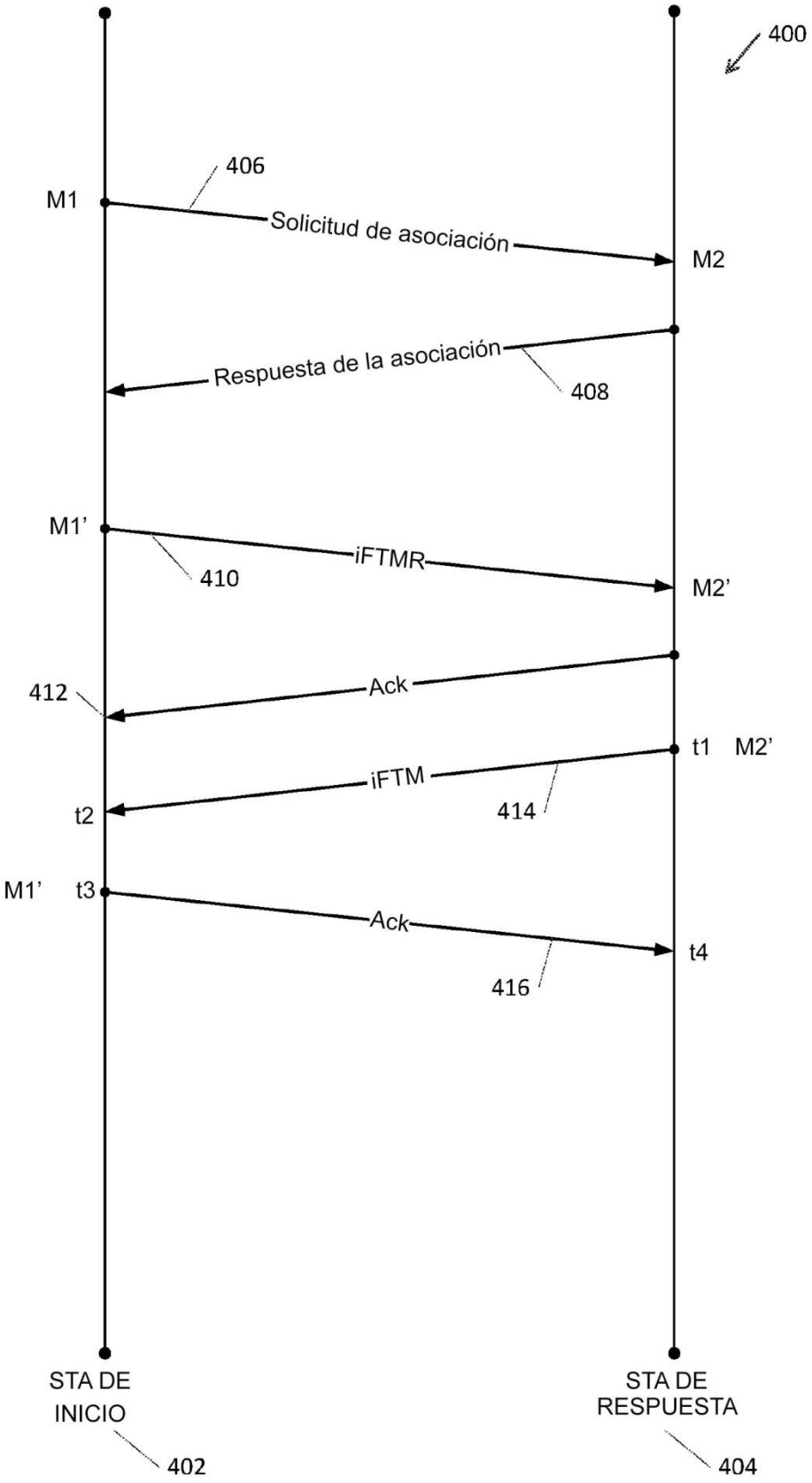

400
406
M1
Solicitud de asociación
M2
Respuesta de la asociación
408
M1'
iFTMR
410
M2'
412
Ack
t1 M2'
iFTM
414
t2
M1' t3
Ack
t4
416
STA DE INICIO
402
STA DE RESPUESTA
404

FIG. 4


500
502
Control de tramas
Duración/ID
Dirección 1
Dirección 2
Dirección 3
Token seguro
...
Control de secuencia
Dirección 4
Control de QoS
Control HT
Cuerpo de la trama
FCS

FIG. 5A

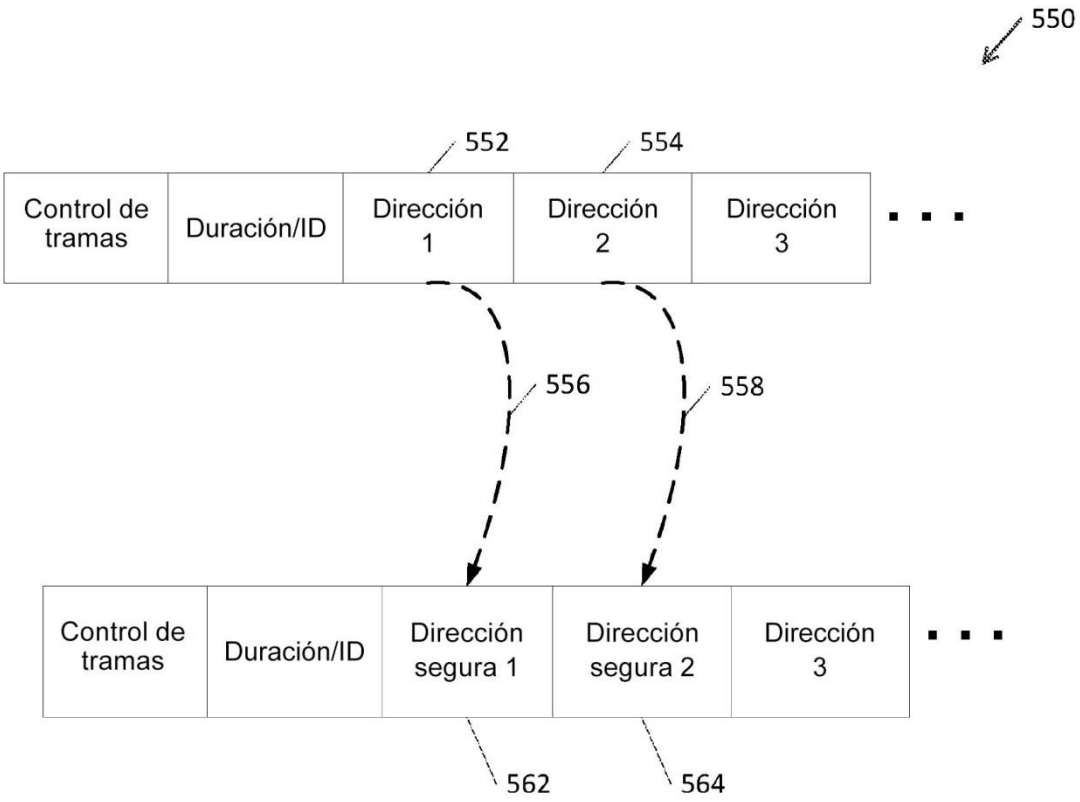

550
552
554
Control de tramas
Duración/ID
Dirección 1
Dirección 2
Dirección 3
556
558
Control de tramas
Duración/ID
Dirección segura 1
Dirección segura 2
Dirección 3
562
564

FIG. 5B

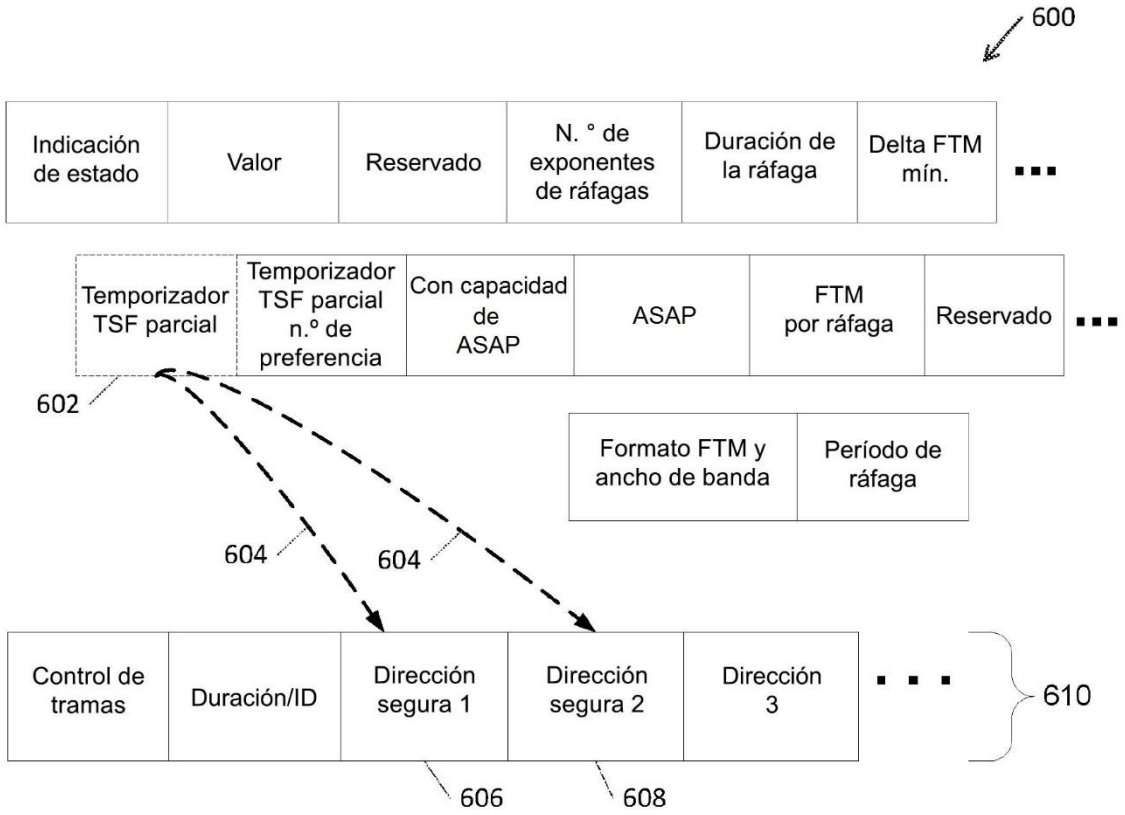

600
Indicación de estado
Valor
Reservado
N. ° de exponentes de ráfagas
Duración de la ráfaga
Delta FTM mín.
Temporizador TSF parcial
Temporizador TSF parcial n.º de preferencia
Con capacidad de ASAP
ASAP
FTM por ráfaga
Reservado
602
Formato FTM y ancho de banda
Período de ráfaga
604
604
Control de tramas
Duración/ID
Dirección segura 1
Dirección segura 2
Dirección 3
610
606
608

FIG. 6A

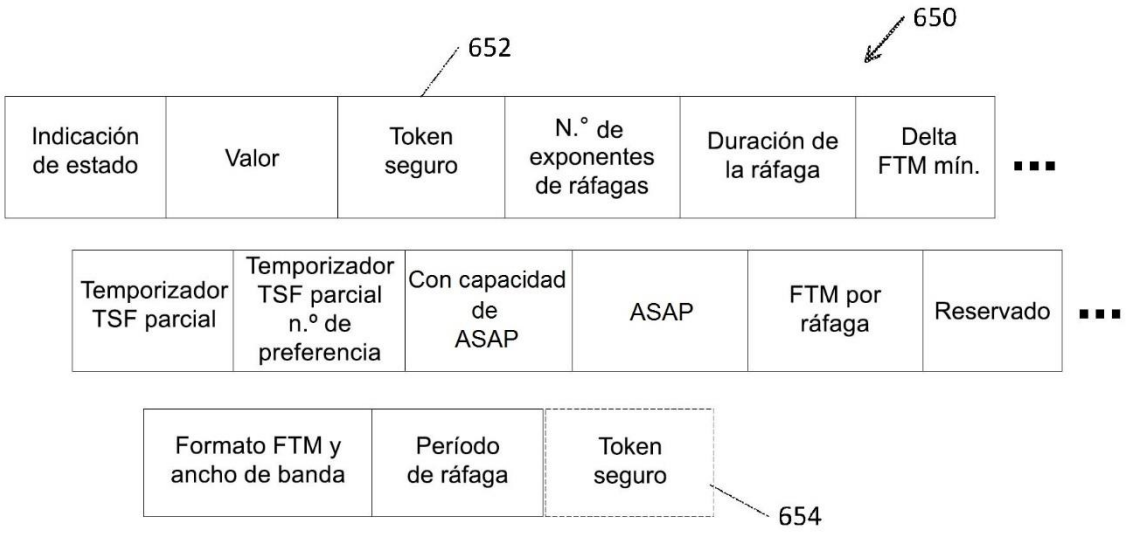

650
652
Indicación de estado
Valor
Token seguro
N.° de exponentes de ráfagas
Duración de la ráfaga
Delta FTM mín.
Temporizador TSF parcial
Temporizador TSF parcial n.º de preferencia
Con capacidad de ASAP
ASAP
FTM por ráfaga
Reservado
Formato FTM y ancho de banda
Período de ráfaga
Token seguro
654

FIG. 6B

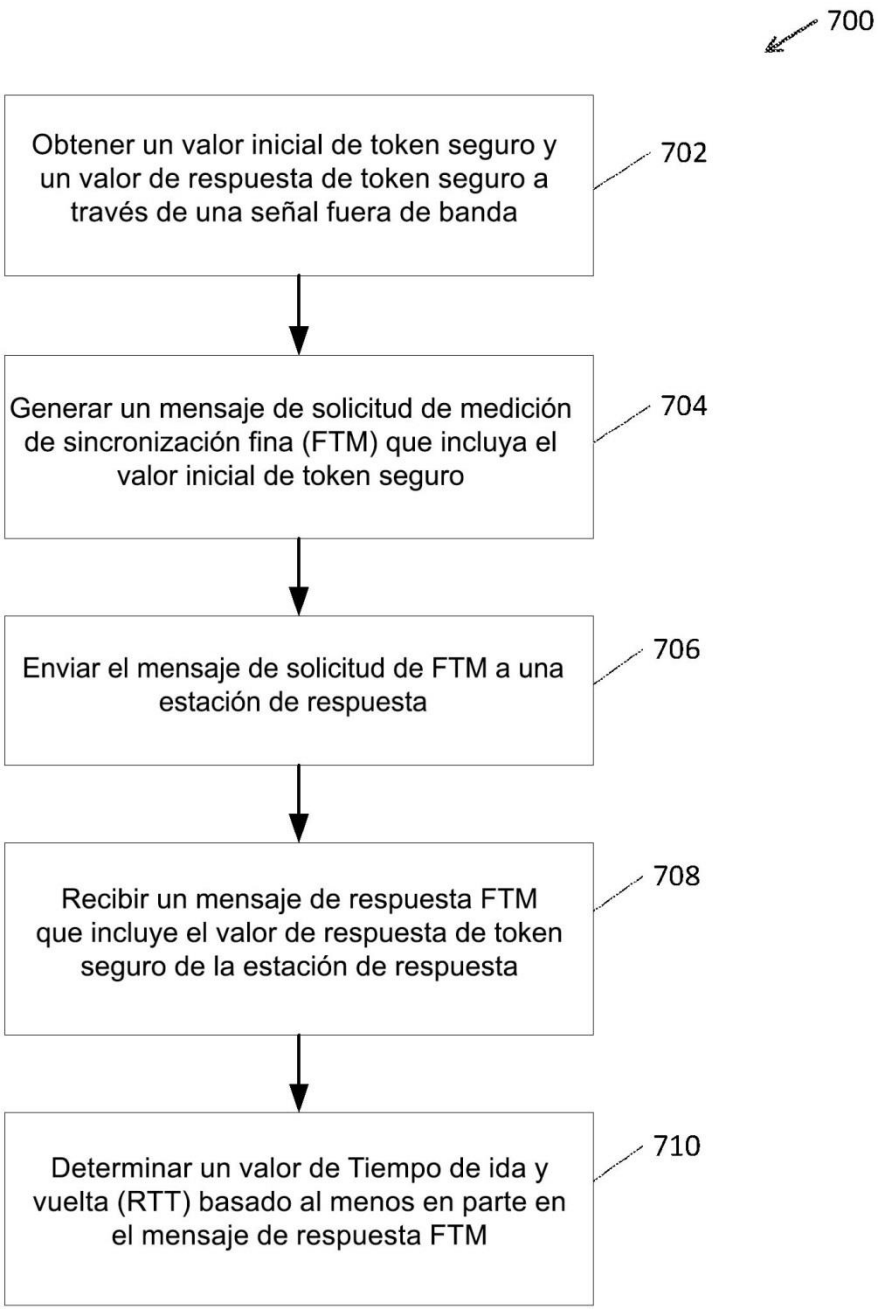

700
Obtener un valor inicial de token seguro y un valor de respuesta de token seguro a través de una señal fuera de banda
702
Generar un mensaje de solicitud de medición de sincronización fina (FTM) que incluya el valor inicial de token seguro
704
Enviar el mensaje de solicitud de FTM a una estación de respuesta
706
Recibir un mensaje de respuesta FTM que incluye el valor de respuesta de token seguro de la estación de respuesta
708
Determinar un valor de Tiempo de ida y vuelta (RTT) basado al menos en parte en el mensaje de respuesta FTM
710

FIG. 7A

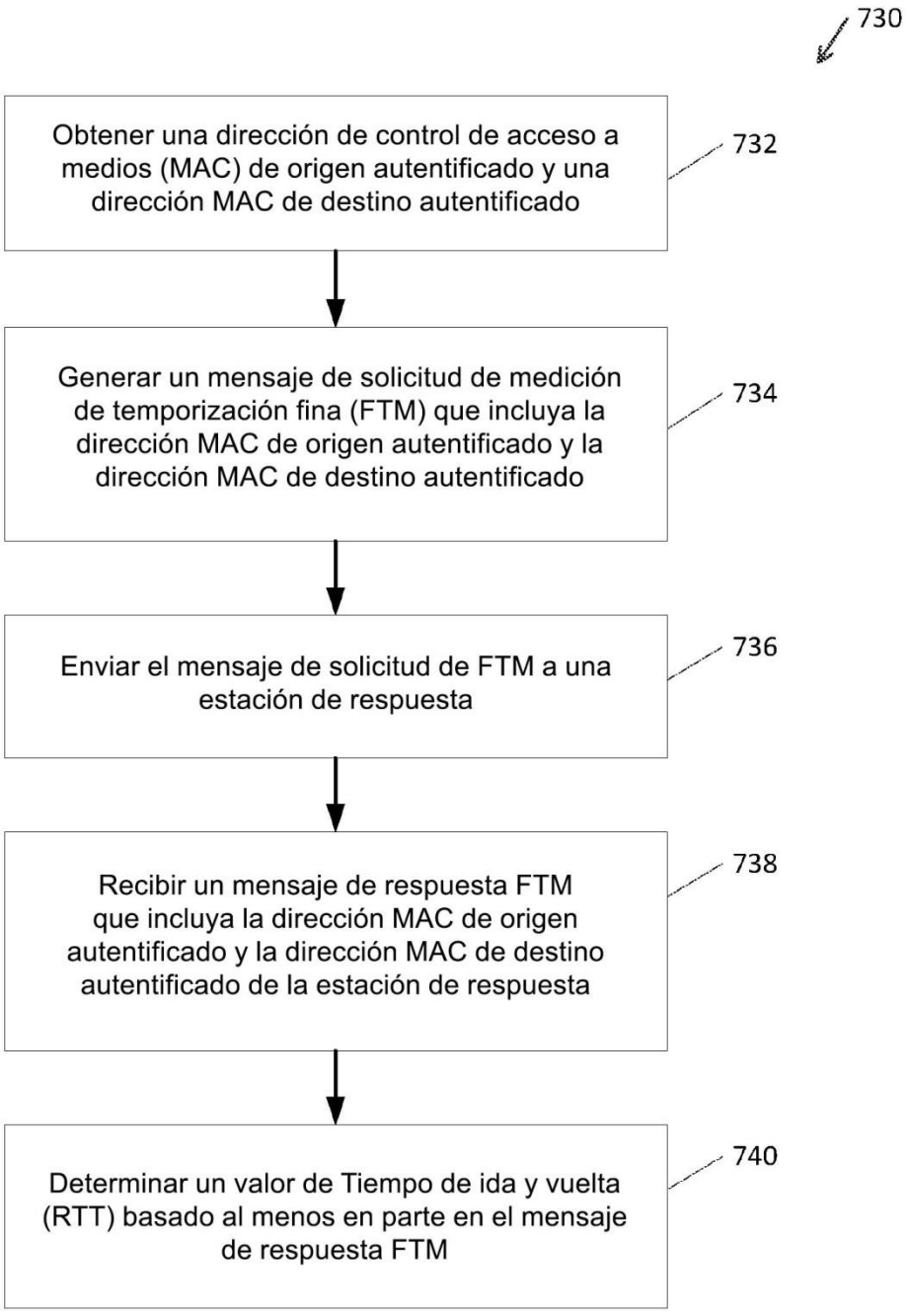

730
Obtener una dirección de control de acceso a medios (MAC) de origen autentificado y una dirección MAC de destino autentificado
732
Generar un mensaje de solicitud de medición de temporización fina (FTM) que incluya la dirección MAC de origen autentificado y la dirección MAC de destino autentificado
734
Enviar el mensaje de solicitud de FTM a una estación de respuesta
736
Recibir un mensaje de respuesta FTM que incluya la dirección MAC de origen autentificado y la dirección MAC de destino autentificado de la estación de respuesta
738
Determinar un valor de Tiempo de ida y vuelta (RTT) basado al menos en parte en el mensaje de respuesta FTM
740

FIG. 7B

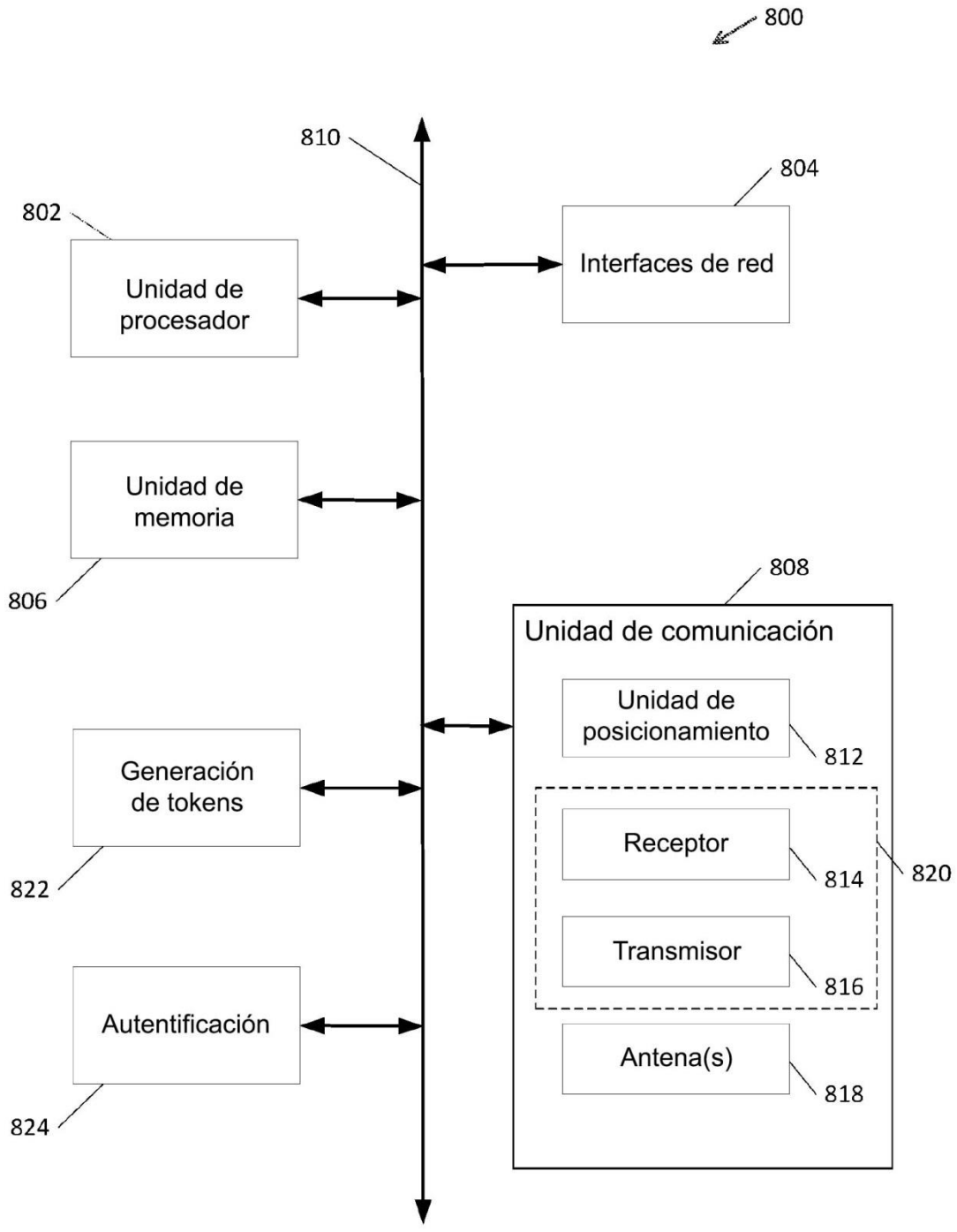

800
810
804
802
Interfaces de red
Unidad de procesador
Unidad de memoria
806
808
Unidad de comunicación
Unidad de posicionamiento
812
Generación de tokens
Receptor
814
820
822
Transmisor
816
Autentificación
Antena(s)
818
824

FIG. 8A

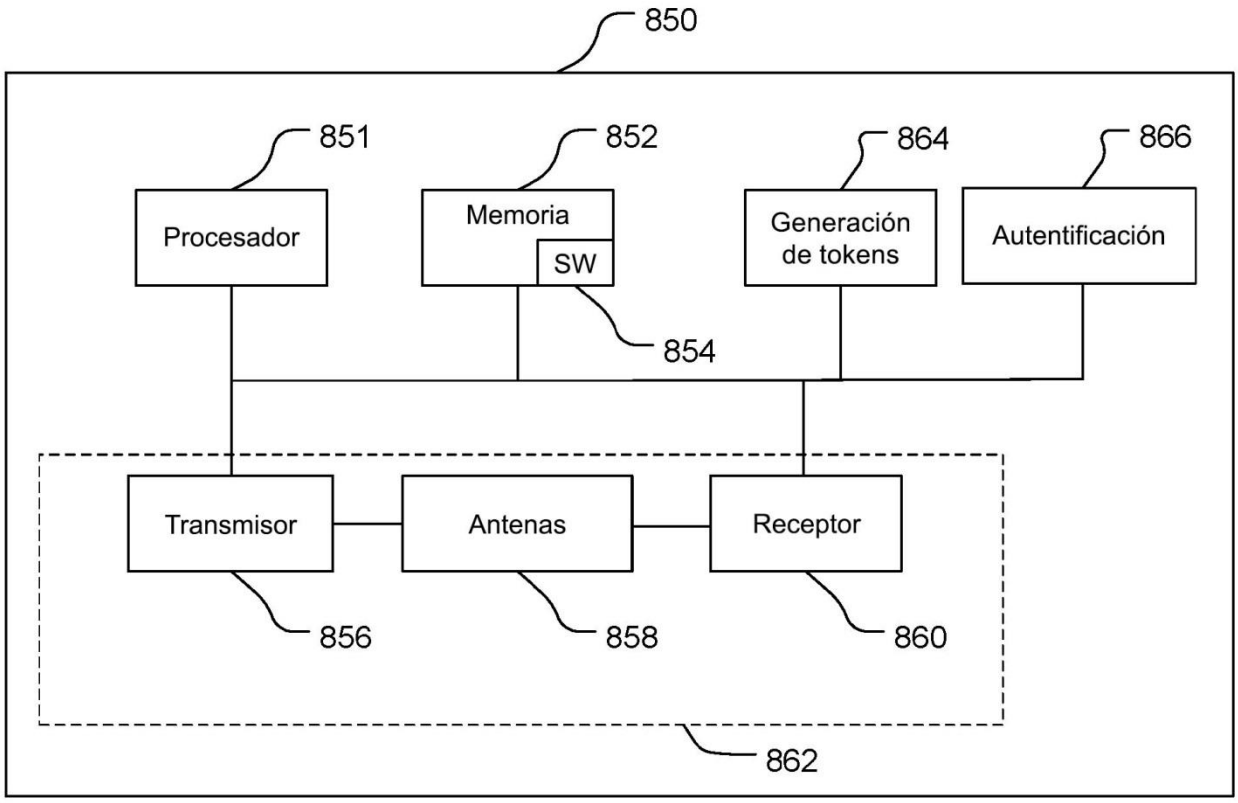

850
851
852
864
866
Procesador
Memoria
SW
Generación de tokens
Autentificación
854
Transmisor
Antenas
Receptor
856
858
860
862

FIG. 8B