(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 381**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04L 29/06 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.12.2012 PCT/US2012/069588**

(87) Fecha y número de publicación internacional: **18.07.2013 WO13106163**

(96) Fecha de presentación y número de la solicitud europea: **13.12.2012 E 12813189 (3)**

(97) Fecha y número de publicación de la concesión europea: **14.11.2018 EP 2803218**

(54) Título: **Un sistema y método para una comunicación segura**

(30) Prioridad:

12.01.2012 US 201213349543

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2019

(73) Titular/es:

THE BOEING COMPANY (100.0%)
100 North Riverside Plaza
Chicago, IL 60606-1596, US

(72) Inventor/es:

ANDREWS, ERIC, J.;
EIGLE, TED y
HOFFMAN, CEILIDH

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Un sistema y método para una comunicación segura

Campo

Los modos de realización de la presente divulgación se refieren en general a sistemas de comunicación. Más concretamente, los modos de realización de la presente divulgación se refieren a sistemas de comunicación encriptados para una comunicación segura.

Antecedentes

En general, las redes inalámbricas comerciales no encriptan ni protegen los datos de información del usuario que se transmiten por el aire. Se espera que la seguridad y la integridad de los datos sean controladas por una aplicación de usuario final. La mayoría de las aplicaciones de usuario final que van a través de la red de Protocolo de Internet (IP) recurren a métodos de encriptación de clave pública tanto para la autenticación del usuario final como para la seguridad de los datos.

Con la omnipresencia de las redes de área local inalámbricas en los espacios públicos, los organismos de estándares de la industria inalámbrica comercial han implementado una capa adicional de seguridad que sirve como control de acceso para otorgar acceso solo a usuarios autorizados; Es decir, usuarios que tienen una clave de encriptación-desencriptación correcta de la red. Sin embargo, una señal de radiofrecuencia (RF) transmitida por el aire no está protegida contra escuchas ilegales. Por el contrario, la mayoría de las redes inalámbricas militares admiten tanto la seguridad de los datos del usuario final como la protección de la señal de RF transmitida por el aire. Sin embargo, dichas redes están cerradas y son propietarias y, en general, no pueden interactuar con dispositivos inalámbricos disponibles comercialmente, como teléfonos móviles, ordenadores personales y tabletas. El estado de la técnica se conoce a partir del documento US2010/0088511 A1 que describe un método para asegurar la transmisión de información en una red de comunicación, en donde las direcciones de destino están encriptadas.

Resumen

La invención se define en las reivindicaciones independientes. Se divulga un sistema y métodos para una comunicación segura utilizando equipos comerciales modificados. Se trata de un paquete de red que comprende una dirección de red encriptada para la seguridad de transmisión que comprende una dirección de red no encriptada encriptada mediante un primer tiempo de Sistema de Posicionamiento Global (GPS) y un primer número pseudoaleatorio. La dirección de red encriptada se desencripta utilizando el primer tiempo GPS y el primer número pseudoaleatorio para proporcionar la dirección de red no encriptada. El paquete de red se transmite en basándose en la dirección de red no encriptada. De esta manera, los modos de realización de la divulgación hacen uso de redes disponibles comercialmente (COTS) de gran ancho de banda y bajo coste para transmitir datos clasificados.

En un modo de realización, un método para una comunicación segura recibe un paquete de red que comprende una dirección de red encriptada que comprende una dirección de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio. El método desencripta además la dirección de red encriptada utilizando el primer tiempo GPS y el primer número pseudoaleatorio para proporcionar la dirección de red no encriptada. El método además transmite el paquete de red basándose en la dirección de red no encriptada. De manera ventajosa, el método incluye además transmitir el paquete de red a través de una red comercial cerrada. La red comercial cerrada incluye una o más de: una red de protocolo de Internet, una red con conmutación de circuitos, una red de conmutación por paquetes o una red de comunicación inalámbrica. De manera ventajosa, el paquete de red puede incluir además datos encriptados.

En otro modo de realización, un sistema para una comunicación segura comprende un módulo receptor, un módulo de desencriptación y un módulo transmisor. El módulo receptor funciona para recibir un paquete de red que comprende una dirección de red encriptada que comprende una dirección de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio. El módulo de desencriptación funciona para desencriptar la dirección de red encriptada para proporcionar una dirección de red no encriptada. El módulo transmisor funciona para transmitir el paquete de red basándose en la dirección de red no encriptada. De manera ventajosa, el sistema comprende un dispositivo de comunicación móvil. De manera ventajosa, el módulo transmisor funciona además para transmitir el paquete de red a través de una red comercial cerrada. La red comercial cerrada incluye una o más de: una red de protocolo de Internet, una red con conmutación de circuitos, una red de conmutación por paquetes o una red de comunicación inalámbrica.

En un modo de realización adicional, un medio de almacenamiento legible por ordenador comprende instrucciones ejecutables por ordenador para realizar un método de comunicación segura. El método ejecutado por las instrucciones ejecutables por ordenador recibe un paquete de red que comprende una dirección de red encriptada que comprende una dirección de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio. El método desencripta además la dirección de red encriptada utilizando el primer tiempo GPS y el primer número pseudoaleatorio para proporcionar la dirección de red no encriptada. El método además transmite el paquete de red basándose en la dirección de red no encriptada. De manera ventajosa, el método ejecutado por las

instrucciones ejecutables por ordenador incluye además la transmisión del paquete de red a través de una red comercial cerrada. La red comercial cerrada incluye una o más de: una red de protocolo de Internet, una red con conmutación de circuitos, una red de conmutación por paquetes o una red de comunicación inalámbrica.

Este resumen se proporciona para introducir una selección de conceptos en una forma simplificada que se describen con más detalle a continuación en la descripción detallada. Este resumen no tiene la intención de identificar características clave o características esenciales de la materia reivindicada, ni pretende ser utilizado como una ayuda para determinar el alcance de la materia reivindicada.

Breve descripción de los dibujos

Se puede obtener una comprensión más completa de los modos de realización de la presente divulgación haciendo referencia a la descripción detallada y a las reivindicaciones cuando se consideran conjuntamente con las siguientes figuras, en donde números de referencia similares se refieren a elementos similares en todas las figuras. Las figuras se proporcionan para facilitar la comprensión de la divulgación sin limitar la amplitud, alcance, escala o la aplicabilidad de la divulgación. Los dibujos no están necesariamente realizados a escala.

La Figura 1 es una ilustración de un entorno de comunicación inalámbrica de ejemplo para transmitir y recibir información segura de acuerdo con un modo de realización de la divulgación.

La Figura 2 es una ilustración de un proceso de encriptación de ejemplo de un paquete de red encriptado de acuerdo con un modo de realización de la divulgación.

La Figura 3 es una ilustración de un diagrama de bloques funcional esquemático de ejemplo de un sistema de enrutamiento encriptado de acuerdo con un modo de realización de la divulgación.

La Figura 4 es una ilustración de un diagrama de flujo de ejemplo que muestra un proceso para la comunicación segura de acuerdo con un modo de realización de la divulgación.

Descripción detallada

La siguiente descripción detallada es a modo de ejemplo y no pretende limitar la divulgación o la aplicación y usos de los modos de realización de la divulgación. Las descripciones de dispositivos, técnicas y aplicaciones específicas se proporcionan solo como ejemplos. Modificaciones a los ejemplos descritos en el presente documento serán inmediatamente evidentes para los expertos en la técnica, y los principios generales definidos en el presente documento pueden aplicarse a otros ejemplos y aplicaciones sin apartarse del alcance de la divulgación. Asimismo, no hay ninguna intención de estar sujeto a ninguna teoría expresa o implícita presentada en el campo anterior, los antecedentes, el resumen o la siguiente descripción detallada. Se ha de otorgar a la presente divulgación un alcance coherente con las reivindicaciones, y no limitado a los ejemplos descritos y mostrados en el presente documento.

Los modos de realización de la divulgación se pueden describir en el presente documento en términos de componentes de bloques funcionales y/o lógicos y diversas etapas de procesamiento. Hay que señalar que la divulgación, sin embargo, no se limita a dichas aplicaciones de teléfono móvil, y las técnicas descritas en el presente documento también pueden utilizarse en otras aplicaciones. Por ejemplo, los modos de realización pueden ser aplicables a un ordenador de escritorio, un ordenador portátil o ultraportátil, un teléfono Droid™, un Phone™, un ordenador central, un servidor, un cliente, o cualquier otro tipo de dispositivo informático de aplicación general o especializado internamente o externamente habilitado para GPS según sea deseable o apropiado para una aplicación o entorno determinado.

Como resultará evidente para un experto en la técnica después de leer esta descripción, los siguientes son ejemplos y modos de realización de la divulgación y no están limitados a funcionar según estos ejemplos. Se pueden utilizar otros modos de realización y se pueden hacer cambios sin apartarse del alcance de los modos de realización de ejemplo de la presente divulgación.

Con la proliferación de dispositivos inalámbricos disponibles comercialmente de bajo coste (COTS) (debido a las economías de escala) y los rápidos avances tecnológicos en estándares inalámbricos comerciales, es deseable modificar tanto los dispositivos inalámbricos COTS como su diseño de red asociado de modo que se ofrezca la seguridad de grado militar en serie tanto para los datos del usuario final como para las señales de RF por el aire.

Los modos de realización de la divulgación permiten que cualquier red comercial cerrada se utilice para comunicaciones seguras y clasificadas de gran ancho de banda, enlazando redes comerciales con cualquier red aislada, como una red para comunicarse con: drones, aeronaves, radios portátiles de fuerzas terrestres u otra red segura.

La figura 1 es una ilustración de un entorno 100 de comunicación inalámbrica de ejemplo para transmitir y recibir información segura de acuerdo con un modo de realización de la divulgación.

El entorno 100 de comunicación inalámbrica comprende una red 102 aislada, una red 104 ad hoc y una red 106 de infraestructura, una pluralidad de dispositivos 108 de comunicación móvil que comprenden cada uno un sistema 300

de encriptación para una comunicación segura dentro del entorno 100 de comunicación inalámbrica. Cada una de la red 102 aislada, la red 104 ad hoc y la red 106 de infraestructura pueden comprender, por ejemplo, pero sin limitación, una red de protocolo de Internet, una red con conmutación de circuitos, una red de conmutación por paquetes y una red de comunicación inalámbrica.

Los dispositivos 108 de comunicación móvil comprenden cada uno el sistema 300 de encriptación como se explica con más detalle a continuación en el contexto de la exposición de la figura 3. El sistema 300 de encriptación (sistema 300) comprende una seguridad de transmisión de alto grado (TRANSEC) que permite al dispositivo 108 de comunicación móvil comunicarse con la red 102 aislada a un gran ancho de banda (por ejemplo, 50Mbps) para la comunicación de datos (por ejemplo, mapas, voz, vídeo). El sistema 300 de encriptación permite que cualquier red comercial cerrada, como la red 104 ad hoc y la red 106 de infraestructura, se utilice para una comunicación segura y clasificada de gran ancho de banda a través de un enlace 114 de comunicación. De esta manera, estas redes comerciales cerradas pueden enlazarse con cualquier red aislada como la red 102 aislada.

Los dispositivos 108 de comunicación móvil, pueden comunicarse:

- entre pares en la red 104 ad hoc a través de un canal 110 de comunicación;

- base a usuario en la red 106 de infraestructura a través de un canal 112 de comunicación a una estación 116 base;

- por puente a la red 104 ad hoc que se interconecta con una red de comunicación aislada;

- por puente a la red 106 de infraestructura que se interconecta con la red 102 aislada;

- por puente a la red 104 ad hoc que se conecta con otra red móvil entre pares o de infraestructura a través de la red 102 aislada utilizada como red principal de tránsito; y

- por puente a la red 106 de infraestructura que se conecta con otra red móvil entre pares o de infraestructura a través de una red de comunicación aislada que se utiliza como red principal de tránsito u otro canal de comunicación.

Los dispositivos 108 de comunicación móvil pueden comprender, por ejemplo, pero sin limitación, un ordenador de escritorio, un ordenador portátil o ultraportátil, un teléfono Droid™, un iPhone™, un ordenador central, un servidor, un cliente o cualquier otro tipo de dispositivo informático de aplicación general o especializado internamente o externamente habilitado para GPS según sea deseable o apropiado para una aplicación o entorno determinado.

La red 102 aislada puede comprender canales de comunicación configurados para soportar, por ejemplo, pero sin limitación, un Formato de Onda de Red de Banda Ancha (WNW), un Sistema de Reporte Ampliado de Localización de Posición (EPLRS), un Formato de Onda de Radio de Soldado (SRW), Comunicaciones por Satélite 165 (SATCOM 165), Acceso Múltiple Asignado por la Demanda (DAMA), un Sistema de Objetivo de Usuario Móvil (MUOS), un Sistema de Radio Terrestre y Aerotransportado de Canal Simple (SINCGARS), u otra red segura. La red 102 aislada se puede utilizar para la comunicación con, por ejemplo, pero sin limitación, drones, aeronaves, radios portátiles de fuerzas terrestres u otros dispositivos seguros.

La red 104 ad hoc y la red 106 e infraestructura pueden comprender una red comercial cerrada que comprende canales de comunicación 110/112 configurados para soportar protocolos de comunicación de estándares industriales como, pero sin limitación, el Proyecto de Asociación de Tercera Generación de Evolución a Largo Plazo (3GPP LTE)™, el Proyecto de Asociación de Tercera Generación 2 de Banda Ancha Ultra Móvil (3Gpp2 UMB)™, Acceso Múltiple por División de Código Síncrono de División de Tiempo (TD-SCDMA)™ e Interoperabilidad Inalámbrica para Acceso de Microondas (WiMAX)™, y otros protocolos de comunicación de uso común. Los canales de comunicación 110/112 también pueden configurarse para soportar protocolos de comunicación de datos inalámbricos alternativos o adicionales, incluyendo Wi-Fi™, Bluetooth™, etc.

La figura 2 es una ilustración de un proceso 200 de encriptación de un paquete 224 de red de acuerdo con un modo de realización de la divulgación. El paquete 224 de red comprende una dirección 202 de red (dirección 202 de red no encriptada) y un mensaje 204 de datos. La dirección 202 de red se puede encriptar a través de una Seguridad de las Transmisiones (TRANSEC) utilizando un tiempo 212 GPS del día (tiempo 212 GPS) y un número 214 pseudoaleatorio para proporcionar una dirección 208 de red encriptada. Los datos 204 de mensaje pueden encriptarse mediante un encriptado de seguridad en las comunicaciones (COMSEC) para proporcionar datos 210 encriptados.

Un módulo 222 de encriptación recibe el tiempo 212 GPS y el número 214 pseudoaleatorio en un encriptador 218 del mismo. El encriptador 218 utiliza el tiempo 212 GPS y el número 214 pseudoaleatorio para proporcionar una palabra 216 clave de encriptación (palabra 216 clave). La palabra 216 clave puede ser exclusiva o utilizada por un módulo 220 XOR con la dirección 202 de red para proporcionar la dirección 208 de red encriptada.

TRANSEC es un componente de seguridad en las comunicaciones (COMSEC) que resulta de la aplicación de medidas diseñadas para proteger las transmisiones de la interceptación y la explotación por medios distintos al

criptoanálisis. Los objetivos de seguridad de la transmisión incluyen baja probabilidad de interceptación (LPI), baja probabilidad de detección (LPD), Antiinterferencias-resistencia a interferencias u otra característica. Los modos de realización de la divulgación se pueden utilizar para LPI mediante el uso de cobertura TRANSEC utilizando, por ejemplo, un tiempo GPS del día como el tiempo 212 GPS y un número pseudoaleatorio como el número 214 pseudoaleatorio para el encriptado de la dirección 202 de red para una transmisión a través de una red comercial cerrada como la red 104 ad hoc y la red 106 de infraestructura.

El encriptado es un método para convertir texto sin formato en un formato ilegible e ininteligible llamado texto cifrado. El proceso de conversión de texto cifrado de nuevo a un formato reconocible y legible se denomina desencriptación. Al utilizar el proceso de encriptación, un usuario puede almacenar o enviar información confidencial a través de redes públicas (por ejemplo, utilizando los protocolos SIPRNet existentes en los Estados Unidos) de una manera más segura que simplemente enviando o almacenando datos en texto sin formato. Cuando los usuarios previstos de los datos desean acceder a los datos encriptados, utilizan el proceso de desencriptación para convertir de nuevo el texto cifrado a un formato legible.

La criptografía puede definirse de manera general como la ciencia del uso de las matemáticas para encriptar y desencriptar datos permitiendo el almacenamiento y la transmisión de datos confidenciales de una manera segura. Un sistema criptográfico comprende un algoritmo criptográfico, o cifrado, que es una función matemática para encriptar y desencriptar datos y todas las claves y protocolos posibles que lo hacen funcionar. Utilizando una clave, el cifrado criptográfico se puede utilizar para convertir texto sin formato hacia y desde texto cifrado.

La figura 3 es una ilustración de un diagrama de bloques funcional esquemático de un sistema de enrutamiento 300 encriptado (sistema 300, sistema 300 de encriptación en la figura 1) de acuerdo con un modo de realización de la divulgación. Los diversos bloques, módulos, lógica de procesamiento y circuitos ilustrativos descritos en relación con el sistema 300 pueden implementarse o ejecutarse con un procesador de aplicación general, una memoria de contenido direccionable, un procesador de señales digitales, un circuito integrado de aplicación específica, una matriz de puertas programables por campo, cualquier dispositivo lógico programable adecuado, una lógica de puerta discreta o de transistor, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. El modo de realización mostrado en la figura 3 puede tener funciones, materiales y estructuras que son similares a los modos de realización mostrados en las figuras 1-2. Por lo tanto, es posible que las características, funciones y elementos comunes no se describan de manera redundante aquí.

El sistema 300 puede comprender un módulo 302 de encriptación (222 en la figura 2), un módulo 304 de desencriptación, un módulo 306 receptor, un módulo 308 transmisor, un módulo 310 de comunicación de red, un módulo 312 de procesador y un módulo 314 de memoria. El sistema 300 generalmente comprende una carcasa física (no mostrada).

El sistema 300 ilustrado representa un modo de realización sencillo para facilitar la descripción. Estos y otros elementos del sistema 300 están interconectados entre sí, lo que permite la comunicación entre los diversos elementos del sistema 300. En un modo de realización, estos y otros elementos del sistema 300 pueden interconectarse entre sí a través de un bus 316 de comunicación de datos. El sistema 300 puede implementarse en el dispositivo 108 de comunicación móvil como se explicó anteriormente.

El sistema 300 recibe el paquete 224 de red (Figura 2) que comprende la dirección 208 de red encriptada y los datos 210 encriptados, desencripta la dirección de red 208 encriptada para proporcionar una dirección de red no encriptada y transmite el paquete 224 de red basándose en la dirección de red no encriptada.

El módulo 302 de encriptación (222 en la figura 2) funciona para encriptar el paquete 224 de red como se explicó anteriormente. Además, el módulo 302 de encriptación también calcula la dirección de red de la siguiente etapa para el paquete de red a través de la red comercial cerrada, como la red 104 ad hoc y la red 106 de infraestructura, y encripta la dirección de red de la siguiente etapa utilizando un segundo tiempo GPS y segundo número pseudoaleatorio para proporcionar la dirección 208 de red encriptada. En un modo de realización, el segundo tiempo GPS puede ser el primer tiempo GPS y el segundo número pseudoaleatorio puede ser el primer número pseudoaleatorio. En otros modos de realización, el segundo tiempo GPS puede ser diferente del primer tiempo GPS, y el segundo número pseudoaleatorio puede ser diferente del primer número pseudoaleatorio.

El módulo 304 de desencriptación funciona para desencriptar la dirección 208 de red encriptada (figura 2) para proporcionar la dirección de red 202 no encriptada. El módulo 304 de desencriptación recibe el paquete 224 de red desde el módulo 306 receptor. El paquete 224 de red comprende la dirección de red 208 encriptada que comprende la dirección 202 de red no encriptada encriptada por el tiempo 212 GPS (figura 2) y el número 214 pseudoaleatorio (figura 2). El módulo 304 de desencriptación desencripta la dirección 208 de red encriptada utilizando el tiempo 212 GPS y el número 214 pseudoaleatorio para proporcionar la dirección 202 de red no encriptada. El paquete 224 de red puede transmitirse entonces por el módulo 308 transmisor basándose en la dirección 202 de red no encriptada.

El módulo 306 receptor funciona para recibir el paquete 224 de red a través de una antena 318. El paquete 224 de red comprende la dirección 208 de red encriptada que comprende una dirección de red no encriptada encriptada

mediante un primer tiempo GPS como el tiempo 212 GPS y un primer número pseudoaleatorio, como el número 214 pseudoaleatorio. El paquete 224 de red también puede comprender datos encriptados, como los datos 210 encriptados.

El módulo 308 transmisor funciona para transmitir el paquete 224 de red basándose en la dirección 202 de red no encriptada.

El módulo 310 de comunicación de red funciona para habilitar los canales de comunicación 110/112/114 para la comunicación entre la red 104 ad hoc, la red 106 de infraestructura, la red 102 aislada o cualquier otra red con conmutación de circuitos de red de protocolo de Internet y la red por conmutación de paquetes.

El módulo 306 receptor y el módulo 308 transmisor están acoplados a su respectiva antena 318/320. Aunque en un sistema 300 sencillo puede requerirse solo una antena 318 para recibir información y solo una antena 320 para transmitir información, un sistema 300 más sofisticado puede estar provisto de configuraciones de antena múltiples y/o más complejas. Además, aunque no se muestra en esta figura 3, los expertos en la técnica se darán cuenta que un transmisor puede transmitir a más de un receptor, y que múltiples transmisores pueden transmitir al mismo receptor.

El módulo 312 de procesador puede implementarse, o realizarse, con un procesador de aplicación general, una memoria de contenido direccionable, un procesador de señales digitales, un circuito integrado de aplicación específica, una matriz de puertas programables por campo, cualquier dispositivo lógico programable adecuado, una lógica de puerta discreta o de transistor, componentes de hardware discretos o cualquier combinación de los mismos, diseñados para realizar las funciones descritas en el presente documento. De esta manera, un procesador puede realizarse como un microprocesador, un controlador, un microcontrolador, una máquina de estados o similares.

Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un procesador de señales digitales y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de procesador de señales digitales o cualquier otra configuración de este tipo. En la práctica, los módulos 312 de procesador comprenden la lógica de procesamiento que está configurada para llevar a cabo las funciones, técnicas y tareas de procesamiento asociadas con el funcionamiento del sistema 300.

En concreto, la lógica de procesamiento está configurada para soportar el método de comunicación segura del sistema 300. Por ejemplo, el módulo 312 de procesador puede configurarse de manera adecuada para dirigir al sistema 300 para que encripte la dirección 202 de red no encriptada mediante el primer tiempo 212 GPS y el primer número 214 pseudoaleatorio para proporcionar la dirección 208 de red encriptada y transmitir el paquete 224 de red basándose en la dirección 202 de red no encriptada. Para otro ejemplo, el módulo 312 de procesador puede configurarse de manera adecuada para dirigir al sistema 300 para que desencripte la dirección 208 de red encriptada mediante el primer tiempo 212 GPS y el primer número 214 pseudoaleatorio para proporcionar la dirección 202 de red no encriptada y transmitir el paquete 224 de red basándose en la dirección 202 de red no encriptada.

Además, las etapas de un método o algoritmo descrito en relación con los modos de realización divulgados en el presente documento pueden realizarse directamente en hardware, en firmware, en un módulo de software ejecutado por el módulo 312 de procesador o en cualquier combinación práctica de los mismos.

El módulo 314 de memoria puede realizarse como un dispositivo de almacenamiento no volátil (memoria de semiconductor no volátil, dispositivo de disco duro, dispositivo de disco óptico y similares), un dispositivo de almacenamiento de acceso aleatorio (por ejemplo, SRAM, DRAM) o cualquier otra forma de medio de almacenamiento conocida en la técnica. El módulo 314 de memoria se puede acoplar al módulo 312 de procesador, respectivamente, de modo que el módulo 312 de procesador pueda leer información y escribir información en el módulo 314 de memoria.

Como ejemplo, el módulo 312 de procesador y el módulo 314 de memoria pueden residir en sus respectivos ASIC. El módulo de memoria 314 también puede integrarse en los módulos 312 de procesador respectivamente. En un modo de realización, el módulo 314 de memoria puede incluir una memoria caché para almacenar variables temporales u otra información intermedia durante la ejecución de las instrucciones a ejecutar por el módulo 312 de procesador. El módulo 314 de memoria también puede incluir memoria no volátil para almacenar las instrucciones a ejecutar por el módulo 312 de procesador.

El módulo 314 de memoria puede incluir una base de datos (no mostrada) para almacenar el paquete 224 de red de acuerdo con un modo de realización de la divulgación. La base de datos puede configurarse para almacenar, mantener y proporcionar datos según sea necesario para ayudar a la funcionalidad del sistema 300 de la manera que se describe a continuación. Además, la base de datos puede ser una base de datos local acoplada al módulo 312 de procesador, o puede ser una base de datos remota, por ejemplo, una base de datos de red central, y similares. La base de datos puede incluir una tabla de consulta con el fin de almacenar la información de encriptación. El módulo 314 de memoria también puede almacenar un programa informático que es ejecutado por el

módulo 312 de procesador, un sistema operativo, un programa de aplicación, datos provisionales utilizados en la ejecución de un procesamiento de programa u otra aplicación.

Los expertos en la técnica reconocerán que los diversos bloques, módulos, circuitos y lógica de procesamiento ilustrativos descritos en relación con los modos de realización descritos en el presente documento pueden implementarse en hardware, software legible por ordenador, firmware o cualquier combinación práctica de los mismos. Para ilustrar claramente esta intercambiabilidad y compatibilidad de hardware, firmware y software, varios componentes, bloques, módulos, circuitos y etapas ilustrativos se describen de manera general en cuanto a su funcionalidad.

Si dicha funcionalidad se implementa como hardware, firmware o software depende de la aplicación concreta y las restricciones de diseño impuestas al sistema en general. Aquellos que conocen los conceptos descritos en el presente documento pueden implementar dicha funcionalidad de una manera adecuada para cada aplicación en concreto, pero dichas decisiones de implementación no han de interpretarse como causantes de un alejamiento del alcance de la presente invención.

La Figura 4 es una ilustración de un diagrama de flujo de ejemplo que muestra un proceso 400 para una comunicación segura de acuerdo con un modo de realización de la divulgación. Las diversas tareas realizadas en relación con el proceso 400 pueden realizarse mediante software, hardware, firmware, un medio legible por ordenador que tenga instrucciones ejecutables por ordenador para realizar el método de proceso, o cualquier combinación de los mismos. El proceso 400 puede grabarse en un medio legible por ordenador como una memoria de semiconductor, un disco magnético, un disco óptico y similares, y puede accederse y ejecutarse, por ejemplo, mediante una CPU de ordenador como el módulo 312 de procesador en el que se almacena el medio legible por ordenador.

Hay que señalar que el proceso 400 puede incluir cualquier número de tareas adicionales o alternativas, las tareas que se muestran en la figura 4 no necesitan realizarse en el orden ilustrado, y el proceso 400 puede incorporarse en un procedimiento o proceso más completo que tenga funcionalidades adicionales no descritas en detalle en el presente documento. En modos de realización prácticos, porciones del proceso 400 pueden ser realizadas por diferentes elementos 100 del entorno, el paquete 224 de red y el sistema 300 como: el dispositivo 108 de comunicación móvil, el módulo 302 de encriptación, el módulo 304 de desencriptación, el módulo 306 receptor, el módulo 308 transmisor, el módulo 310 de comunicación de red, el módulo 312 de procesador, el módulo 314 de memoria, etc. El proceso 400 puede tener funciones, materiales y estructuras que son similares a los modos de realización mostrados en las figuras 1-3. Por lo tanto, es posible que las características, funciones y elementos comunes no se describan de manera redundante aquí.

El proceso 400 puede comenzar recibiendo un paquete de red como el paquete 224 de red que comprende una dirección de red encriptada como la dirección 208 de red encriptada que comprende una dirección de red no encriptada como la dirección 202 de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio, como el primer tiempo 212 GPS y el primer número 214 pseudoaleatorio respectivamente (tarea 402).

El proceso 400 puede continuar con la desencriptación de la dirección 208 de red encriptada utilizando el primer tiempo 212 GPS y el primer número 214 pseudoaleatorio para proporcionar la dirección 202 de red no encriptada (tarea 404).

El proceso 400 puede continuar con la transmisión del paquete 224 de red basándose en la dirección 202 de red no encriptada (tarea 406).

El proceso 400 puede continuar con el cálculo de una dirección de red de la siguiente etapa para el paquete de red a través de una red comercial cerrada como la red 104 ad hoc y la red 106 de infraestructura (tarea 408).

El proceso 400 puede continuar con el encriptado de la dirección de red de la siguiente etapa utilizando un segundo tiempo GPS y un segundo número pseudoaleatorio para proporcionar la dirección 208 de red encriptada (tarea 410). Como se mencionó anteriormente, en un modo de realización, el segundo tiempo GPS puede ser el primer tiempo 212 GPS y el segundo número pseudoaleatorio puede ser el primer número 214 pseudoaleatorio. En otros modos de realización, el segundo tiempo GPS puede ser diferente del primer tiempo 212 GPS, y el segundo número pseudoaleatorio puede ser diferente del primer número 214 pseudoaleatorio. El proceso 400 puede continuar con la transmisión del paquete 224 de red a través de la red comercial cerrada (tarea 412).

Si bien al menos un modo de realización de ejemplo se ha presentado en la anterior descripción detallada, hay que señalar que existe un gran número de variaciones. También hay que señalar que el modo de realización de ejemplo o los modos de realización descritos en el presente documento no pretenden limitar el alcance, la aplicabilidad o la configuración de la materia de ninguna manera. Más bien, la anterior descripción detallada proporcionará a los expertos en la técnica un plan de trabajo conveniente para implementar el modo de realización o modos de realización descritos. Ha de entenderse que se pueden realizar varios cambios en la función y la disposición de los elementos sin apartarse del alcance definido por las reivindicaciones, que incluye equivalentes conocidos y equivalentes previsibles en el momento de la presentación de esta solicitud de patente.

En este documento, el término "módulo" como se utiliza en el presente documento, se refiere a software, firmware, hardware y cualquier combinación de estos elementos para realizar las funciones asociadas descritas en el presente documento. Además, con fines expositivos, los diversos módulos se describen como módulos discretos; sin embargo, como será evidente para un experto en la técnica, se pueden combinar dos o más módulos para formar un único módulo que realice las funciones asociadas de acuerdo con los modos de realización de la presente divulgación.

En este documento, los términos "producto de programa informático", "medio legible por ordenador" y similares pueden utilizarse de manera general para referirse a medios como, por ejemplo, memoria, dispositivos de almacenamiento o unidad de almacenamiento. Estas y otras formas de medios legibles por ordenador pueden involucrarse en el almacenamiento de una o más instrucciones para su uso por los módulos 312 de procesador para hacer que los módulos 312 de procesador realicen operaciones específicas. Dichas instrucciones, generalmente conocidas como "código de programa informático" o "código de programa" (que pueden agruparse en forma de programas informáticos u otros agrupamientos), cuando se ejecutan, permiten un método de utilización de un sistema.

La descripción anterior se refiere a elementos o nodos o características que están "conectados/as" o "acoplados/as" juntos. Como se utiliza en el presente documento, a menos que se indique expresamente lo contrario, "conectado/a" significa que un elemento/nodo/característica se une directamente a (o se comunica directamente con) otro elemento/nodo/característica y no necesariamente de manera mecánica. Del mismo modo, a menos que se indique expresamente lo contrario, "acoplado/a" significa que un elemento/nodo/característica se une directa o indirectamente a (o se comunica directa o indirectamente con) otro elemento/nodo/característica y no necesariamente de manera mecánica. Por tanto, aunque las figuras 1-3 representan ejemplos de disposiciones de elementos, elementos, dispositivos, características o componentes intermedios adicionales pueden estar presentes en un modo de realización de la divulgación.

Los términos y frases utilizados en este documento y las variaciones de los mismos, a menos que se indique expresamente lo contrario, han de interpretarse como de uso general y no como limitativos. Como ejemplos de lo anterior: el término "que incluye" ha de leerse con el significado de "que incluye, sin limitación" o similares; el término "ejemplo" se utiliza para proporcionar casos de ejemplo del objeto expuesto, no una lista exhaustiva o limitativa del mismo; y los adjetivos como "convencional", "tradicional", "normal", "estándar", "conocido/a" y los términos de significado similar no han de interpretarse como limitantes del objeto descrito a un período de tiempo determinado o a un objeto disponible a partir de un momento determinado, sino que, por el contrario, ha de interpretarse en el sentido de que abarcan tecnologías convencionales, tradicionales, normales o estándar que pueden estar disponibles o conocidas ahora o en cualquier momento en el futuro.

Del mismo modo, un grupo de objetos vinculados con la conjunción "y" no ha de interpretarse como un requisito para que todos y cada uno de esos objetos estén presentes en el agrupamiento, sino que ha de interpretarse como "y/o" a menos que se indique expresamente lo contrario. De la misma manera, un grupo de objetos vinculados con la conjunción "o" no ha de interpretarse como que se requiera de exclusividad mutua entre ese grupo, sino que también ha de interpretarse como "y/o" a menos que se indique expresamente lo contrario.

Además, aunque los objetos, elementos o componentes de la divulgación pueden describirse o reivindicarse en singular, se contempla que el plural esté dentro del alcance de la misma a menos que se establezca explícitamente la limitación al singular. La presencia de palabras y frases ampliadas como "uno/a o más", "al menos", "pero no limitada/a a" u otras frases similares en algunos casos no debe interpretarse en el sentido de que la intención o la necesidad de un caso más restringido sea mayor en los casos en que dichas frases de ampliación puedan estar ausentes. El término "aproximadamente" cuando se refiere a un valor o rango numérico pretende abarcar los valores resultantes de un error experimental que puede ocurrir al tomar mediciones.

Como se utiliza en el presente documento, a menos que se indique expresamente lo contrario, "que funciona" significa que se puede utilizar, es apto o listo para su uso o servicio, que se puede utilizar para un propósito específico, y que es capaz de realizar una función mencionada o deseada descrita en el presente documento. En relación con los sistemas y dispositivos, el término "que funciona" significa que el sistema y/o el dispositivo es totalmente funcional y está calibrado, comprende elementos para, y cumple con los requisitos de funcionamiento aplicables para realizar una función mencionada cuando se activa. En relación con los sistemas y circuitos, el término "que funciona" significa que el sistema y/o el circuito es totalmente funcional y está calibrado, comprende lógica para, y cumple con los requisitos de funcionamiento aplicables para realizar una función mencionada cuando se activa.

REIVINDICACIONES

1. Un método para una comunicación segura, el método que comprende:

recibir (402) un paquete de red que comprende una dirección de red encriptada que comprende una dirección de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio;

desencriptar (404) la dirección de red encriptada utilizando el primer tiempo GPS y el primer número pseudoaleatorio para proporcionar la dirección de red no encriptada;

transmitir (406) el paquete de red basándose en la dirección de red no encriptada; y

calcular (408) una dirección de red de la siguiente etapa para el paquete de red a través de una red comercial cerrada; y

encriptar (410) la dirección de red de la siguiente etapa utilizando un segundo tiempo GPS y un segundo número pseudoaleatorio para proporcionar la dirección de red encriptada.

2. El método de la reivindicación 1, que comprende además transmitir el paquete de red a través de la red comercial cerrada.

3. El método de la reivindicación 1, en donde la red comercial cerrada comprende una o más de una red IP, una red de conmutación por paquetes, una red con conmutación de circuitos o una red de comunicación inalámbrica.

4. El método de la reivindicación 3, en donde el segundo tiempo GPS es el primer tiempo GPS, y el segundo número pseudoaleatorio es el primer número pseudoaleatorio.

5. El método de la reivindicación 3, en donde el segundo tiempo GPS es diferente del primer tiempo GPS, y el segundo número pseudoaleatorio es diferente del primer número pseudoaleatorio.

6. Un sistema para una comunicación segura, el sistema que comprende:

un módulo (306) receptor que funciona para recibir un paquete de red que comprende una dirección de red encriptada que comprende una dirección de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio;

un módulo (304) de desencriptación que funciona para desencriptar la dirección de red encriptada utilizando el primer tiempo GPS y el primer número pseudoaleatorio para proporcionar la dirección de red no encriptada;

un módulo (308) transmisor que funciona para transmitir el paquete de red basándose en la dirección de red no encriptada;

un módulo (302) de encriptación que funciona para calcular una dirección de red de la siguiente etapa para el paquete de red a través de una red comercial cerrada; y

encriptar la dirección de red de la siguiente etapa utilizando un segundo tiempo GPS y un segundo número pseudoaleatorio para proporcionar la dirección de red encriptada.

7. El sistema de la reivindicación 6, en donde el módulo (308) transmisor puede además funcionar para transmitir el paquete de red a través de la red comercial cerrada.

8. El sistema de la reivindicación 6, en donde la red comercial cerrada comprende una o más de una red IP, una red de conmutación por paquetes, una red con conmutación de circuitos o una red de comunicación inalámbrica.

9. El sistema de la reivindicación 8, en donde el segundo tiempo GPS es el primer tiempo GPS, y el segundo número pseudoaleatorio es el primer número pseudoaleatorio.

10. El sistema de la reivindicación 8, en donde el segundo tiempo GPS es diferente del primer tiempo GPS, y el segundo número pseudoaleatorio es diferente del primer número pseudoaleatorio.

11. Un medio de almacenamiento legible por ordenador que comprende instrucciones ejecutables por ordenador para realizar un método para una comunicación segura, el método ejecutado por las instrucciones ejecutables por ordenador que comprende:

recibir (402) un paquete de red que comprende una dirección de red encriptada que comprende una dirección de red no encriptada encriptada mediante un primer tiempo GPS y un primer número pseudoaleatorio;

desencriptar (404) la dirección de red encriptada utilizando el primer tiempo GPS y el primer número pseudoaleatorio para proporcionar la dirección de red no encriptada;

transmitir el paquete de red basándose en la dirección de red no encriptada; y

calcular una dirección de red de la siguiente etapa para el paquete de red a través de una red comercial cerrada; y

encriptar la dirección de red de la siguiente etapa utilizando un segundo tiempo GPS y un segundo número pseudoaleatorio para proporcionar la dirección de red encriptada.

12. El medio de almacenamiento legible por ordenador de la reivindicación 11, el método ejecutado por las instrucciones ejecutables por ordenador que comprende además transmitir el paquete de red a través de una red comercial cerrada.

13. El medio de almacenamiento legible por ordenador de la reivindicación 11, en donde la red comercial cerrada comprende una o más de una red IP, una red de conmutación por paquetes, una red con conmutación de circuitos o una red de comunicación inalámbrica.

14. El medio de almacenamiento legible por ordenador de la reivindicación 13, en donde el segundo tiempo GPS es el primer tiempo GPS, y el segundo número pseudoaleatorio es el primer número pseudoaleatorio.

15. El medio de almacenamiento legible por ordenador de la reivindicación 13, en donde el segundo tiempo GPS es diferente del primer tiempo GPS, y el segundo número pseudoaleatorio es diferente del primer número pseudoaleatorio.

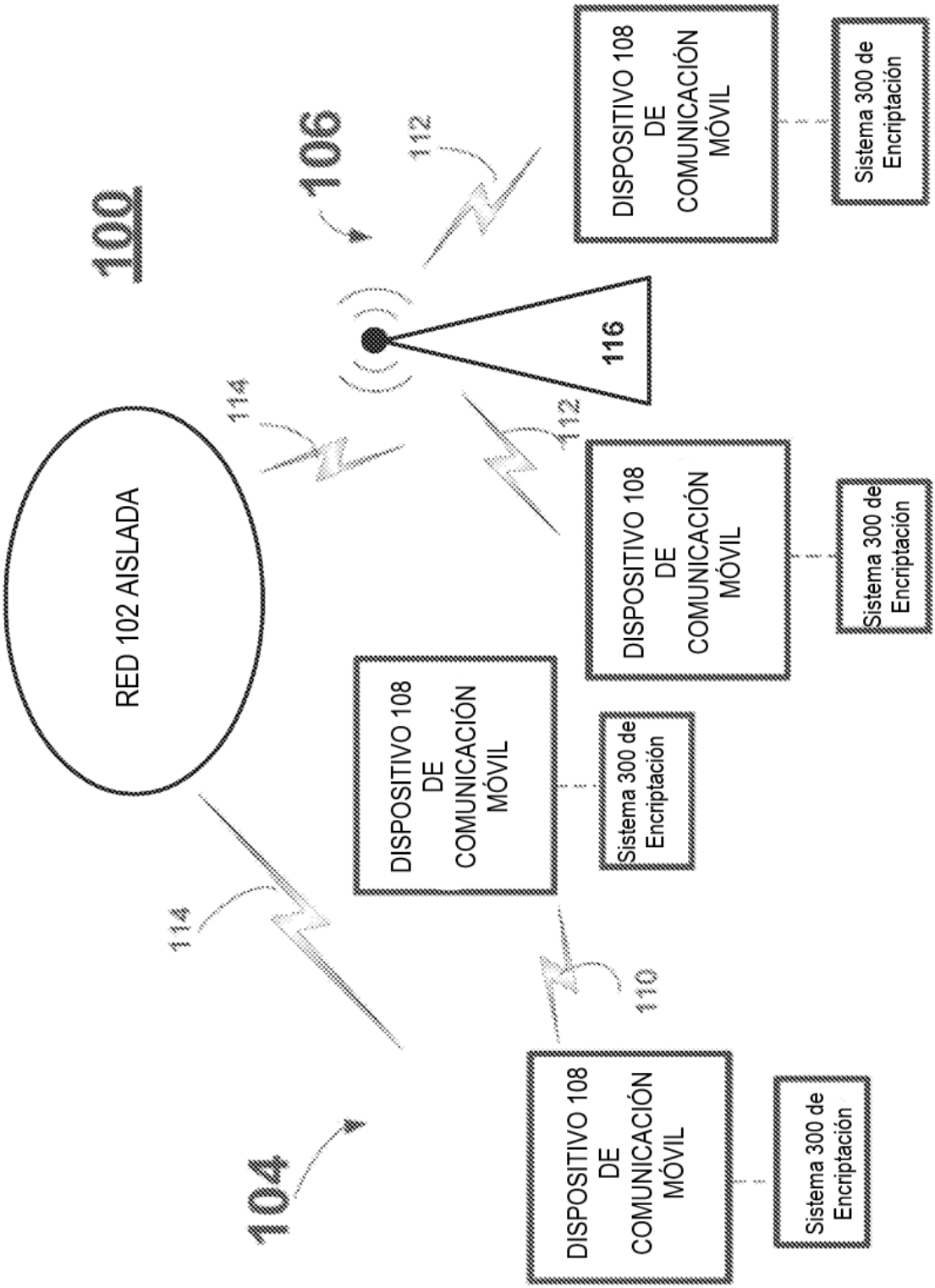
100
RED 102 AISLADA
104
106
116
112
114
110
DISPOSITIVO 108 DE COMUNICACIÓN MÓVIL
Sistema 300 de Encriptación

FIG. 1

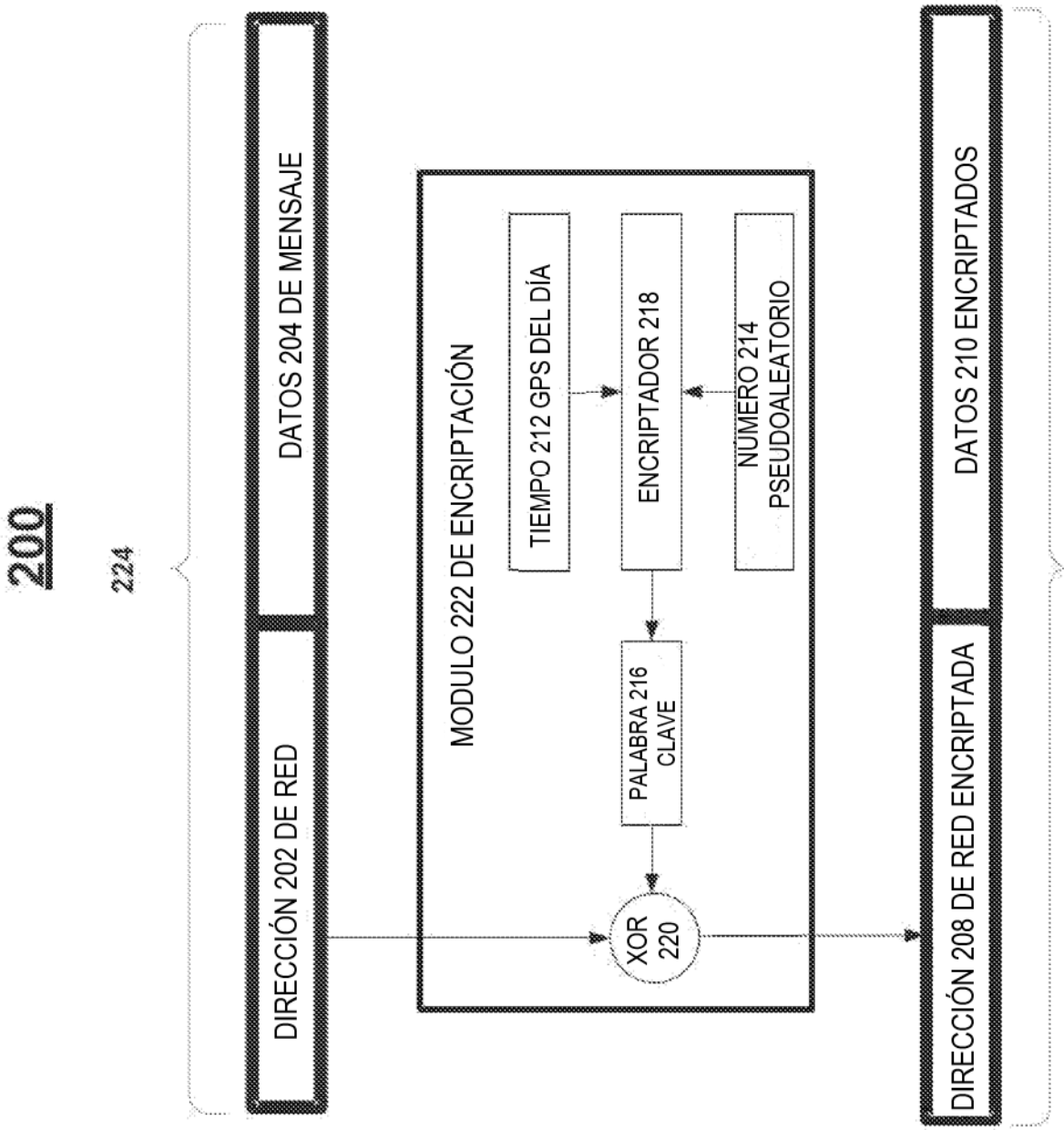
200
224
DIRECCIÓN 202 DE RED
DATOS 204 DE MENSAJE
MODULO 222 DE ENCRIPTACIÓN
TIEMPO 212 GPS DEL DÍA
ENCRIPTADOR 218
NÚMERO 214 PSEUDOALEATORIO
PALABRA 216 CLAVE
XOR 220
DIRECCIÓN 208 DE RED ENCRIPTADA
DATOS 210 ENCRIPTADOS
224

FIG. 2

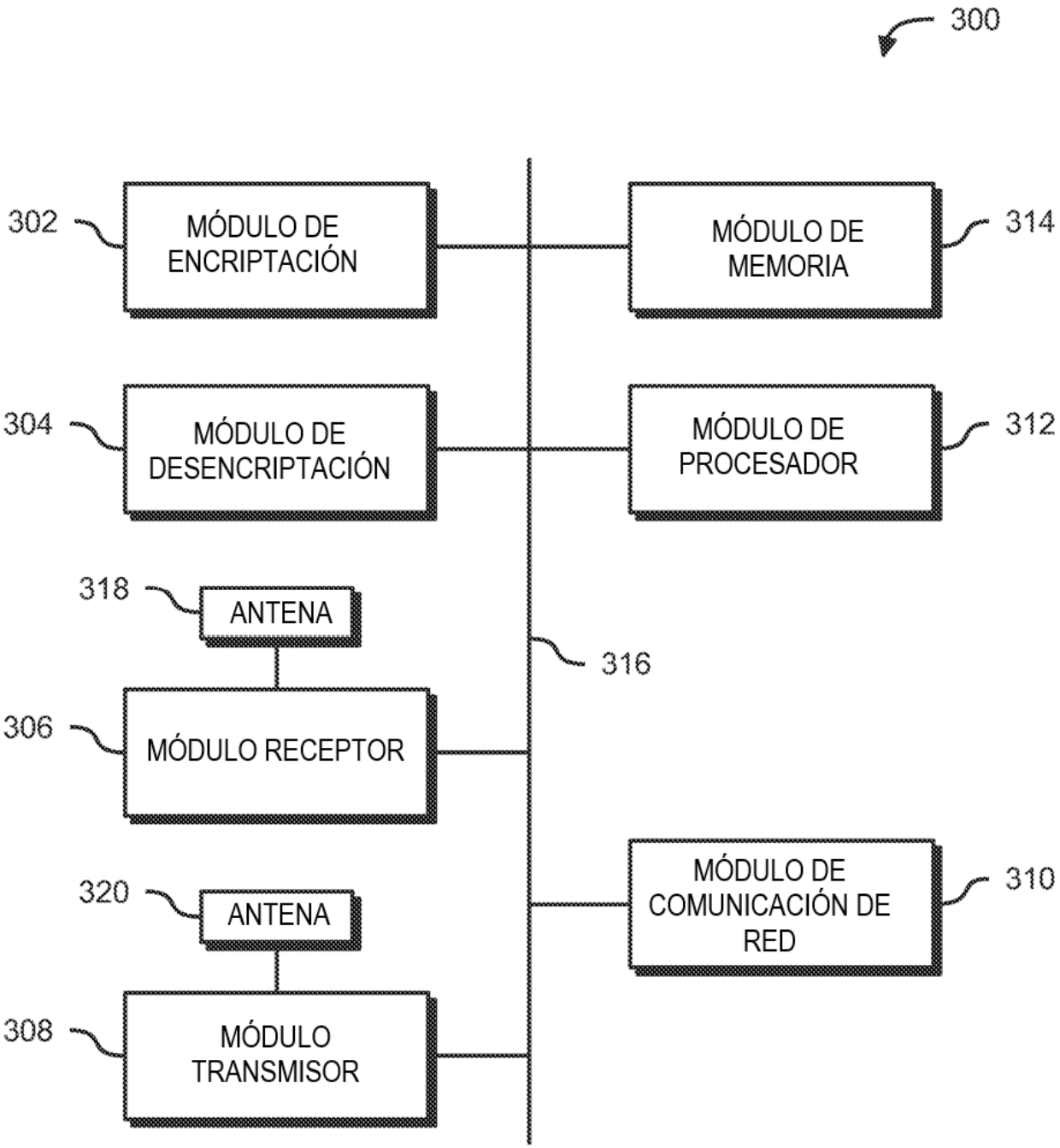
300
302
MÓDULO DE ENCRIPTACIÓN
314
MÓDULO DE MEMORIA
304
MÓDULO DE DESENCRIPTACIÓN
312
MÓDULO DE PROCESADOR
318
ANTENA
316
306
MÓDULO RECEPTOR
310
MÓDULO DE COMUNICACIÓN DE RED
320
ANTENA
308
MÓDULO TRANSMISOR

FIG. 3

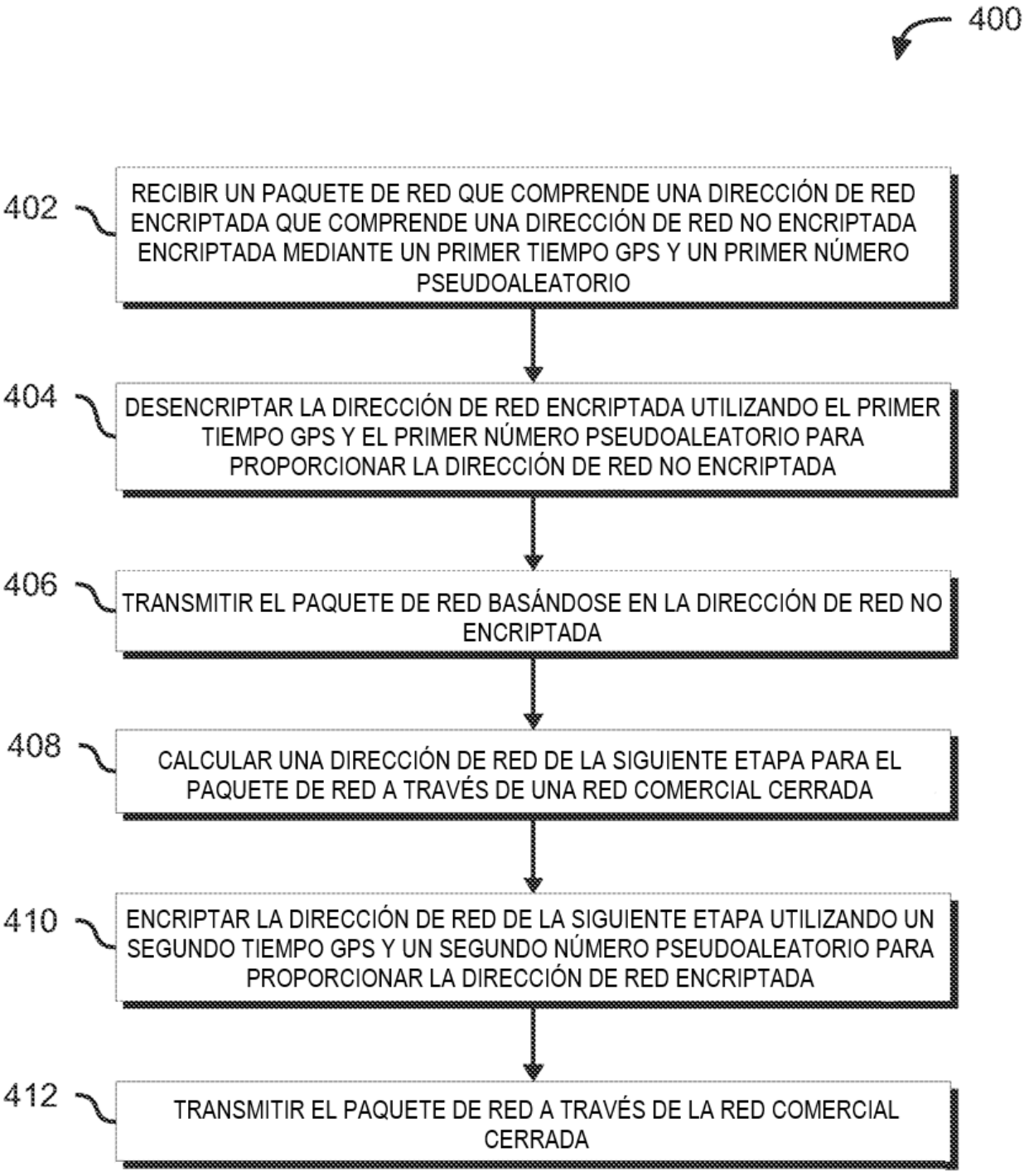
400
402
RECIBIR UN PAQUETE DE RED QUE COMPRENDE UNA DIRECCIÓN DE RED ENCRIPTADA QUE COMPRENDE UNA DIRECCIÓN DE RED NO ENCRIPTADA ENCRIPTADA MEDIANTE UN PRIMER TIEMPO GPS Y UN PRIMER NÚMERO PSEUDOALEATORIO
404
DESENCRIPTAR LA DIRECCIÓN DE RED ENCRIPTADA UTILIZANDO EL PRIMER TIEMPO GPS Y EL PRIMER NÚMERO PSEUDOALEATORIO PARA PROPORCIONAR LA DIRECCIÓN DE RED NO ENCRIPTADA
406
TRANSMITIR EL PAQUETE DE RED BASÁNDOSE EN LA DIRECCIÓN DE RED NO ENCRIPTADA
408
CALCULAR UNA DIRECCIÓN DE RED DE LA SIGUIENTE ETAPA PARA EL PAQUETE DE RED A TRAVÉS DE UNA RED COMERCIAL CERRADA
410
ENCRIPTAR LA DIRECCIÓN DE RED DE LA SIGUIENTE ETAPA UTILIZANDO UN SEGUNDO TIEMPO GPS Y UN SEGUNDO NÚMERO PSEUDOALEATORIO PARA PROPORCIONAR LA DIRECCIÓN DE RED ENCRIPTADA
412
TRANSMITIR EL PAQUETE DE RED A TRAVÉS DE LA RED COMERCIAL CERRADA

FIG. 4