

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 877 358**

51 Int. Cl.:

H04W 12/02 (2009.01)

H04W 12/12 (2011.01)

H04L 29/06 (2006.01)

H04L 9/12 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **30.03.2015** **PCT/US2015/023395**

87 Fecha y número de publicación internacional: **08.10.2015** **WO15153489**

96 Fecha de presentación y número de la solicitud europea: **30.03.2015** **E 15772432 (9)**

97 Fecha y número de publicación de la concesión europea: **12.05.2021** **EP 3127309**

54 Título: **Transmisión de un mensaje de baliza**

30 Prioridad:

04.04.2014 CN 201410136738

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

16.11.2021

73 Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD.
(100.0%)

Cayman Corporate Centre, 27 Hospital Road
George Town, Grand Cayman KY1-9008, KY

72 Inventor/es:

QIN, JIAN

74 Agente/Representante:

ARIAS SANZ, Juan

ES 2 877 358 T3

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

DESCRIPCIÓN

Transmisión de un mensaje de baliza

Referencia cruzada a solicitudes de patente relacionadas

Esta solicitud reivindica la prioridad de la solicitud de patente china n.º 201410136738.0, presentada el 4 de abril de 2014, titulada "Method and Device for Transmission of Beacon Message for Beacon-based Service".

Campo técnico

Esta presente divulgación se refiere a una tecnología de red de comunicación, más particularmente, a una transmisión de datos de baliza.

Antecedentes

Con la popularidad de la tecnología de teléfonos inteligentes, el dispositivo móvil se ha arraigado profundamente en la vida de las personas. Por ejemplo, usando la tecnología de posicionamiento móvil, los dispositivos móviles proporcionan a los usuarios servicios personalizados y localizados.

El GPS (sistema de posicionamiento global) es actualmente una tecnología de posicionamiento ampliamente usada. Sin embargo, cuando un receptor GPS funciona en una sala, la sala atenúa la señal y disminuye la precisión del GPS. Recientemente, se han desarrollado tecnologías de posicionamiento en interiores, tales como WiFi (fidelidad inalámbrica), ZigBee, Bluetooth y red de comunicación inalámbrica de banda ultraancha.

Las balizas implementan una tecnología de posicionamiento en interiores y proporcionan una solución prometedora para el posicionamiento en el interior de edificios. Las balizas generan tramas de radio y transmiten a dispositivos móviles en una determinada región de señales de baliza. Sin embargo, puesto que las aplicaciones que residen en los dispositivos móviles pueden recuperar información sensible del usuario durante la comunicación entre las balizas y los dispositivos móviles, la seguridad se ha vuelto un problema para comercializar la tecnología de balizas.

El documento EP 1355468 da a conocer un método y aparato que incorporan un sistema para permitir la modificación adaptativa del nivel de seguridad de un nodo en una red. El sistema puede aplicarse particularmente a redes dinámicas, es decir, redes en las que los nodos pueden ser móviles y en las que la topología de red no es constante. El nodo recibe señales de baliza desde otros nodos en la red, proporcionando dichas señales una indicación del nivel de alerta de los otros nodos y una indicación de si los otros nodos son elementos fiables de la red. El nivel de alerta del nodo se determina basándose en las señales recibidas.

El documento WO 2008/021041 da a conocer sistemas y métodos para llevar a cabo autenticación de transacciones y telefonía segura a través de dispositivos electrónicos. Más específicamente, la explicación se refiere a sistemas y métodos para llevar a cabo telefonía de red segura, incluyendo pero sin limitarse a comunicaciones a través de internet, otras redes informáticas, redes por cable o inalámbricas, o audio, vídeo o multimedia, incluyendo un método de enviar datos desde un primer usuario a un segundo usuario durante una sesión de comunicación que comprende las etapas de: generar una clave; cifrar dicha clave para formar una clave cifrada; enviar dicha clave cifrada al segundo usuario para descifrar dicha clave cifrada en dicho segundo usuario; iniciar la sesión de comunicación entre el primer usuario y el segundo usuario; cifrar primeros datos relacionados con un primer evento de comunicación con dicha clave para formar primeros datos cifrados; y enviar dichos primeros datos cifrados relacionados con un primer evento de comunicación desde dicho primer usuario a dicho segundo usuario para descifrar dichos primeros datos cifrados usando dicha clave descifrada por dicho segundo usuario.

Sumario

Este sumario se proporciona para presentar una selección de conceptos de forma simplificada que se describen adicionalmente a continuación en la descripción detallada. No se pretende que este sumario identifique todas las características clave o características esenciales del contenido reivindicado, ni se pretende que se use sólo como ayuda para determinar el alcance del contenido reivindicado. El término "técnicas", por ejemplo, puede referirse a aparato(s), sistema(s), método(s) y/o instrucciones ejecutables por ordenador tal como se permita por el contexto anterior y en la totalidad de la presente divulgación.

Implementaciones de esta presente divulgación se refieren a métodos para transmitir un mensaje de baliza, según la reivindicación 1.

Implementaciones de esta presente divulgación se refieren además a uno o más medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador que, cuando se ejecutan por uno o más procesadores, ordenan que el uno o más procesadores realicen acciones. Las acciones son tal como se describen en la reivindicación 4.

Implementaciones de esta presente divulgación se refieren además a un sistema tal como se describe en la reivindicación 8.

Implementaciones de esta presente divulgación se refieren además a otro sistema, tal como se describe en la reivindicación 11.

- 5 Implementaciones de esta presente divulgación pueden generar un cifrado variable en el tiempo asociado con el ID de baliza de tal manera que un programa malicioso (*malware*) no autorizado no pueda obtener un ID real y estable de la baliza. Por tanto, es difícil falsificar ID de baliza correspondientes a servicios, lo que puede involucrar información sensible del usuario. Esto protege el interés del usuario y mejora la seguridad de red de balizas.

Breve descripción de los dibujos

La descripción detallada se describe con referencia a las figuras adjuntas. El uso de los mismos números de referencia en diferentes figuras indica elementos similares o idénticos.

- 10 La figura 1 es un diagrama esquemático de un entorno informático ilustrativo, que permite la transmisión de un mensaje de baliza.

La figura 2 es un diagrama de flujo de un procedimiento ilustrativo para transmitir un mensaje de baliza.

La figura 3 es un diagrama de flujo de un procedimiento ilustrativo para proporcionar un servicio basado en balizas.

- 15 Las figuras 4 y 5 son diagramas esquemáticos de arquitecturas informáticas ilustrativas que permiten la transmisión de un mensaje de baliza.

Descripción detallada

- 20 En técnicas convencionales, se transmite un identificador (ID) de una baliza a través de un mensaje no cifrado. Algunas aplicaciones en el dispositivo móvil pueden obtener el ID. Esto proporciona una oportunidad para un programa malicioso. Después de que diseñadores de software malicioso obtengan un ID de baliza, pueden conducir a los clientes a un servidor de pesca y usan páginas falsas de pedidos/pago para obtener información financiera de los clientes.

- 25 Implementaciones de esta presente divulgación se refieren a nuevos métodos de transmisión de datos de baliza para abordar problemas de las técnicas convencionales. La figura 1 es un diagrama esquemático de un entorno informático 100 ilustrativo, que permite la transmisión de un mensaje de baliza. El entorno puede incluir una baliza 102 que puede generar una señal de baliza 104, y un dispositivo móvil 106 que puede recibir la señal de baliza 104 dentro de una determinada distancia. En algunas implementaciones, la señal de baliza 104 puede incluir información cifrada 112 asociada con la baliza 102 y/o un servicio asociado con la baliza 102. El dispositivo móvil 106 y la baliza 102 pueden usar diversos protocolos inalámbricos soportados para la transmisión de datos. El dispositivo móvil 106 puede comunicarse además con un servidor 108 a través de una red 110. En algunas implementaciones, la baliza 30 102 puede conectarse a una red de comunicación móvil, servidores de gestión de red y/u otros dispositivos para el intercambio de datos. Los tipos de dispositivos móviles, protocolos o estructuras de red de comunicaciones inalámbricas usados en el entorno informático 100 no están limitados por las implementaciones de esta presente divulgación.

- 35 Una implementación de esta presente divulgación puede cifrar un ID de la baliza 102 para generar un mensaje de baliza que incluye información de cifrado, tal como un ID cifrado de la baliza 102. El mensaje de baliza puede cifrarse usando un método de cifrado, que puede modificarse con el tiempo. En algunas realizaciones, después de recibir el mensaje de baliza, el dispositivo móvil 106 puede enviar el mensaje de baliza al servidor 108. El servidor 108 puede descifrar el mensaje de baliza y proporcionar un servicio correspondiente a un cliente asociado con el dispositivo móvil 106.

- 40 La figura 2 es un diagrama de flujo de un procedimiento ilustrativo para transmitir un mensaje de baliza. En 202, la baliza 102 puede determinar, basándose en un algoritmo predeterminado, un método de cifrado que usa un tiempo actual como parámetro. En algunas implementaciones, la baliza 102 puede determinar el algoritmo de cifrado usando el tiempo actual. En algunas implementaciones, la baliza 102 puede implementar un algoritmo de cifrado predeterminado para determinar una clave privada usando el tiempo actual. Alternativamente, la baliza 102 puede 45 determinar el algoritmo de cifrado y la clave privada usando el tiempo actual. Dicho de otro modo, el método de cifrado puede incluir un algoritmo de cifrado y/o la clave privada. En estos casos, el servidor 108 puede usar los métodos de descifrado correspondientes para el descifrado.

- 50 En algunas implementaciones, la baliza 102 puede instalarse en una determinada ubicación y puede realizarse una configuración inicial después de la instalación. Después de la configuración inicial, la baliza 102 puede generar una trama de radio basándose en la configuración inicial y transmitir la trama de radio a un dispositivo informático tal como el dispositivo móvil 106. En algunas implementaciones, el cifrado en la baliza 102 puede realizarse por la baliza 102, y el descifrado puede realizarse por el servidor 108. En algunas implementaciones, el servidor 108 y la baliza 102 pueden comunicarse rara vez. En estos casos, pueden implementarse el cifrado y descifrado usando una referencia mutua para sincronizar y/o modificar el método de cifrado y el método de descifrado, respectivamente. Por 55 ejemplo, la referencia mutua puede incluir un tiempo actual.

La baliza 102 y el servidor 108 pueden modificar el método de cifrado y el método de descifrado durante un periodo de tiempo predeterminado, respectivamente. En algunas implementaciones, puede determinarse una frecuencia de modificación basándose en diversas condiciones. Por ejemplo, el método de cifrado y el método de descifrado pueden modificarse después de un intervalo de tiempo fijo y/o variable. El método de cifrado y el método de descifrado pueden modificarse al mismo tiempo de manera correspondiente, de tal manera que un mensaje cifrado por la baliza 102 puede descifrarse por el servidor 108.

Por ejemplo, la baliza 102 y el servidor 108 pueden implementar un algoritmo de cifrado simétrico predeterminado (por ejemplo, usando descifrado y clave privada idénticos). El cifrado y la clave privada pueden determinarse basándose en un algoritmo que usa un número entero del tiempo actual (por ejemplo, 9 para 9:45) como parámetro de entrada. Por consiguiente, la baliza 102 y el servidor 108 pueden modificar el método de cifrado y el método de descifrado cada hora, respectivamente.

En algunas implementaciones, la baliza 102 puede preestablecer N tipos de métodos de cifrado. N es un número natural mayor que 1. La baliza 102 puede mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado y designar un método de cifrado correspondiente a M como el método de cifrado determinado. M es un número natural, mayor que o igual a 1, y menor que N. En algunas implementaciones, el servidor 108 puede presentar N métodos de descifrado tipo correspondientes a los N tipos de métodos de cifrado. Según el mismo algoritmo de mapeo, el servidor 108 puede obtener el método de descifrado de número M, que puede implementarse como método de descifrado determinado. Por consiguiente, la baliza 102 y el servidor 108 pueden tener métodos de cifrado y descifrado correspondientes, respectivamente.

En 204, la baliza 102 puede cifrar un ID de la baliza usando el método de cifrado determinado para obtener un mensaje de baliza que incluye un ID cifrado de la baliza 102. En algunas implementaciones, una trama de radio generada y/o transmitida por la baliza 102 puede incluir el mensaje de baliza. En estos casos, la trama de radio puede incluir un ID único de la baliza 102 y otra información de baliza, tal como un código de ubicación de la baliza 102 e información de equipos de la baliza 102. La baliza 102 puede cifrar el ID y/u otra información de baliza asociada con la baliza 102 siempre que el servidor 108 puede descifrar correctamente la información cifrada.

Por ejemplo, una trama de radio de la baliza 102 puede incluir los siguientes tipos de información: UUID, mayor (por ejemplo, características principales de la baliza 102), menor (por ejemplo, características menores de la baliza 102), potencia medida (por ejemplo, medición de potencia). El UUID puede ser un ID de 128 bits usado para identificar de manera única la baliza 102: el ID de baliza. Mayor y menor son ID de 16 bits, y se establecen por un operario de baliza para portar información de ID adicional de la baliza 102. Por ejemplo, una tienda puede incluir información de ubicación en mayor, e incluir un número de referencia y/o ID asociados con la tienda. Por ejemplo, si la baliza 102 se instala en un dispositivo, los modelos de producto pueden incluirse en mayor, y los números de referencia correspondientes a tipos de errores pueden incluirse en menor.

La potencia medida puede representar una referencia de intensidad que indica la intensidad de señal generada por la baliza 102 cuando la distancia entre un módulo de transmisión de la baliza y un receptor (por ejemplo, el dispositivo móvil 106) es aproximadamente una distancia predeterminada (por ejemplo, un metro). El receptor puede determinar la distancia basándose en la referencia de intensidad y la intensidad de señal que se recibe actualmente. Durante el cifrado, la baliza 102 puede cifrar al menos uno de UUID, mayor o menor asociados con la baliza 102.

En 206, la baliza 102 puede generar una trama de radio que incluye el ID cifrado e información asociada con un dispositivo informático de descifrado (por ejemplo, el servidor 108).

En algunas implementaciones, el dispositivo móvil 106 puede recibir una trama de radio, recuperar un ID no cifrado de la baliza 102 a partir de la trama de radio, y realizar una determinada acción correspondiente al ID no cifrado. En algunas implementaciones, la determinada acción puede incluir ubicar y conectar con una dirección de un servidor correspondiente. Por ejemplo, el dispositivo móvil 106 puede identificar una dirección de servidor correspondiente del servidor 108 e iniciar una conexión con el servidor 108. En otras implementaciones, el ID de la baliza 102 puede cifrarse, y el dispositivo móvil 106 puede no ser capaz de descifrar el ID cifrado. En estos casos, el servidor 108 puede estar configurado para descifrar el ID cifrado. Por tanto, la información del servidor 108 y el ID cifrado pueden incluirse en la trama de radio de tal manera que el dispositivo móvil 106 puede transmitir el ID cifrado a un servidor apropiado (por ejemplo, el servidor 108), que tiene un método de descifrado correspondiente.

La baliza 102 puede recuperar la información del servidor 108 y empaquetar la información en una trama de radio. En algunas implementaciones, la baliza 102 puede recuperar la información usando una aplicación que reside en el dispositivo móvil 106 y analiza la trama de radio. Por ejemplo, la información puede incluir una dirección IP (protocolo de internet), una dirección URL (localizador uniforme de recursos), o un número el servidor 108 reconocido por la aplicación de tal manera que el dispositivo móvil 106 puede identificar y/o ubicar el servidor 108 por consiguiente.

En 208, la baliza 102 puede transmitir la trama de radio al dispositivo móvil 106, que identifica el servidor 108 y transmite una petición para el descifrado al servidor 108.

La figura 3 es un diagrama de flujo de un procedimiento ilustrativo para proporcionar un servicio basado en balizas.

En 302, el servidor 108 puede determinar, basándose en un algoritmo predeterminado, un método de descifrado que usa un tiempo actual como parámetro. En algunas implementaciones, el método de descifrado puede incluir un algoritmo de descifrado y/o una clave privada.

En algunas implementaciones, el servidor 108 puede preestablecer N tipos de métodos de descifrado. N es un número natural mayor que 1. El servidor 108 puede mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado y designar un método de descifrado correspondiente a M como el método de cifrado determinado. M es un número natural, mayor que o igual a 1, y menor que N. Puesto que el método de descifrado asociado con el servidor 108 corresponde al método de cifrado asociado con la baliza 102, el servidor 108 puede determinar el método de descifrado basándose en el método de cifrado que se determina y/o designa por la baliza 102.

En 304, el servidor 108 puede recibir un mensaje cifrado que incluye el ID cifrado de la baliza 102. Por ejemplo, el dispositivo móvil 106 puede recibir la trama de radio y recuperar información del servidor 108 así como el mensaje cifrado a partir de la trama de radio. El dispositivo móvil 106 puede transmitir el mensaje cifrado que incluye el ID cifrado de la baliza 102 al servidor 108.

En 306, el servidor 108 puede obtener el ID de la baliza 102 basándose en el método de descifrado correspondiente al ID cifrado de la baliza 102. Además del ID de la baliza 102, el servidor 108 puede descifrar otra información de baliza, tal como un código de ubicación de la baliza 102 e información de equipos de la baliza 102.

En 308, el servidor 108 puede determinar información de una tarea (por ejemplo, un servicio) correspondiente al ID de la baliza 102 y transmitir la información al dispositivo móvil 106. En algunas implementaciones, el servidor 108 puede identificar y/o ubicar una tarea correspondiente al ID de la baliza 102, y transmitir la información de la tarea al dispositivo móvil 106. Por ejemplo, el servidor 108 puede almacenar información de una tienda asociada con la baliza 102. La información puede incluir servicios proporcionados por la tienda a un cliente. El servidor 108 puede obtener el ID de la baliza 102, identificar y/o ubicar la tienda asociada con la baliza 102, y proporcionar al cliente la información de los servicios asociados con la tienda.

Puesto que el dispositivo móvil 106 puede transmitir el ID de la baliza 102 e información adicional al servidor 108, el servidor 108 puede proporcionar información detallada y exacta de servicios al dispositivo móvil 106. En algunas implementaciones, el servidor 108 puede facilitar además los servicios basándose en información adicional transmitida desde el dispositivo móvil 106 al servidor 108. La información adicional puede incluir al menos uno de la ubicación de la baliza 102, información de equipos de la baliza 102, información de entorno (por ejemplo, tiempo meteorológico y tráfico) asociada con la baliza 102, o información de dispositivo asociada con el dispositivo móvil 106.

Supóngase que la baliza 102 es una baliza de Bluetooth (por ejemplo, iBeacon®). Pueden realizarse algoritmos de cifrado y descifrado asimétricos (por ejemplo, RSA) en el UUID de la baliza 102. Estos algoritmos pueden realizarse en la baliza 102 y el servidor 108, respectivamente. En algún caso, el método de cifrado del servidor 108 y la baliza 102 pueden ser una clave privada y una clave pública, respectivamente. La clave privada y la clave pública pueden determinarse basándose en la fecha actual. En algunas implementaciones, la baliza 102 puede preestablecer K claves públicas, y el servidor 108 puede preestablecer K claves privadas. En estos casos, las K claves públicas corresponden a las K claves privadas. Una clave pública individual y la clave privada correspondiente pueden adoptarse por la baliza 102 y el servidor 108, respectivamente. La baliza 102 y el servidor 108 pueden modificar además la clave pública individual y la clave privada individual correspondiente, respectivamente.

En algunas implementaciones, claves públicas K y el tiempo actual pueden almacenarse en la baliza 102. La baliza 102 puede determinar y/o establecer una clave privada basándose en el tiempo actual y un algoritmo predeterminado. La baliza 102 puede cifrar además UUID y transmitir información que incluye el mensaje cifrado e información asociada con el servidor 108 al dispositivo móvil 106.

Puesto que la baliza 102 puede transmitir tramas de radio a una frecuencia fija, la baliza 102 puede determinar el número de tramas de radio que la baliza 102 envía en un cierto tiempo. Por tanto, la baliza 102 puede determinar si la clave privada tiene que modificarse. En algunas implementaciones, la baliza 102 puede modificar la clave privada en respuesta a una determinación de que el número de tramas de radio es igual a un número total de tramas de radio que se permite que se transmitan al día. La baliza 102 puede entonces modificar el método de cifrado, y volver a contar el número de tramas de radio. En un día inicial, puede determinarse un número inicial basándose en el tiempo actual y la frecuencia de transmisión de tramas de radio de tal manera que el número de tramas de radio puede alcanzar el número total de tramas de radio que se permite que se transmitan al día a las cero horas del día siguiente.

Después del establecimiento inicial, la baliza 102 puede entrar un modo automático. En algunas implementaciones, la baliza 102 puede transmitir tramas de radio a una frecuencia predeterminada. En respuesta a una determinación de que un número de transmisiones de trama de radio es igual a un número total de transmisiones de trama de radio que se permite que se transmitan al día, la baliza 102 puede adoptar la nueva clave privada junto a la clave privada actual. La baliza puede cifrar el UUID y otros parámetros usando la nueva clave privada para obtener un nuevo

mensaje cifrado. La baliza 102 puede entrar en un nuevo día de difusión. Cuando el dispositivo móvil 106 recibe la trama de radio desde la baliza 102, el dispositivo móvil 106 puede recuperar información del servidor de descifrado (por ejemplo, el servidor 108) así como el mensaje cifrado que incluye el UUID y otro parámetro. El dispositivo móvil 106 puede transmitir entonces el mensaje cifrado al servidor 108.

- 5 Después de que el servidor 108 reciba el mensaje cifrado, el servidor 108 puede, basándose en la fecha actual y un algoritmo predeterminado, determinar y/o ubicar la clave privada correspondiente para descifrar el mensaje cifrado para obtener el UUID y otros parámetros asociados con la baliza 102. El servidor 108 puede determinar una tarea correspondiente al UUID, y transmitir información de la tarea al dispositivo móvil 106.

- 10 Implementaciones de esta presente divulgación pueden cifrar el ID de la baliza 102 y generar un mensaje cifrado que puede modificarse con el tiempo. Aunque terceros puedan obtener el mensaje cifrado, sería difícil para ellos obtener información asociada con la baliza 102 puesto que el mensaje cifrado cambia con el tiempo. Además, los terceros pueden no ser capaces de sustraer información sensible desde el dispositivo móvil 106. De manera similar, aplicaciones no autorizadas en el dispositivo móvil 106 pueden obtener simplemente el mensaje cifrado, y la información cifrada en el mensaje cifrado no puede obtenerse por las aplicaciones no autorizadas.

- 15 Las figuras 4 y 5 son diagramas esquemáticos de arquitecturas informáticas ilustrativas que permiten la transmisión de un mensaje de baliza. La figura 4 es un diagrama de un dispositivo informático 400 (por ejemplo, la baliza 102). El dispositivo informático 400 puede ser un dispositivo de usuario o un servidor para un control de inicio de sesión de ubicación múltiple. En una configuración a modo de ejemplo, el dispositivo informático 400 incluye uno o más procesadores 402, interfaces de entrada/salida 404, interfaz de red 406 y memoria 408.

- 20 La memoria 408 puede incluir medios legibles por ordenador en forma de memoria volátil, tal como memoria de acceso aleatorio (RAM) y/o memoria no volátil, tal como memoria de sólo lectura (ROM) o RAM flash. La memoria 408 es un ejemplo de medios legibles por ordenador.

- 25 Los medios legibles por ordenador incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para almacenamiento de información tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los ejemplos de medios de almacenamiento informático incluyen, pero no se limitan a, memoria de cambio de fase (PRAM), memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica (DRAM), otros tipos de memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), memoria de sólo lectura programable y borrable eléctricamente (EEPROM), memoria flash u otra tecnología de memoria, memoria de sólo lectura de disco compacto (CD-ROM), discos versátiles digitales (DVD) u otro almacenamiento óptico, cintas magnéticas, cinta magnética, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio sin transmisión que puede usarse para almacenar información para el acceso por un dispositivo informático. Tal como se definen en el presente documento, los medios legibles por ordenador no incluyen medios transitorios tales como señales de datos moduladas y ondas portadoras.

- 35 Volviendo a la memoria 408 con más detalle, la memoria 408 puede incluir un módulo de determinación de cifrado 410, un módulo de cifrado 412 y un módulo de transmisión 414. El módulo de determinación de cifrado 410 está configurado para determinar, basándose en un algoritmo predeterminado, un método de cifrado que usa un tiempo actual como parámetro. El módulo de cifrado 412 está configurado para cifrar un ID de una baliza usando el cifrado determinado para obtener un ID cifrado de la baliza. El módulo de transmisión 414 está configurado para generar una trama de radio que incluye el ID cifrado e información asociada con un dispositivo informático de descifrado (por ejemplo, el servidor 108), y transmitir la trama de radio al dispositivo móvil 106.

- 40 En algunas implementaciones, el módulo de determinación de cifrado 410 puede incluir un módulo de preestablecimiento de cifrado, un módulo de mapeo de cifrado y un módulo de selección de cifrado. El módulo de preestablecimiento de cifrado está configurado para preestablecer N tipos de métodos de cifrado. N es un número natural mayor que 1. El módulo de mapeo de cifrado está configurado para mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado. M es un número natural, mayor que o igual a 1, y menor que N. El módulo de selección de cifrado está configurado para designar un método de cifrado correspondiente a M como el método de cifrado determinado.

- 45 En algunas implementaciones, el método de cifrado es una clave pública, y en el que el tiempo actual es una fecha actual. En algunos casos, el módulo de determinación de cifrado 410 puede incluir un módulo de recuento total, un módulo de recuento y un módulo de modificación de cifrado. El módulo de recuento total está configurado para determinar un número total de veces de transmisión de tramas de radio en un día basándose en una frecuencia de transmisión de radio. El módulo de recuento está configurado para contar un número de veces de transmisión de las tramas de radio basándose en el tiempo actual y la frecuencia de transmisión de radio. El módulo de modificación de cifrado está configurado para modificar el método de cifrado basándose en el algoritmo predeterminado en respuesta a una determinación de que el número de veces de transmisión es igual al número total de veces de transmisión, y vuelve a contar el número de veces de transmisión. En algunas implementaciones, el método de cifrado puede incluir una clave privada y/o un algoritmo de cifrado.

La figura 5 es un diagrama de un dispositivo informático 500 (por ejemplo, el servidor 108). El dispositivo informático 500 puede ser un dispositivo de usuario o un servidor para un control de inicio de sesión de ubicación múltiple. En una configuración a modo de ejemplo, el dispositivo informático 500 incluye uno o más procesadores 502, interfaces de entrada/salida 504, interfaz de red 506 y memoria 508.

- 5 La memoria 508 puede incluir medios legibles por ordenador en forma de memoria volátil, tal como memoria de acceso aleatorio (RAM) y/o memoria no volátil, tal como memoria de sólo lectura (ROM) o RAM flash. La memoria 508 es un ejemplo de medios legibles por ordenador.

Los medios legibles por ordenador incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para almacenamiento de información tales como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los ejemplos de medios de almacenamiento informático incluyen, pero no se limitan a, memoria de cambio de fase (PRAM), memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica (DRAM), otros tipos de memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), memoria de sólo lectura programable y borrrable eléctricamente (EEPROM), memoria flash u otra tecnología de memoria, memoria de sólo lectura de disco compacto (CD-ROM), discos versátiles digitales (DVD) u otro almacenamiento óptico, cintas magnéticas, cinta magnética, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético o cualquier otro medio sin transmisión que puede usarse para almacenar información para el acceso por un dispositivo informático. Tal como se definen en el presente documento, los medios legibles por ordenador no incluyen medios transitorios tales como señales de datos moduladas y ondas portadoras.

- 20 Volviendo a la memoria 508 con más detalle, la memoria 508 puede incluir un módulo de determinación de descifrado 510, un módulo de recepción de mensaje cifrado 512, un módulo de descifrado 514 y un módulo de provisión de tarea 516. El módulo de determinación de descifrado 510 está configurado para determinar, basándose en un algoritmo predeterminado, un método de descifrado que usa un tiempo actual como parámetro. El módulo de recepción de mensaje cifrado 512 está configurado para recibir un ID cifrado de una baliza desde un dispositivo móvil. El módulo de descifrado 514 está configurado para descifrar el ID cifrado usando el método de descifrado determinado para obtener un ID de la baliza. El módulo de provisión de tarea 516 está configurado para proporcionar una tarea correspondiente al ID al dispositivo móvil.

- 30 En algunas implementaciones, el servidor 108 puede preestablecer N tipos de métodos de descifrado. N es un número natural mayor que 1. El servidor 108 puede mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado y designar un método de descifrado correspondiente a M como el método de descifrado determinado. M es un número natural, mayor que o igual a 1, y menor que N.

- 35 En técnicas convencionales, las balizas transmiten tramas de radio sin cifrado. Implementaciones de la presente divulgación pueden cifrar el ID de la baliza 102 y modificar el método de cifrado con el tiempo. Por consiguiente, aplicaciones no autorizadas por la baliza 102 no pueden obtener un ID estable de la baliza 102; no puede proporcionarse un servicio no autorizado a través de la baliza 102. Esto evita no sólo la divulgación de información sensible de clientes sino también la sustracción de mensajes de baliza.

- 40 Las implementaciones son simplemente para ilustrar la presente divulgación y no se pretende que limiten el alcance de la presente divulgación. Debe entenderse por expertos en el campo técnico que pueden realizarse determinadas modificaciones y mejoras y deben considerarse bajo la protección de la presente divulgación sin apartarse del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método implementado por ordenador (200) para transmitir un mensaje de baliza (104), comprendiendo el método:

5 determinar (202), por uno o más procesadores de una baliza (102) basándose en un algoritmo predeterminado, un método de cifrado que usa un tiempo actual como parámetro, en el que la determinación (202) comprende:

preestablecer N tipos de métodos de cifrado, siendo N un número natural mayor que 1, comprendiendo cada método de cifrado un algoritmo de cifrado;

mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado, siendo M
10 un número natural, mayor que o igual a 1, y menor que N; y

designar un método de cifrado correspondiente a M como el método de cifrado determinado;

cifrar (204) un identificador de una baliza usando el método de cifrado determinado para obtener un mensaje de baliza (104) que comprende un identificador cifrado de la baliza (112);

15 generar (206) una trama de radio que comprende el mensaje de baliza (104) e información asociada con un dispositivo informático de descifrado (500); y

transmitir (208) la trama de radio a un dispositivo móvil (106).
2. El método (200) según la reivindicación 1, en el que el método de cifrado determinado comprende adicionalmente una clave privada.
3. El método (200) según cualquier reivindicación anterior, en el que el mensaje de baliza (104) comprende
20 además información que comprende al menos uno de una ubicación de la baliza (102), una configuración de la baliza (102), un servicio asociado con la baliza (102) o un parámetro de hardware de la baliza (102).
4. Uno o más medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador que, cuando se ejecutan por uno o más procesadores, ordenan que el uno o más procesadores realicen acciones, que comprenden:

25 determinar (302), basándose en un algoritmo predeterminado, un método de descifrado usando un tiempo actual como parámetro, en la que la determinación (302) comprende:

preestablecer N tipos de métodos de descifrado, siendo N un número natural mayor que 1, comprendiendo cada método de descifrado un algoritmo de descifrado;

mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado, siendo M
30 un número natural, mayor que o igual a 1, y menor que N; y

designar un método de descifrado correspondiente a M como el método de descifrado determinado;

recibir (304), desde un dispositivo móvil (106), un mensaje de baliza (104) que comprende un identificador cifrado (112) de una baliza (102);

35 descifrar (306) el identificador cifrado (112) usando el método de descifrado determinado para obtener un identificador de la baliza (102); y

proporcionar (308) una tarea correspondiente al identificador de la baliza (102) al dispositivo móvil (106).
5. El uno o más medios legibles por ordenador según la reivindicación 4, en el que el método de descifrado determinado (306) comprende adicionalmente una clave privada.
6. El uno o más medios legibles por ordenador según la reivindicación 5, en el que el tiempo actual es una
40 fecha actual.
7. El uno o más medios legibles por ordenador según una cualquiera de las reivindicaciones 4 a 6, en el que el mensaje de baliza (104) comprende además información que comprende al menos uno de una ubicación de la baliza (102), una configuración de la baliza (102), un servicio asociado con la baliza (102) o un parámetro de hardware de la baliza (102).
8. Un sistema (400) que comprende:

45 uno o más procesadores (402); y

- una memoria (408) para mantener una pluralidad de componentes ejecutables por el uno o más procesadores (402), comprendiendo la pluralidad de componentes:
- un módulo de determinación de cifrado (410) configurado para determinar (202), basándose en un algoritmo predeterminado, un método de cifrado que usa un tiempo actual como parámetro, en el que el módulo de determinación de cifrado (410) comprende:
- un módulo de preestablecimiento de cifrado configurado para preestablecer N tipos de métodos de cifrado, siendo N un número natural mayor que 1, comprendiendo cada método de cifrado un algoritmo de cifrado;
- un módulo de mapeo de cifrado configurado para mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado, siendo M un número natural, mayor que o igual a 1, y menor que N; y
- un módulo de selección de cifrado configurado para designar un método de cifrado correspondiente a M como el método de cifrado determinado;
- un módulo de cifrado (412) configurado para cifrar (204) un identificador de una baliza (102) usando el método de cifrado determinado para obtener un mensaje de baliza (104) que comprende un identificador cifrado (112) de una baliza, y
- un módulo de transmisión (414) configurado para:
- generar (206) una trama de radio que comprende el mensaje de baliza (104) e información asociada con un dispositivo informático de descifrado (500), y
- transmitir (208) la trama de radio a un dispositivo móvil (106).
9. El sistema (400) según la reivindicación 8, en el que el método de cifrado (204) comprende adicionalmente una clave privada.
10. El sistema (400) según la reivindicación 8 o la reivindicación 9, en el que el mensaje de baliza (104) comprende además información que comprende al menos uno de una ubicación de la baliza (102), una configuración de la baliza (102), un servicio asociado con la baliza (102) o un parámetro de hardware de la baliza (102).
11. Un sistema (500) que comprende:
- uno o más procesadores (502); y
- una memoria (508) para mantener una pluralidad de componentes ejecutables por el uno o más procesadores (502), comprendiendo la pluralidad de componentes:
- un módulo de determinación de descifrado (510) configurado para determinar (302), basándose en un algoritmo predeterminado, un método de descifrado que usa un tiempo actual como parámetro, en el que la determinación (302) comprende:
- preestablecer N tipos de métodos de descifrado, siendo N un número natural mayor que 1, comprendiendo cada método de descifrado un algoritmo de descifrado;
- mapear el tiempo actual con respecto a M usando un algoritmo de mapeo predeterminado, siendo M un número natural, mayor que o igual a 1, y menor que N; y
- designar un método de descifrado correspondiente a M como el método de descifrado determinado,
- un módulo de recepción de mensaje cifrado (512) configurado para recibir (304) un mensaje de baliza (104) que comprende un identificador cifrado (112) de una baliza desde un dispositivo móvil (106),
- un módulo de descifrado (514) configurado para descifrar (306) el identificador cifrado (112) usando el método de descifrado determinado para obtener un identificador de la baliza (102), y
- un módulo de provisión de tarea (516) configurado para proporcionar (308) una tarea correspondiente al identificador de la baliza al dispositivo móvil (106).
12. El sistema (500) la reivindicación 11, en el que el método de descifrado (306) comprende adicionalmente una clave privada.
13. El sistema (500) según la reivindicación 12, en el que el tiempo actual es una fecha actual.

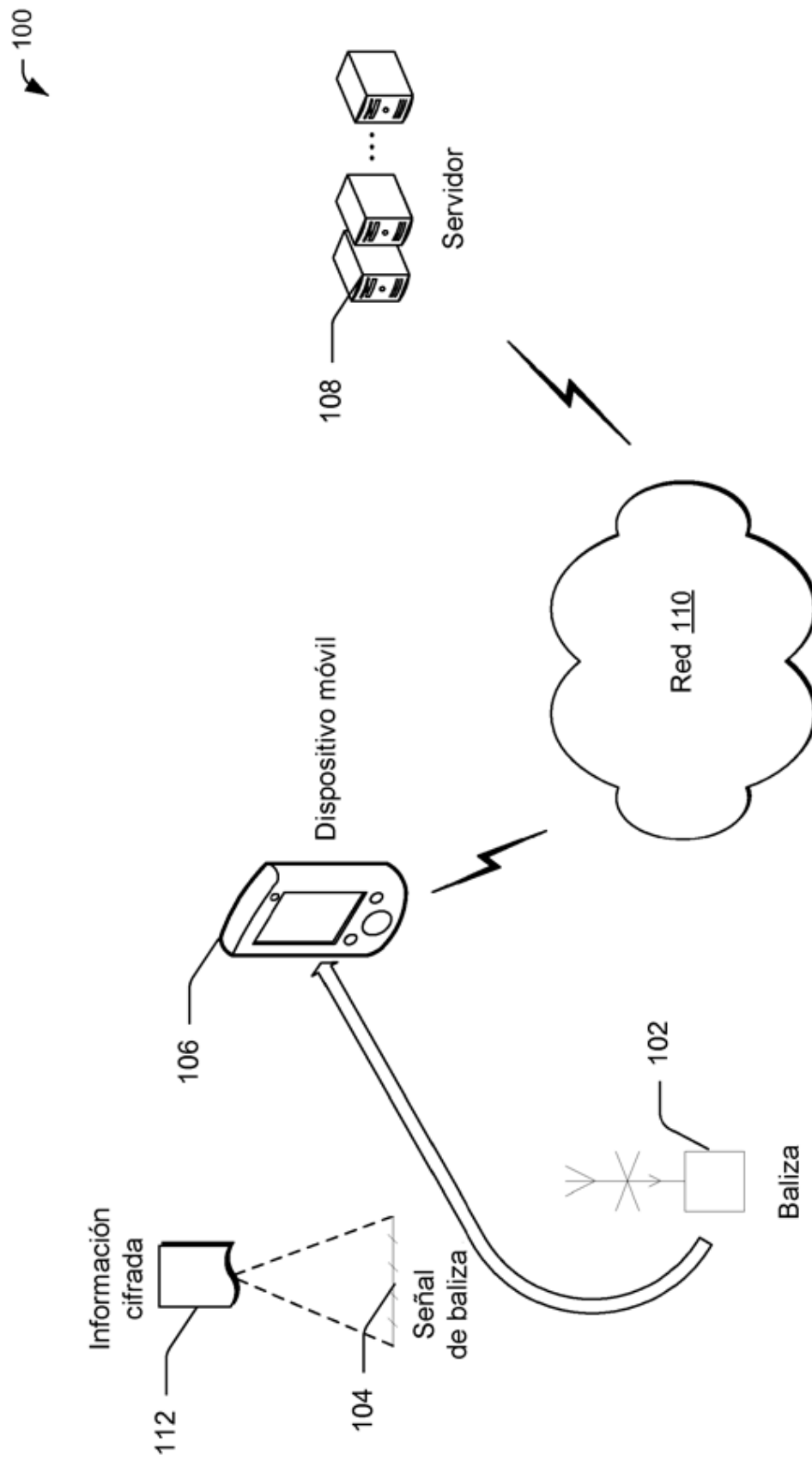


FIG. 1

↖ 200

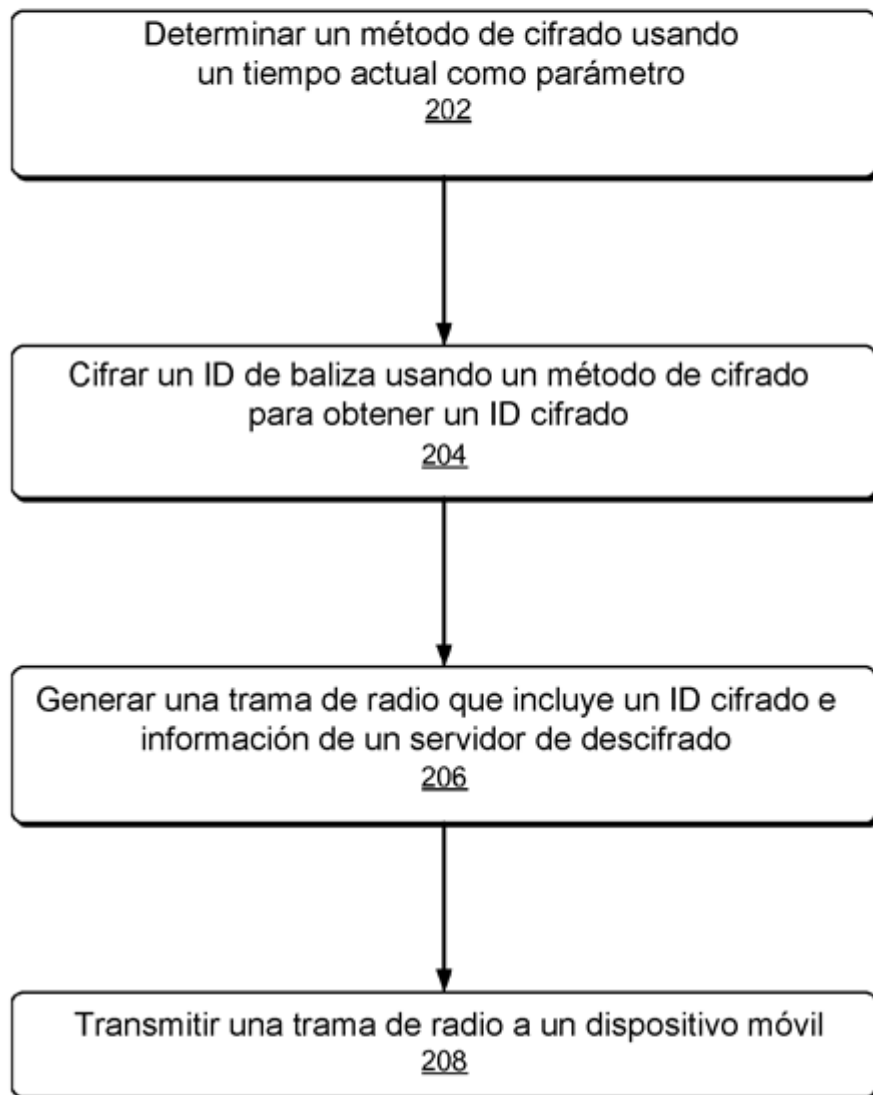


FIG. 2

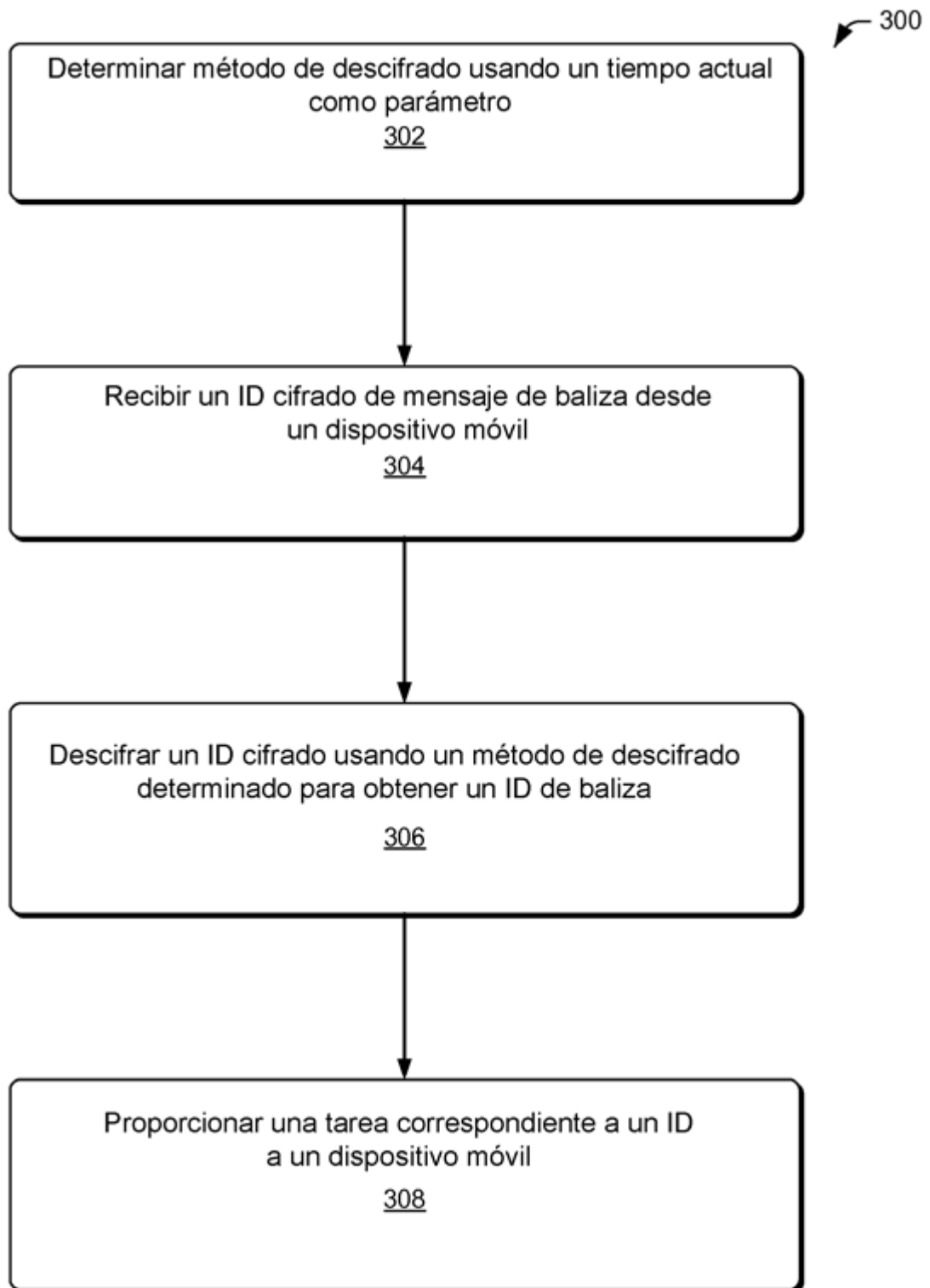


FIG. 3

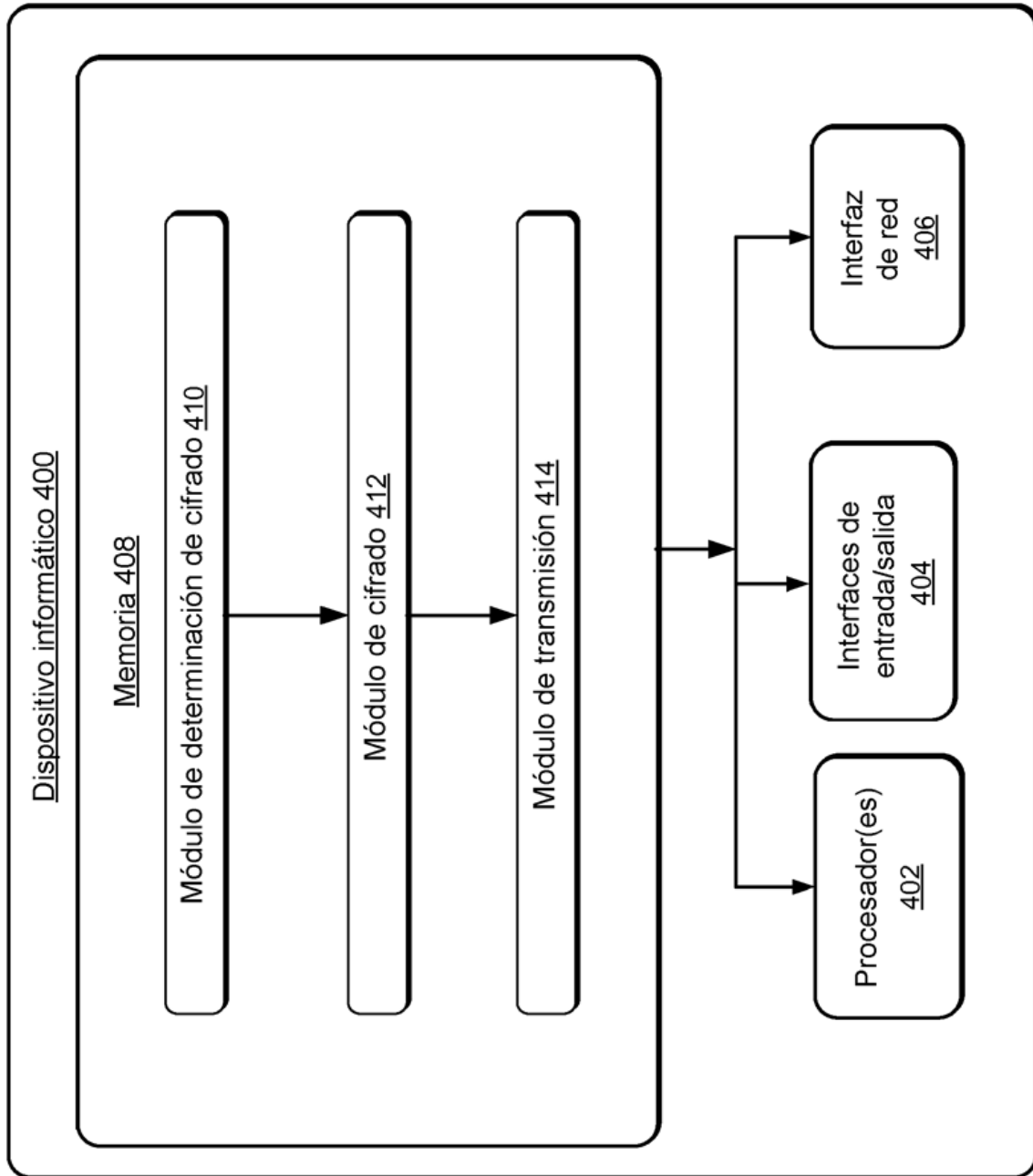


FIG. 4

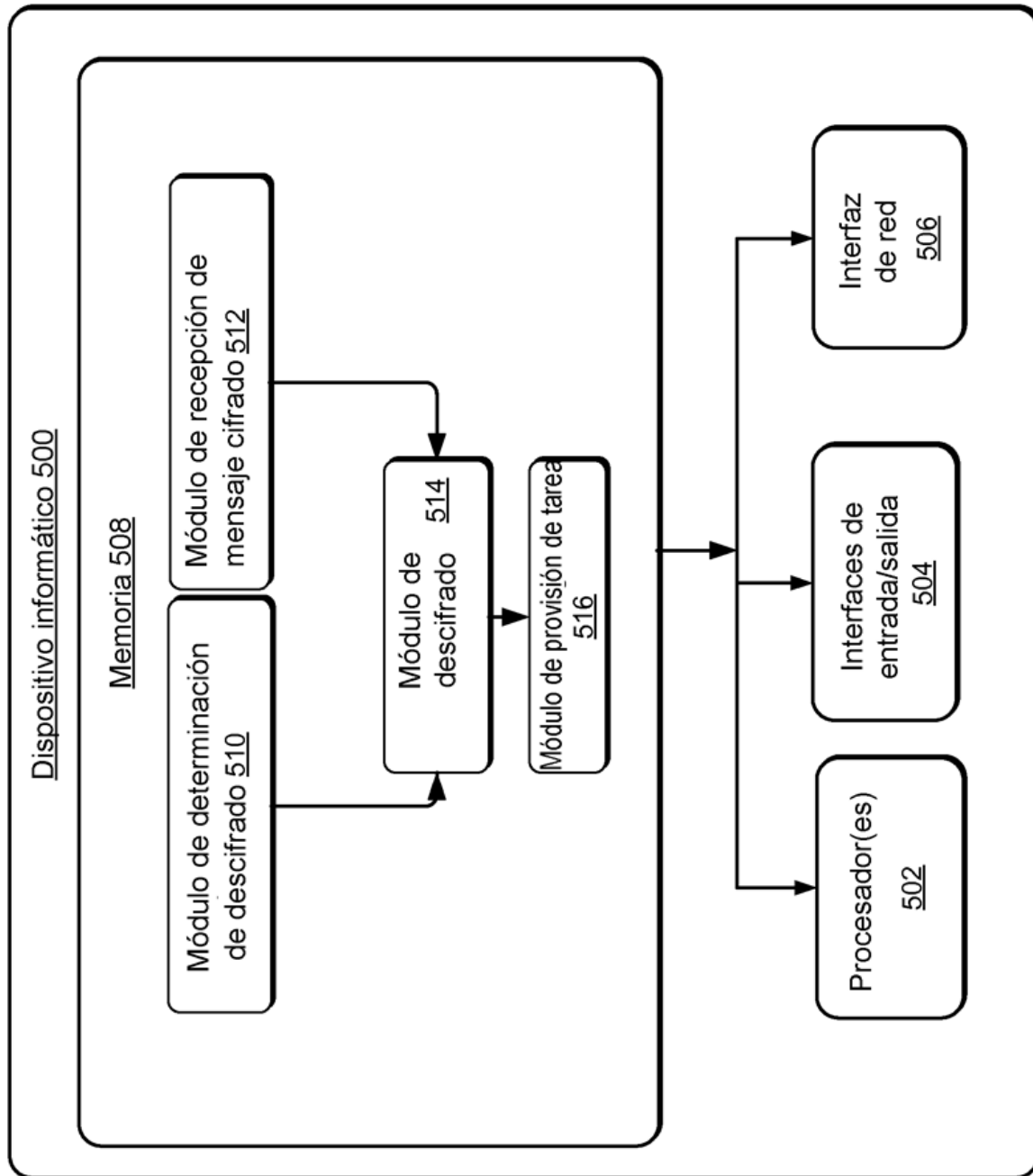


FIG. 5