(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 442 015**

(51) Int. CI.:

H04W 8/26 (2009.01)
H04W 8/00 (2009.01)
H04W 48/08 (2009.01)
H04W 92/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.07.2008 E 08772383 (9)**

(97) Fecha y número de publicación de la concesión europea: **09.10.2013 EP 2168334**

(54) Título: **Entrega de nuevos identificadores en una red punto a punto**

(30) Prioridad:

10.07.2007 US 948966 P
27.06.2008 US 147967

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.02.2014

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
ATTN: INTERNATIONAL IP ADMINISTRATION,
5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121-1714, US

(72) Inventor/es:

PARK, VINCENT D.;
LAROIA, RAJIV y
LI, JUNYI

(74) Agente/Representante:

FÀBREGA SABATÉ, Xavier

DESCRIPCIÓN

Entrega de nuevos identificadores en una red punto a punto.

ANTECEDENTES

I. Campo

La siguiente descripción se refiere en general a las comunicaciones inalámbricas, y más concretamente de archivos descubrimiento en redes punto a punto ad hoc.

II. Antecedentes

Los sistemas o las redes de comunicación inalámbrica están ampliamente desplegados para proporcionar diversos tipos de comunicación, por ejemplo, voz y/o datos pueden proporcionarse mediante sistemas de comunicación inalámbrica. Un sistema o una red de comunicación inalámbrica típicos, puede proporcionar acceso múltiple a los usuarios a uno o más recursos compartidos. Por ejemplo, un sistema puede utilizar una variedad de múltiples técnicas de acceso tales como multiplexación por división de frecuencia (FDM), multiplexación por división de tiempo (TDM), multiplexación por división de código (CDM), multiplexación por división ortogonal de frecuencia (OFDM) y otros.

Las redes de comunicación inalámbricas se utilizan comúnmente para transmitir información sin importar dónde se encuentre el usuario (dentro o fuera de una estructura) y si un usuario está parado o en movimiento (por ejemplo, en un vehículo, caminando). En general, las redes de comunicación inalámbricas se establecen a través de un dispositivo móvil que se comunica con una estación base, punto de acceso o enrutador de acceso. El punto de acceso abarca una zona geográfica o célula y, al funcionar el dispositivo móvil, puede moverse dentro y fuera de estas células geográficas.

Algunas redes pueden construirse utilizando únicamente la comunicación punto a punto, sin la utilización de estaciones base, puntos de acceso o enrutadores de acceso. Este tipo de redes se denominan a veces redes ad hoc. La comunicación en este tipo de redes puede, en algunos casos, limitarse a los intercambios entre los dispositivos que se encuentran dentro del rango de transmisión inalámbrica directa entre ellos, mientras que en otros casos puede darse soporte a transmisiones de múltiples saltos enviadas entre los dispositivos no adyacentes. Se pueden utilizar diversas técnicas para mantener la conectividad y/o enviar información, tal como la topología de los cambios en la red (por ejemplo, como los dispositivos se unen, abandonan o se mueven). Algunas redes pueden construirse utilizando una combinación de ambos, punto a punto y estaciones de base, puntos de acceso o enrutadores de acceso.

Dado que los dispositivos se mueven dentro y fuera de las redes, el potencial para las comunicaciones de capas superiores con otros dispositivos puede determinarse en base a un proceso de descubrimiento de homólogos.

Un procedimiento para transmitir y recibir paquetes en una red combinada cableada e inalámbrica ha sido publicado en la solicitud de patente US 2004/0090958.

La solicitud de patente US 2003/0112823 describe procedimientos que permiten las comunicaciones que deben establecerse independientemente de la presencia de bloqueadores de comunicaciones en el camino entre dos dispositivos de computación.

En el contexto de las identidades punto a punto, la solicitud de patente US 2004/0111515 se refiere a las interfaces de programación de aplicaciones que permiten a una aplicación crear, importar, exportar, gestionar, enumerar y eliminar identidades punto a punto.

Para permitir el descubrimiento de homólogos, la información asociada con un dispositivo (por ejemplo, identificador, forma de establecer la comunicación, etc.) se publicada o anuncia (por ejemplo, difusión) a otros dispositivos dentro del alcance. Esto puede comprometer el anonimato y puede conducir a problemas de privacidad.

La solicitud de patente internacional WO 2007/012881 se refiere a un procedimiento en una red móvil para asociar un número adicional para servicios de voz o de mensajería con un módulo de identidad existente asociado de forma desmontable con un dispositivo de telefonía móvil.

RESUMEN

La invención se define por las reivindicaciones independientes.

A continuación se presenta un resumen simplificado de uno o más aspectos con el fin de proporcionar una comprensión básica de dichos aspectos. Este resumen no es una extensa visión general de todos los aspectos

contemplados, y no pretende identificar los elementos clave o críticos de todos los aspectos ni delimitar el alcance de cualquiera o de todos los aspectos. Su único propósito es presentar algunos conceptos de uno o más aspectos en una forma simplificada como un preludio a la descripción más detallada que se presenta más adelante.

De acuerdo con uno o más aspectos y la correspondiente divulgación de los mismos, se describen diversos aspectos en relación con facilitar la asignación de un primer identificador basado en un segundo identificador para aumentar la seguridad. Un par puede ser elegido de forma explícita para recibir una clave asociada con el primer identificador y, teniendo conocimiento del primer identificador y de la clave, puede determinar el segundo identificador. Como tal, el par puede establecer la comunicación con el dispositivo de envío. La clave puede tener un rango de validez asociado, después del que expira la clave. De acuerdo con algunos aspectos, el primer identificador es un identificador público y el segundo identificador es un identificador privado.

Un aspecto se refiere a un procedimiento para transmitir información de descubrimiento de homólogos. El procedimiento incluye generar una pluralidad de claves asociadas con un primer identificador y comunicar el primer identificador y por lo menos una clave de la pluralidad de claves a un primer nodo homólogo. El procedimiento también incluye derivar un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves y anunciar el segundo identificador a una pluralidad de nodos homólogos.

Otro aspecto se refiere a un aparato de comunicaciones inalámbricas que comprende una memoria y un procesador. La memoria retiene instrucciones relacionadas con la generación de una pluralidad de claves asociadas con un primer identificador y comunicar el primer identificador y por lo menos una clave de la pluralidad de claves a un primer nodo homólogo. La memoria también retiene instrucciones relacionadas con derivar un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves y anunciar el segundo identificador a una pluralidad de nodos homólogos. El procesador está acoplado a la memoria y configurado para ejecutar las instrucciones retenidas en la memoria.

Otro aspecto más, se refiere a un aparato que comprende un medio para crear una pluralidad de claves asociadas con un primer identificador y un medio para transmitir el primer identificador y por lo menos una clave de la pluralidad de claves a un primer nodo homólogo. El aparato incluye también un medio para derivar un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves y un medio para anunciar el segundo identificador a una pluralidad de nodos homólogos.

Un aspecto adicional se refiere a un producto de programa de ordenador que comprende un medio legible por ordenador. El medio legible por ordenador incluye un primer conjunto de códigos para hacer que un ordenador para generar una pluralidad de claves asociadas con un primer identificador y un segundo conjunto de códigos para hacer que el ordenador se comunique el primer identificador y por lo menos una clave de la pluralidad de claves para un primer nodo homólogo. El medio legible por ordenador también incluye un tercer conjunto de códigos para hacer que el ordenador para derivar un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves y un cuarto conjunto de códigos para hacer que el ordenador anunciar el segundo identificador a una pluralidad de nodos homólogos.

Otro aspecto se refiere a al menos un procesador configurado para transmitir información de descubrimiento de homólogos. El procesador incluye un primer módulo para la creación de una pluralidad de claves asociadas con un primer identificador y un segundo módulo para comunicar el primer identificador y por lo menos una clave de la pluralidad de claves a un primer nodo homólogo. También se incluye en el procesador un tercer módulo para derivar un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves y un cuarto módulo para anunciar el segundo identificador a una pluralidad de nodos homólogos.

Un aspecto adicional se refiere a un procedimiento para recibir información de descubrimiento de homólogos. El procedimiento incluye recibir un primer identificador y al menos una clave asociada con un nodo homólogo y determinar un segundo identificador a base a, al menos en parte, el primer identificador y la al menos una clave. El procedimiento también incluye monitorizar la recepción del segundo identificador.

Sin embargo, otro aspecto se refiere a un aparato de comunicaciones inalámbricas que comprende una memoria y un procesador. La memoria retiene instrucciones relacionadas con recibir un primer identificador y al menos una clave asociada con un nodo homólogo, determinar un segundo identificador en base a, al menos en parte, el primer identificador y la al menos una clave, y monitorizar la recepción del segundo identificador. El procesador está acoplado a la memoria y está configurado para ejecutar las instrucciones retenidas en la memoria.

Otro aspecto adicional se refiere a un aparato que comprende un medio para recibir un primer identificador y al menos una clave asociada con un nodo homólogo. También se incluye en el aparato un medio para determinar un segundo identificador en base a, al menos en parte, el primer identificador y la al menos una clave y un medio para monitorizar la recepción del segundo identificador.

Otro aspecto se refiere a un producto de programa de ordenador que comprende un medio legible por ordenador. El medio legible por ordenador incluye un primer conjunto de códigos para hacer que un ordenador reciba un primer

identificador y al menos una clave asociada con un nodo homólogo. El medio legible por ordenador también incluye un segundo conjunto de códigos para hacer que el equipo determine un segundo identificador a base a, al menos en parte, el primer identificador y la al menos una clave y un tercer conjunto de códigos para hacer que el ordenador monitoriza la recepción del segundo identificador.

Otro aspecto adicional se refiere a al menos un procesador configurado para transmitir información de descubrimiento de homólogos. El procesador incluye un primer módulo para recibir un primer identificador y al menos una clave asociada con un nodo homólogo y un segundo módulo para determinar un segundo identificador en base a, al menos en parte, el primer identificador y la al menos una clave. También se incluye un tercer módulo para monitorizar la recepción del segundo identificador y un cuarto módulo para recibir un identificador anunciado por un nodo cercano. Un quinto módulo para determinar si el identificador recibido es el segundo identificador determinado también está incluido en el procesador.

Para la realización de los fines anteriores y relacionados, el uno o más aspectos comprenden las características descritas en lo sucesivo plenamente y particularmente señaladas en las reivindicaciones. La siguiente descripción y los dibujos adjuntos indican en detalle ciertas características ilustrativas de los uno o más aspectos. Estas características son indicativas, sin embargo, de sólo algunas de las diversas formas en las que pueden emplearse los principios de los diversos aspectos. Otras ventajas y características novedosas se pondrán de manifiesto a partir de la siguiente descripción detallada cuando se consideran en conjunto con los dibujos y los aspectos descritos están destinados a incluir todos estos aspectos y sus equivalentes.

Breve descripción de los dibujos

La Figura 1 ilustra una red de comunicación inalámbrica de acuerdo con diversos aspectos presentados en este documento.

La Figura 2 ilustra un sistema que genera y distribuye selectivamente la información para facilitar el descubrimiento de homólogos.

La Figura 3 ilustra un ejemplo de sistema que monitoriza la información de detección de homólogos.

La Figura 4 muestra claves de seguridad con diferentes periodos de usabilidad.

La Figura 5 ilustra un ejemplo de derivar una clave de nivel inferior en base a una clave de nivel más alto y alguna información conocida.

La Figura 6 ilustra un ejemplo de obtención de una o más claves de nivel inferior en base a una clave de nivel más alto y por lo menos dos piezas distintas de información conocida.

La Figura 7 ilustra un procedimiento para transmitir información de descubrimiento de homólogos.

La Figura 8 ilustra un procedimiento para recibir información de descubrimiento de homólogos.

La Figura 9 ilustra un ejemplo de terminal inalámbrico de acuerdo con una o más de los aspectos divulgados.

La Figura 10 ilustra un ejemplo de sistema para la transmisión de información de detección de homólogos.

La Figura 11 ilustra un ejemplo de sistema que recibe información de descubrimiento de homólogos.

Descripción detallada

Varios aspectos se describen a continuación con referencia a los dibujos. En la siguiente descripción, con fines explicativos, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión completa de uno o más aspectos. Puede ser evidente, sin embargo, que tal(es) aspecto(s) puede(n) ponerse en práctica sin estos detalles específicos. En otros casos, estructuras y dispositivos bien conocidos se muestran en forma de diagrama de bloques con el fin de facilitar la descripción de estos aspectos.

Tal como se utiliza en esta solicitud, los términos "componente", "módulo", "sistema", y similares pretenden hacer referencia a una entidad relacionada con las computadoras, ya sea hardware, firmware, una combinación de hardware y software, software, o software en la ejecución. Por ejemplo, un componente puede ser, pero no se limita a ser, un proceso que se ejecuta en un procesador, un procesador, un objeto, un ejecutable, un hilo de ejecución, un programa, y/o un ordenador. A modo de ilustración, tanto una aplicación que se ejecuta en un dispositivo de computación como tal dispositivo pueden ser un componente. Uno o más componentes pueden residir dentro de un proceso y/o hilo de ejecución y un componente puede estar localizado en un ordenador y/o distribuido entre dos o más ordenadores. Además, estos componentes pueden ejecutarse desde diversos medios legibles por ordenador que tienen diversas estructuras de datos almacenadas en los mismos. Los componentes pueden comunicarse por

medio de procesos locales y/o remotos de acuerdo con una señal que tiene uno o más paquetes de datos (por ejemplo, datos de un componente interactuando con otro componente en un sistema local, sistema distribuido y/o a través de una red tal como Internet con otros sistemas por medio de la señal).

Además, se describen diversos aspectos en este documento en relación con un terminal inalámbrico. Un terminal inalámbrico también puede denominarse sistema, unidad de abonado, estación de abonado, estación móvil, móvil, dispositivo móvil, estación de dispositivo remoto, terminal remoto, terminal de acceso, terminal de usuario, terminal, dispositivo de comunicación inalámbrica, agente de usuario, dispositivo del usuario o equipo de usuario (UE). Un terminal móvil puede ser un teléfono celular, un teléfono inalámbrico, un protocolo de inicio de teléfono de Sesión (SIP), un teléfono inteligente, una estación de bucle local inalámbrico (WLL), un asistente digital personal (PDA), un ordenador portátil, un dispositivo de comunicación portátil, un dispositivo de computación portátil, una radio por satélite y/u otro dispositivo de procesamiento para la comunicación a través de un sistema inalámbrico. Por otra parte, se describen diversos aspectos en este documento en conexión con una estación base. Una estación base puede ser utilizada para la comunicación con el(los) terminal(es) inalámbrico(s) y también puede denominarse punto de acceso, Nodo B o alguna otra terminología.

Varios aspectos o características se presentan en términos de sistemas que pueden incluir una serie de dispositivos, componentes, módulos y similares. Se debe entender y apreciar que los distintos sistemas pueden incluir dispositivos adicionales, componentes, módulos, etcétera y/o pueden no incluir todos los dispositivos, componentes, módulos, etcétera, discutidos en conexión con las figuras. También puede utilizarse una combinación de estos enfoques.

Haciendo referencia ahora a La Figura 1, se ilustra una red de comunicación inalámbrica 100 de acuerdo con diversos aspectos presentados en este documento. La red 100 puede ser una red de comunicación inalámbrica ad hoc y puede dar soporte a comunicaciones punto a punto. Durante la comunicación punto a punto, nodos, dispositivos, terminales o estaciones podrán comunicarse directamente entre sí, en lugar de utilizar estaciones base, puntos de acceso y/o enrutadores de acceso para traspasar o transmitir comunicaciones. En algunas de tales redes, los dispositivos dentro de la red pueden transmitir o reenviar el tráfico destinado a otros dispositivos. Algunas redes ad hoc pueden incluir dos terminales y puntos de acceso.

La red 100 puede incluir cualquier número de dispositivos móviles o nodos, de los cuales se ilustran seis, que dan soporte a la comunicación inalámbrica. Los dispositivos móviles pueden ser, por ejemplo, teléfonos móviles, teléfonos inteligentes, computadoras portátiles, dispositivos portátiles de comunicación, dispositivos informáticos portátiles, radios satélite, sistemas de posicionamiento global, PDAs y/o cualquier otro dispositivo adecuado para la comunicación a través del sistema de comunicación inalámbrica 100. Los nodos, tal como se utilizan en este documento, incluyen dispositivos móviles, puntos de acceso, estaciones de base, enrutadores de acceso, o similares.

Los nodos 102, 104, 106, 108, 110, y 112 se ilustran como configurados en topología punto a punto ad hoc. Cada nodo puede estar dentro del alcance de uno o más de otros nodos y puede comunicarse con los otros nodos a través de la utilización de otros nodos, tales como en una topología de múltiples saltos (por ejemplo, las comunicaciones pueden saltar de nodo a nodo hasta llegar a un destino final). Por ejemplo, un nodo emisor 102 puede desear comunicarse con el nodo receptor 112. Para habilitar la transferencia de paquetes entre el emisor nodo 102 y el nodo receptor 112, pueden utilizarse uno o más nodos intermedios 104, 106, 108, y/o 110. Se debe entender que cualquier nodo 102-112 puede ser un nodo emisor y/o un nodo receptor y puede realizar funciones envío o recepción de información sustancialmente al mismo tiempo (por ejemplo, puede transmitir o comunicar la información a aproximadamente el mismo tiempo que recibe información). También debe entenderse que cualquier nodo 102-112 también podría proporcionar acceso a otra infraestructura de comunicaciones, tal como una red cableada (no mostrado) y en algunos casos puede funcionar similar a un punto de acceso.

Periódicamente o en base a otros criterios, un nodo (denominado en este documento como nodo o dispositivo de envío) puede transmitir o anunciar su presencia a otros nodos dentro de su rango, lo que puede ser utilizado durante el descubrimiento de homólogos. Los nodos que reciben información de presencia (denominados de aquí en este documento como nodos o dispositivos receptores) son conscientes de la existencia del nodo de envío en base a la información recibida. Tales nodos pueden determinar la posibilidad de establecer la comunicación con el nodo de envío en base a la información recibida. Debe entenderse que, aunque los nodos dentro de una red de comunicación 100 podrían no ser capaces de distinguir a los otros nodos dentro de la red de comunicación (por ejemplo, conocer el usuario, el servicio, la función, el interés, etcétera, asociada con un nodo en particular), se conoce la presencia (o existencia) de los otros nodos. Por lo tanto, si hay se producen conversaciones, las conversaciones se pueden coordinar para tener en cuenta diversos factores, tal como la capacidad de ancho de banda, la mitigación de la interferencia y otros problemas.

La información anunciada durante el descubrimiento de homólogos puede incluir información relacionada con el usuario del nodo o dispositivo (por ejemplo, dispositivo de envío), una aplicación que se ejecuta en el nodo o dispositivo de envío, un servicio proporcionado por el nodo o dispositivo de envío, y así sucesivamente, y puede ser transmitido como un identificador público o privado. En diversas situaciones, el usuario de un dispositivo de envío

podría no desear que ciertos individuos (por ejemplo, usuarios de otros dispositivos de recepción) se den cuenta de su presencia (por ejemplo, para mantener un nivel de anonimato). En otras situaciones, los usuarios del dispositivo de envío pueden desear que otro individuo (por ejemplo, usuario del dispositivo receptor) esté al tanto de su presencia, pero sólo por un tiempo limitado. Por lo tanto, los nodos 102-112 pueden estar configurados para permitir explícitamente varios nodos de recepción para reconocer a un nodo de envío, en base al conocimiento de un primer identificador asociado con el nodo emisor y claves distribuidas selectivamente a los nodos receptores para permitir que dichos nodos deriven un segundo identificador (por ejemplo, saber cuándo sus compañeros, amigos, socios, etc. se encuentran dentro de un área geográfica similar) emitido por el nodo de envío en un momento particular. De acuerdo con algunos aspectos, el primer identificador es un identificador público y el segundo identificador es un identificador privado.

Una clave es una cadena de datos que, cuando se combina con datos de origen (por ejemplo, de acuerdo con un algoritmo) produce una salida que es ilegible hasta que ha sido descifrada. Las claves derivadas de la primera identificador pueden ser distribuidos con diversos periodos de caducidad (por ejemplo, un dispositivo en particular puede obtener la clave para un año, mientras que otro dispositivo puede obtener la clave de tan sólo tres meses). Adicional o alternativamente, las claves y/o algoritmos pueden incluir parámetros de localización, y otros parámetros (por ejemplo, un grupo pertenece el usuario, un juego el usuario desea participar en, un cierto tipo de persona que el usuario desea encontrarse y así sucesivamente), una combinación de parámetros puede ser utilizado. De acuerdo con algunos aspectos, las claves u otra información distribuida a uno o más dispositivos receptores pueden ser revocados en cualquier momento, incluso antes de que un rango de validez clave o período ha expirado.

Dado que los dispositivos o nodos se mueven por la red 100, los demás dispositivos o nodos deben utilizar una tecnología de comunicación similar. Cada dispositivo receptor puede obtener el conocimiento de los otros dispositivos (por ejemplo, dispositivos de envío) en la zona y los identificadores correspondientes asociados a cada dispositivo durante la búsqueda de homólogos. Sin embargo, un dispositivo receptor (y el usuario del dispositivo) no puede saber a quién pertenecen esos identificadores (por ejemplo, no puede distinguir un identificador de otro), ya que los identificadores anunciados o difundidos pueden ser identificadores privados, no identificadores conocidos públicamente. Sin embargo, a través de la utilización de los aspectos divulgados, cuando un usuario de un dispositivo de recepción está buscando el identificador de un compañero, el dispositivo del usuario (por ejemplo, el dispositivo receptor) puede saber específicamente qué identificador privado debería enviar el dispositivo homólogo (por ejemplo, dispositivo de envío) en base a derivar varias claves a partir de una combinación de un identificador público y una clave conocida distribuida.

Los identificadores privados pueden cambiar con el tiempo y pueden determinarse o derivarse de una jerarquía de claves previamente distribuida a un dispositivo receptor a lo largo de un determinado intervalo (por ejemplo, antes de que expire la clave distribuida). Tales cambios periódicos mitigan la probabilidad de que una persona pueda ser seguida o tenga problemas de seguridad. Por ejemplo, si un usuario pícaro sigue a alguien (por ejemplo, a un usuario inocente) por un tiempo (por ejemplo, un período de seguimiento), el usuario pícaro podría ser capaz de determinar un identificador privado asociado con el usuario inocente. Por ejemplo, el usuario pícaro puede revisar los identificadores recibidos durante el período de seguimiento y, si el mismo identificador está siempre presente mientras que otros identificadores varían, el usuario pícaro puede determinar qué identificador pertenece a un usuario inocente. Para mitigar este seguimiento, los identificadores pueden cambiar aleatoriamente en intervalos periódicos o predeterminados. Por lo tanto, el identificador puede estar cambiando a una frecuencia determinada y de forma aleatoria por lo que el seguimiento es más difícil.

Un dispositivo de envío también puede recibir una clave distribuida desde un dispositivo de recepción a fin de que el dispositivo de envío sea capaz de asociar un segundo identificador anunciado por el dispositivo receptor con un primer identificador. Un solo dispositivo puede realizar funciones tanto de envío de información de descubrimiento de homólogos como para recibir información de descubrimiento de homólogos de acuerdo con los diversos aspectos descritos en este documento.

Volviendo a La Figura 2, se ilustra un sistema 200 que genera y distribuye selectivamente información para facilitar el descubrimiento de homólogos. El sistema 200 se puede configurar para permitir que la presencia de los usuarios de dispositivos, aplicaciones y/o servicios se anuncie durante un intervalo especificado a otros usuarios seleccionados de dispositivos, aplicaciones y/o servicios, añadiendo así un nivel de seguridad. La presencia puede ser anunciada por el sistema 200 de manera que conserva la privacidad para el usuario cuya presencia se está anunciando a un grupo selecto de personas. Por ejemplo, un personaje conocido, como un actor, tal vez quiera pasar un día visitando varias zonas o tiendas y tal vez no queremos que todos en la misma zona conozcan su ubicación. El sistema 200 puede anunciar de forma selectiva su presencia a un círculo de amigos a través de la distribución selectiva de claves.

En más detalle, el sistema 200 incluye un nodo transmisor 202 que anuncia o difunde su presencia a un nodo receptor 204. Se debe entender que se pueden incluir más de un nodo transmisor 202 y un nodo receptor 204 en el sistema 200, sin embargo, se muestra y describe uno de cada uno por simplicidad. El nodo transmisor 202 puede anunciar o difundir información diversa incluyendo identificación, forma de utilizar los servicios del nodo transmisor 202 para comunicarse en una red ad hoc punto a punto y otra información.

De acuerdo con algunos aspectos, el nodo transmisor 202 puede realizar las funciones de nodo receptor 204 y el nodo receptor 204 puede realizar las funciones de nodo transmisor 202. Es decir, un único nodo puede transmitir y recibir información de acuerdo con los uno o más aspectos divulgados en esta descripción detallada. De tal manera, un nodo puede transmitiendo información y sustancialmente al mismo tiempo puede estar también recibiendo información desde otros nodos en la vecindad, así como realizando otras funciones (por ejemplo, comunicación, transmisión de información y así sucesivamente).

Cada nodo que participa en la red punto a punto puede tener un identificador relativamente permanente y conocido públicamente (por ejemplo, el primer identificador), tal como un identificador de acceso a la red (por ejemplo, john.doe@isp.com) o una dirección de Protocolo de Internet (IP). Este identificador permanente y conocido públicamente puede ser transformado en un identificador privado (por ejemplo, un segundo identificador) que se anuncia como parte del proceso de descubrimiento de homólogos para permitir al nodo de usuario retener un nivel de privacidad.

Para transmitir selectivamente información de presencia, el nodo transmisor 202 puede incluir un generador de claves 206 que crea una multitud de claves asociadas con un primer identificador. Al menos una de las claves está asociada con un período de validez, una región geográfica o combinaciones de los mismos. Por ejemplo, cada clave es válida de forma temporal y vencerá con una frecuencia o intervalo predeterminado (por ejemplo, minutos, horas, días, u otros intervalos, los cuales pueden o no estar basados en el tiempo). En algunos casos, una clave puede derivarse como una función de un hash de control de otra clave y alguna otra información (por ejemplo, información de tiempo, información de ubicación, información de grupo, información de juego, o combinaciones de los mismos). De acuerdo con algunos aspectos, la multitud de claves puede crear una jerarquía de claves, lo que se discutirá en mayor detalle a continuación.

El nodo transmisor 202 también incluye un comunicador 208 que transmite el primer identificador y por lo menos una de las claves de la multitud de claves a un primer nodo homólogo. El primer nodo homólogo es un nodo que debe recibir información para permitir la detección de la presencia (por ejemplo, recibir una clave distribuida). El primer identificador y las claves se pueden comunicar de forma segura. De acuerdo con algunos aspectos, el comunicador 208 transmite el primer identificador y al menos una segunda clave (diferente de la al menos una clave de transmisión a la primera nodo homólogo) a un segundo nodo homólogo.

Por ejemplo, para un miembro de la familia, podría desearse monitorización continua (por ejemplo, un año). Sin embargo, para los compañeros en el trabajo, podría ser deseable permitir la monitorización sólo durante un mes. Para algunos individuos (por ejemplo, cita a ciegas) podría desearse un intervalo más corto (por ejemplo, de 6 horas). Por lo tanto, pueden distribuirse diferentes claves a los diferentes pares o nodos en base a una duración deseada.

Se debe entender que las claves se pueden distribuir utilizando una variedad de técnicas conocidas, algunas de las cuales pueden ser efectivamente fuera de banda (por ejemplo, transmitido mediante intercambio físico de medios grabados o mediante una combinación de comunicación verbal y configuración manual). Por ejemplo, una persona famosa puede estar caminando por ahí con su dispositivo, pero no quiere anunciar de forma continua que está en las cercanías. Sin embargo, ella quiere que algunos amigos de confianza sean capaces de detectar su presencia. Cada amigo seleccionado puede recibir una clave que permite a sus respectivos dispositivos derivar un segundo identificador que la persona famosa está anunciando en base al conocimiento de su primer identificador y la clave distribuidos.

La determinación de qué dispositivos o nodos deben distribuir una clave se puede hacer en base a una entrada manual (por ejemplo, selección de uno o varios contactos de una lista) o puede basarse en otros factores (por ejemplo, un nodo con el que nodo transmisor 202 se comunica actualmente). La determinación de qué clave debe ser distribuida a un nodo o a un homólogo en particular en base a un intervalo predeterminado, por lo que una vez transcurrido el intervalo, los nodos seleccionados ya no son capaces de obtener el identificador privado.

Un segundo identificador es derivado por un módulo de creación de identificadores 210. El segundo identificador se deriva como una función del primer identificador y el uno o más claves. De acuerdo con algunos aspectos, el segundo identificador se deriva como una función del primer identificador y por lo menos dos claves de la pluralidad de claves.

El segundo identificador se transmite a una multitud de nodos homólogos por un anunciante 212. El segundo identificador puede transmitirse a efectos de descubrimiento de homólogos. Anunciar el segundo identificador puede comprender una transmisión inalámbrica que incluye el segundo identificador. De acuerdo con algunos aspectos, el primer identificador es un identificador público y el segundo identificador es un identificador privado.

De acuerdo con algunos aspectos, los identificadores posteriores (por ejemplo, el tercer identificador, el cuarto identificador, y así sucesivamente) son derivados por el módulo de creación de identificadores 210 en base a una clave que es diferente de la clave utilizada para un identificador anterior (por ejemplo, un segundo identificador). La

clave diferente puede corresponder a diferentes intervalos de tiempo y/o regiones geográficas que la clave utilizada para uno o más identificadores anteriores. Por ejemplo, un identificador anterior necesita ser cambiado, ya que se ha visto comprometido, un intervalo de tiempo asociado con el identificador ha expirado o por otras razones. De acuerdo con algunos aspectos, una clave utilizada para derivar la anterior y los identificadores posteriores se basa en una clave superior en una jerarquía (por ejemplo, una clave de primera semana y una clave de segunda semana se derivan ambas de la misma clave de mes). El anunciante 212 puede transmitir el(los) identificador(es) subsiguiente(s) que son creados por el módulo de creación de identificadores 210. De acuerdo con algunos aspectos, la(s) clave(s) anterior(es) puede(n) ser invalidada(s) después de la creación de una clave subsiguiente.

De acuerdo con algunos aspectos, el nodo transmisor 202 puede utilizar varios algoritmos, procedimientos y/o técnicas para crear el segundo (y posterior(es)) identificador que se anuncia (por ejemplo, es difundido), para permitir el descubrimiento de homólogos. Por ejemplo, el nodo transmisor 202 puede crear el segundo (y posterior(es)) identificador en base a un hash seguro del primer identificador y una clave de seguridad (por ejemplo, donde la clave de seguridad ha sido transmitida previamente a homólogos explícitamente relacionados (o anterior)) o en base a otras técnicas de cifrado. De acuerdo con algunos aspectos, el nodo transmisor 202 puede cambiar las claves periódicamente o en base a un intervalo predeterminado.

Uno o más claves pueden ser asignadas a diferentes pares sustancialmente al mismo tiempo, incluso si tales pares tienen diferentes duraciones durante las que tienen acceso al identificador personal. Por ejemplo, un nodo transmisor 202 se mueve de un área o zona geográfica a otra área geográfica. En sustancialmente al mismo tiempo como entrar en una nueva área geográfica y/o periódicamente, el nodo transmisor 202 anunciar su presencia mediante la transmisión de un segundo identificador asociado con el nodo transmisor 202. El segundo identificador puede ser recibido por uno o más nodos 204 dentro del alcance del nodo transmisor receptor 202. Algunos de los nodos 204 receptor no saben (o no pueden determinar) el segundo identificador e ignoran la información o no conocen la identidad del dispositivo. Otros nodos receptores 204 pueden tener información relacionada con el segundo identificador (en base al conocimiento del primer identificador y de la clave distribuida) y, si se desea, pueden establecerse comunicaciones entre el nodo transmisor 202 y el nodo receptor 204.

De acuerdo con algún aspecto, las claves distribuidas pueden ser revocadas selectivamente antes de la expiración de un rango de validez asociado a la clave distribuida. El rango de validez debe tener un punto de partida y un punto final. Pueden utilizarse una multitud de medios para establecer el rango de validez y no se limita a una duración de tiempo, a pesar de que es fácil pensar en un rango de validez en términos de tiempo. Por lo tanto, no es necesario que el rango de validez se relacione con el tiempo real, aunque puede ser. El rango de validez podría ser una secuencia numerada o un rango que es generado por una función hash. El rango de validez puede ser basado en tiempo, basado en números o en base a otros criterios o combinaciones de los mismos, siempre que haya un sistema, procedimiento u otros medios para determinar cuándo el rango de validez comienza y termina.

Una memoria 214 puede estar acoplada operativamente al nodo transmisor 202 para codificar y distribuir las claves asociadas con un segundo identificador. La memoria 214 puede almacenar información y/o retener las instrucciones relacionadas con la generación de una multitud de claves asociadas con un primer identificador y comunicar el primer identificador y por lo menos una de las claves de la multitud de claves a un primer nodo homólogo. La memoria también puede guardar las instrucciones relacionadas con derivar un segundo identificador como una función del primer identificador y por lo menos una clave de la pluralidad de claves y anunciar el segundo identificador a una pluralidad de nodos homólogos.

Un procesador 216 puede estar conectado operativamente al nodo transmisor 202 y/o a la memoria 214 para facilitar el análisis de la información recibida y/o se puede configurar para ejecutar las instrucciones retenidas en la memoria 214. El procesador 216 puede ser un procesador dedicado a analizar la información recibida desde el nodo transmisor 202 y/o para generar información que pueda ser utilizada por los componentes del nodo transmisor 202. Adicional o alternativamente, el procesador 216 puede ser un procesador que controla uno o más componentes de sistema 200 y/o un procesador que analiza la información, genera información y/o controla uno o más componentes del sistema 200.

Con referencia ahora a La Figura 3, se ilustra un sistema de ejemplo 300 que recibe una clave criptográfica y realiza el descubrimiento de homólogos en base en parte al uso de la clave para determinar una asociación entre un primer identificador y un segundo identificador correspondiente (o posterior) utilizado para el descubrimiento de homólogos. El sistema 300 se puede configurar para descubrir uno o más de sus homólogos durante un período de descubrimiento de homólogos y establecer selectivamente comunicaciones con los uno o más de sus homólogos. Una jerarquía de claves puede estar asociada con un primer identificador conocido con el fin de determinar un segundo identificador (y posterior(es)) para ser utilizado con el propósito de descubrimiento de homólogos. La jerarquía de las claves puede relacionarse con duraciones predeterminadas o intervalos durante los que una clave criptográfica es válida. Una de las claves dentro de la jerarquía puede ser válida debido a una expiración de un intervalo. Un homólogo que tiene una clave que está más alta en la jerarquía (por ejemplo, tiene una duración más larga) puede derivar cada clave debajo de él en la jerarquía (por ejemplo, donde cada una de dichas claves corresponde a un subconjunto del período de tiempo asociado con la clave más alta de la que se deriva).

En más detalle, el sistema 300 incluye un nodo transmisor 302 que puede comunicarse con un nodo receptor 304, tal como en una red de tipo punto a punto ad hoc. Puede haber más de uno de cada nodo 302, 304, sin embargo, sólo uno de cada uno se muestra por simplicidad. Los nodos 302, 304 pueden llegar a ser conscientes de otros nodos dentro de una región geográfica durante un período de descubrimiento de homólogos durante el cual los nodos 302, 304 anuncian información relativa a los respectivos identificadores y otra información que permite a los nodos 302, 304 comunicarse. Los nodos 302, 304 pueden asignar claves que tienen diferentes rangos de validez. Por ejemplo, el nodo transmisor 302 puede dar al nodo receptor 304 una clave durante tres horas, pero el nodo receptor 304 puede dar al nodo transmisor una clave para una sola hora.

Con el fin de mantener la privacidad de un usuario de un nodo transmisor 302 (o nodo receptor 304), un segundo identificador puede estar asociado con el transmisor 302 de nodo en base a un primer identificador. Por ejemplo, un usuario podría ser conocido por un primer identificador (por ejemplo, joe.smith@work.com), que en un momento dado está asociado con un segundo identificador en particular (por ejemplo, un valor hexadecimal pseudoaleatorio 0xA65D820C). A medida que el usuario se desplaza de un lugar a otro, puede haber un nivel de privacidad deseado por lo que no todo el mundo en la misma zona que utiliza la red ad hoc es consciente o notificado de la presencia del usuario. De acuerdo con algunos aspectos, el usuario podría desear que ciertos individuos obtengan información de presencia de un intervalo o rango de validez limitado. Pueden utilizarse múltiples medios para establecer el rango de validez y no se limita a una duración de tiempo, a pesar de que es fácil pensar en un rango de validez en términos de tiempo.

Un usuario del nodo transmisor 302 puede seleccionar otros nodos 304 que pueden recibir claves asociadas con el primer identificador, así como un rango de validez durante el cual se pueden utilizar las claves para determinar una asociación entre el primer identificador y un segundo identificador correspondiente (o identificadores posteriores) que se utiliza para descubrimiento de homólogos, permitiendo así que otros nodos 304 detecten la presencia de la entidad asociada con el primer identificador de nodo y el transmisor 302. El nodo receptor 304 puede recibir claves asociadas con el identificador cuando se transmite en una red punto a punto, que incluye tanto el nodo transmisor 302 como el nodo receptor 304. De acuerdo con algunos aspectos, el nodo receptor 304 puede recibir las claves a través de una red de infraestructura (por ejemplo, una red que utiliza estaciones base) o a través de otros medios (por ejemplo, a través de intercambio físico de medios grabados o a través de una combinación de comunicación verbal y configuración manual).

Pueden utilizarse una multitud de técnicas para distribuir las claves, tales como un cambio de clave privada-pública, un intercambio de claves Diffie-Hellman (DH) u otras formas de intercambio de claves de una manera segura. De acuerdo con algunos aspectos, puede determinarse el segundo identificador (o posterior) en base a una control seguro del primer identificador (o anterior) y una clave de seguridad (por ejemplo, la clave de seguridad ha sido transmitida anteriormente o una clave de seguridad derivada al menos en parte a partir de una clave de seguridad que ha sido transmitida previamente).

Los aspectos relacionados con claves asociadas con determinar una asociación entre un primer (o anterior) identificador y un segundo identificador correspondiente (o posterior) se ilustran en la Figura 4, que representa las claves de seguridad 400 con diferentes períodos de usabilidad. Las claves de seguridad 400 pueden ser utilizadas para apoyar las relaciones entre homólogos de diferentes duraciones. Se debe entender que las claves de seguridad 400 ilustran a modo de ejemplo sólo las claves de seguridad y de otro tipo que pueden ser utilizadas. Por lo tanto, mientras que las claves de seguridad 400 que se muestran y describen se refieren a periodos basados en tiempo por simplicidad, los aspectos divulgados no se limitan a las duraciones de tiempo. Por ejemplo, un rango asociado con las claves de seguridad 400 puede ser basado en tiempo, basado en ubicación, basado en números o en base a otros criterios, cumpliendo con un sistema, procedimiento u otros medios para determinar cuándo comienza y termina el rango de validez.

En un momento dado y/o durante un intervalo de tiempo dado, un identificador permanente 402 puede estar asociado con un identificador temporal 404. El identificador temporal 404, correspondiente al identificador permanente 402, puede cambiar con el tiempo, por lo tanto, el identificador temporal puede describirse como temporal o transitorio, en comparación con el identificador relativamente permanente. Para efectos de este ejemplo, duraciones de tiempo de horas, días, semanas y meses. Sin embargo, tal y como se indicó anteriormente pueden utilizarse otros criterios anteriormente indicados para establecer períodos de validez. Puede determinarse el identificador temporal 404 mediante la ejecución de una operación de hash seguro 406 en el identificador permanente 402 con una clave que sólo es válida para la hora actual 408. La clave de hora 408 se puede transmitir a un homólogo que sólo debe ser capaz de realizar la detección durante una hora.

La clave de hora 408 se puede determinar mediante la ejecución de una operación de hash seguro 410 en alguna información de día 412 (por ejemplo, información pseudoaleatoria correspondiente al día), con una clave que es válida para durante día 414. Cabe señalar que la operación en la información de día 412 con la clave de día 414 podría producir un conjunto de claves de hora (por ejemplo, una clave para cada hora del día). Un homólogo al que se le ha transmitido la clave de día 414 puede determinar la clave de hora 408 para cada hora del día y, por lo tanto, el identificador temporal 404 que se utiliza para el descubrimiento de homólogos durante cada hora del día.

De una manera similar, la clave de día 414 se puede determinar mediante la ejecución de una operación de hash seguro 416 en alguna información de semana 418 (por ejemplo, información pseudoaleatoria correspondiente a la semana) con una clave que es válida para la semana 420. Algunos homólogos pueden dar la clave de semana 420 que permite determinar los identificadores temporales utilizados durante la semana. De una manera similar, la clave de semana 420 puede determinarse mediante la realización de una operación de hash seguro 422 en alguna información de mes 424 (por ejemplo, información pseudoaleatoria correspondiente al mes) con una clave que es válida durante el mes 426. Algunos homólogos pueden proporcionar la clave de mes 426 que permite determinar los identificadores temporales utilizados durante todo el mes. Cabe señalar que la operación en la información de semana 418 con la clave de semana 420 podría producir un conjunto de claves de día (por ejemplo, una clave para cada día de la semana). Adicionalmente, la operación en la información de mes 424 con la clave de mes 426 podría producir un conjunto de claves de semana (por ejemplo, una clave para cada semana del mes). En cada caso en que se utiliza un hash seguro para derivar una clave (o un conjunto de claves) de otra clave, es posible una variedad de técnicas alternativas para la derivación de la clave. Por otra parte, el proceso de derivación de claves puede incorporar información adicional o alternativa en el cálculo.

Un homólogo al que se le da la clave de mes 426 puede determinar cada clave inferior en la jerarquía para derivar una clave temporal actual utilizada para determinar una asociación entre el identificador permanente y un identificador temporal. Un homólogo que conoce la clave de semana 420 puede derivar las respectivas claves de día y claves de horas, que están más abajo en la jerarquía. De una manera similar, un homólogo con la clave de día 414 puede derivar las claves de hora respectivas para los períodos de validez de días. Por lo tanto, el conocimiento de una clave dentro de una jerarquía puede suministrar información necesaria para derivar claves inferiores en la jerarquía.

Las claves no se pueden utilizar para derivar claves más altas en la jerarquía. Por lo tanto, un homólogo con la clave de semana 420 no puede derivar la clave de mes 426; un par con la clave de día 414 no puede derivar la clave de semana 420 o la clave de mes 426 y un homólogo que conoce la clave de hora 408 no puede determinar las claves 414, 420, 426 durante un período de validez más largo. Por lo tanto, como el rango extremo asociado con una duración de una clave suministrada expira, un homólogo deseando establecer una comunicación de punto a punto con el usuario asociado con claves distribuidas necesita tener las claves asignadas explícitamente en conformidad con los aspectos divulgados. De tal manera, el identificador temporal puede ser transmitido de forma explícita a los homólogos relacionados y son válidos durante un tiempo limitado. De acuerdo con algunos aspectos, las claves se pueden revocar implícitamente antes de la expiración del rango de validez.

Haciendo referencia de nuevo a La Figura 3, con el fin de aceptar una o más claves y los rangos de validez asociados, en su caso, el nodo receptor 304 puede incluir un obtentor 306 que puede recibir un primer identificador y al menos una clave asociada con un nodo homólogo. La clave recibida puede estar asociada con un rango de validez que indica un período de validez que tiene un punto de partida y un punto final.

También se incluye un identificador 308 que puede determinar un segundo identificador de base, al menos en parte, en el primer identificador y la al menos una clave. El segundo identificador puede determinarse en base a tiempo parcial, en parte de la ubicación, o combinaciones de los mismos. De acuerdo con algunos aspectos, determinar el segundo identificador incluye la generación de al menos una clave adicional. La clave adicional puede estar asociada con un período de validez específica, la región geográfica o combinaciones de los mismos. De acuerdo con algunos aspectos, la clave adicional forma una jerarquía.

Un módulo de observación 310 puede monitorizar la recepción del segundo identificador. De acuerdo con algunos aspectos, monitorizar la recepción del segundo identificador incluye recibir un identificador anunciado por un nodo cercano y determinar si el identificador recibido es el segundo identificador (por ejemplo, es el nodo cerca del homólogo correspondiente). De acuerdo con algunos aspectos, el monitorizar la recepción incluye recibir una transmisión inalámbrica.

Debe entenderse que, dependiendo del mecanismo específico de seguridad en uso y/u otros factores, el nodo receptor 304 puede o bien utilizar un primer identificador de un homólogo junto con una clave asociada para determinar el segundo identificador que se utilizará para descubrimiento de homólogos y, por lo tanto, monitorizar transmisiones de descubrimiento de homólogos para el segundo identificador, o usar un segundo identificador recibido a través de una transmisión de descubrimiento de homólogos junto con una clave asociada con el primer identificador de un homólogo para determinar si un identificador recibido se corresponde con el primer identificador.

De acuerdo con algunos aspectos, si debe cambiarse el segundo identificador debe debido a diversas razones (por ejemplo, el segundo identificador se ha visto comprometido), se puede derivar un tercer identificador. El tercer identificador (o posterior) puede estar relacionado con el segundo identificador (o anterior), pero se basa en una clave diferente (por ejemplo, el tercer identificador y la clave corresponde a un intervalo de tiempo diferente y/o región geográfica). El interruptor de relevo de la segunda clave a la tercera clave puede estar basado en el conocimiento de una clave que está más alta en la jerarquía. Por ejemplo, la segunda clave es una clave para la primera semana y una tercera clave es una clave para la segunda semana. Tanto la segunda clave y la tercera clave se derivan de una clave de mes, que es conocida por el nodo receptor 304, el cual puede derivar las claves de nivel

inferior (por ejemplo, la segunda clave y la tercera clave).

Una memoria 312 puede estar acoplada operativamente al nodo receptor 304 para decodificar un segundo identificador asociado con el modo de transmisor. La memoria 312 puede almacenar la información y/o retener las instrucciones relacionadas con recibir un primer identificador y al menos una clave asociada con un nodo homólogo, determinar un segundo identificador en base a, al menos en parte, el primer identificador y por lo menos una de las claves, y monitorizar recepción del segundo identificador. Memoria 312 pueden retener además instrucciones relacionadas con la información de retención asociado con una clave criptográfica. Memoria 312 pueden retener más instrucciones relacionadas con recibir información con respecto a la presencia de un nodo homólogo cuando está en un cierto rango geográfico (por ejemplo, un nodo homólogo y un nodo receptor se encuentran dentro del alcance del otro).

Un procesador 314 puede estar conectado operativamente al nodo receptor 304 y/o a la memoria 312 para facilitar el análisis de la información recibida y/o puede configurarse para ejecutar las instrucciones almacenadas en la memoria 312. El procesador 314 puede ser un procesador dedicado a analizar la información recibida desde el nodo transmisor 302 y/o a generar información que puede ser utilizada por el obtentor 306, el identificador 308 y/o el verificador 310. Adicional o alternativamente, el procesador 314 puede ser un procesador que controla uno o más componentes del sistema 300 y/o un procesador que analiza la información, genera información y/o controla uno o más componentes de sistema 300.

A efectos de ejemplo y no de limitación, los usuarios pueden embarcarse en un crucero y durante el crucero los distintos individuos de la nave tal vez no tengan acceso a una infraestructura (por ejemplo, a una estación base) ya que están en el mar, lejos de la tierra. Sin embargo, pueden tener acceso a una red punto a punto que puede tener una estructura de costes asociada u otros medios de control de la comunicación. Por ejemplo, los usuarios pueden inscribirse durante cinco días y durante esos cinco días las personas identificadas (por ejemplo, en el crucero) puede comunicarse con ellos. Los diferentes usuarios pueden no querer que otras personas en el crucero se comuniquen con ellos y/o puedan seguirlos. Por lo tanto, pueden distribuirse las claves temporales a los individuos seleccionados que permiten a los individuos para determinar la asociación entre el identificador público y un identificador privado correspondiente utilizado con el propósito de descubrimiento de homólogos. De esta manera, los individuos seleccionados pueden detectar la presencia al tiempo que evita que otros lo hagan.

Con referencia ahora a la Figura 5, se ilustra un ejemplo 500 para derivar una clave de menor nivel basada en una clave de nivel superior y una información conocida. Un dispositivo o nodo puede obtener una clave en un cierto nivel en una jerarquía (por ejemplo, una clave de hora es superior en una jerarquía a una clave de minuto; una clave de año está más alta en una jerarquía que una clave de día). En algunos casos, con el fin de derivar claves de nivel inferior, en su caso, se necesita información adicional, que puede ser basada en el tiempo, basada en la localización, basada en otros criterios , o en combinaciones de los mismos. Un dispositivo puede dar una clave, como la clave A 502, que para este ejemplo es una clave correspondiente a una semana particular. A partir de la Clave A 502, el dispositivo puede incluir alguna información de semana 504, que puede determinarse a partir de un calendario u otras fuentes de temporización. La clave A 502 y la información de semana 504 se procesan a través de una conexión segura (por ejemplo, de un solo sentido) de algoritmo hash 506 (aunque otras técnicas pueden ser utilizadas), que producen una salida 508. La salida 508 se puede dividir en secciones o sub-partes, que puede ser una función de la clave A 502 y la información de semana504. Por ejemplo, una primera parte puede ser una clave de domingo 510, una segunda porción puede ser una clave de lunes 512, una tercera porción puede ser una clave de martes514, y así sucesivamente. Cada una de las claves de sub-parte se puede utilizar para proporcionar el siguiente grupo de claves (por ejemplo, horas, minutos y segundos) utilizando un proceso similar.

La Figura 6 ilustra un ejemplo 600 de derivar una o más claves de nivel inferior en base a una clave de nivel más alto y dos piezas distintas de información conocidas. Para este ejemplo 600, el tiempo y el lugar son utilizados para obtener las claves de nivel inferior. Por ejemplo, un usuario puede viajar entre dos o más lugares con frecuencia, por ejemplo, entre América del Norte y Europa. Un identificador puede derivarse no sólo en función del tiempo, sino también de la ubicación. Por lo tanto, si el usuario está en Europa se utiliza una primera clave, sin embargo, si el usuario está en América del Norte, se utiliza una clave diferente.

Al igual que en el ejemplo anterior, a un dispositivo se le puede dar una clave, como la clave B 602, que para este ejemplo es una clave basada en una semana y una ubicación. A partir de la clave B 602, el dispositivo puede incluir alguna información de semana 604 y alguna información de ubicación 606 que puede ser comprobada a través de diversos medios o combinaciones de diversos medios (por ejemplo, calendario, sistema de posicionamiento global, otros medios de localización, configuración manual y así sucesivamente). La clave B 602 y la combinación de la información de semana 604 y la información de de ubicación 606 se pueden procesar con un algoritmo hash seguro 608 (por ejemplo, de un solo sentido) (u otros medios), que puede producir una salida 610. La clave que se utiliza un dispositivo en un momento dado es una función tanto de ubicación como del tiempo, para este ejemplo. Si es martes 612 y los dispositivos (tanto el transmisor como el receptor) se encuentran en una primera ubicación 614, se debe utilizar una primera clave para determinar un identificador temporal. Sin embargo, si es martes 612 y los dispositivos se encuentran en una segunda ubicación 616, se debe utilizar una segunda clave para determinar un identificador temporal.

Un receptor debe ser capaz de reconstruir, generar o derivar las claves de una manera similar a la del transmisor utilizando una de las claves para calcular un identificador temporal para anunciarse para el descubrimiento de homólogos. Por lo tanto, un dispositivo debe ser consciente de que el usuario está buscando un Colega "X" y tiene claves del Colega X teniendo en cuenta donde se encuentra el dispositivo y la hora del día para determinar el identificador privado que el Colega X debe estar utilizando en ese tiempo en esa zona. Si el Colega X se encuentra en las cercanías, el identificador temporal determinado es el identificador que el Colega X debería estar utilizando.

Se debe entender que, si bien los diversos ejemplos se ilustran y describen con referencia al tiempo y/o ubicación, podrían utilizarse otros factores. Por ejemplo, el tipo de clave (por ejemplo, asimétrica, simétrica), el tiempo que la clave es válida, un juego en el que el usuario desea participar/hacer que otro participe (por ejemplo, la búsqueda de tales usuarios), un grupo que pertenece el usuario, así como otros factores que pueden ser utilizados para permitir selectivamente el descubrimiento de un homólogo, al tiempo que se mantienen los aspectos de confidencialidad.

Haciendo referencia a la Figs. 7-8, se ilustran las metodologías relacionadas con el descubrimiento de homólogos. Mientras que, por simplicidad de la explicación, las metodologías se muestran y describen como una serie de actos, ha de entenderse y apreciarse que las metodologías no están limitadas por el orden de los actos, ya que algunos actos, de conformidad con uno o más aspectos, se producen en diferentes órdenes y/o concurrentemente con otros actos de los que se muestran y describen en este documento. Por ejemplo, los expertos en la técnica entenderán y apreciarán que una metodología podría representarse alternativamente como una serie de estados o eventos, tales como un diagrama de estados interrelacionados. Por otra parte, puede no ser obligado poner en práctica todos los actos ilustrados en una metodología de acuerdo con uno o más aspectos.

Volviendo ahora a la Figura 7, se ilustra un procedimiento 700 para la transmisión de información de detección de homólogos. El procedimiento 700 puede facilitar el mantenimiento de un nivel de confidencialidad o el anonimato en una red de comunicaciones (por ejemplo, red de tipo punto a punto ad hoc) mediante la mitigación de la emisión de un primer identificador asociado con un usuario del dispositivo. El procedimiento 700 permite a los homólogos identificados expresamente derivar un segundo identificador mediante la distribución de una clave criptográfica a tales homólogos. Las claves distribuidas pueden estar asociadas con un rango de validez (por ejemplo, se da una clave de hora a un homólogo que debe ser capaz de descifrar el segundo identificador durante una hora, y así sucesivamente).

El procedimiento 700 se inicia en 702 con la creación de una multitud de claves asociadas con un primer identificador. De acuerdo con algunos aspectos, el primer identificador es un identificador público que se puede elegir, asignar, y/o crear. Al menos una de las claves de la multitud de claves puede estar asociada con un intervalo de tiempo particular (por ejemplo, un período de validez), una zona o región en particular (por ejemplo, una región geográfica), o combinaciones de los mismos.

De acuerdo con algunos aspectos, la multitud de claves también forma una jerarquía (por ejemplo, en el tiempo o en el espacio). La jerarquía puede disponerse de forma que las claves de alto nivel tienen una duración más larga y las claves de bajo nivel tienen una duración más corta. Cada clave incluida en la multitud de claves puede ser válida con carácter temporal y vencerá con una frecuencia predeterminada. De acuerdo con algunos aspectos, una o más claves pueden ser revocadas en cualquier momento. La duración puede ser basada en tiempo, basada en números o combinaciones de los mismos. De acuerdo con algunos aspectos, las claves se pueden derivar en base a un control seguro del identificador público y a la información en relación con el tiempo, ubicación o combinaciones de los mismos.

De acuerdo con algunos aspectos, una expiración opcional puede estar asociada con uno o más claves. La expiración puede ser un período de validación que tiene un punto de partida y un punto final, mediante el cual, después del punto final, la clave particular ya no es válida. El período de validación puede ser basado en tiempo, basado en números o combinaciones de los mismos.

Un receptor de una clave distribuida puede derivar claves que son de niveles inferiores en la jerarquía. Sin embargo, las claves de nivel superior no se pueden derivar de una clave de nivel inferior, de tal modo mitigando las posibilidades de eludir la terminación de una clave en base a la caducidad de la clave. Derivar claves inferiores en la jerarquía puede ser utilizado para determinar un segundo identificador que un dispositivo asociado con las claves está transmitiendo.

En 704, el primer identificador y por lo menos una de las claves de la multitud de claves se comunican a un primer nodo homólogo. La al menos una clave puede ser transportada o distribuida de una manera segura. El primer nodo homólogo es un nodo que se pretende que sea capaz de descubrir el nodo comunicando el primer identificador y la al menos una clave. De acuerdo con algunos aspectos, el primer nodo homólogo es uno de un conjunto seleccionado de homólogos al que el primer identificador y por lo menos una de las claves han sido distribuidos o transmitidos.

De acuerdo con algunos aspectos, el par puede ser identificado de forma explícita, tal como a través de un

identificador público de los homólogos, una selección de una lista de contactos, un alias de correo electrónico u otra información que identifica el dispositivo al que se debe permitir el acceso. Las relaciones con los homólogos podrían no tener duraciones de tiempo equivalentes, por lo que es conveniente establecer las limitaciones y/o controles de tiempo durante un periodo de tiempo durante el cual los homólogos explícitamente relacionados pueden descubrirse entre ellos. Por lo tanto, la indicación del homólogo puede incluir una duración durante el cual el homólogo puede tener acceso a las claves necesarias para descifrar un identificador público a partir de un identificador privado (por ejemplo, saber cuándo un dispositivo de usuario determinado está en los alrededores).

En 706 se deriva un segundo identificador como una función del primer identificador y la al menos una clave. La al menos una clave puede considerarse válida por un determinado período de tiempo, en un lugar o región en particular (por ejemplo, región geográfica) o combinaciones de los mismos. De acuerdo con algunos aspectos, el segundo identificador puede ser derivado usando dos o más claves de la multitud de claves. De acuerdo con algunos aspectos, el segundo identificador es un identificador privado.

En 708, el segundo identificador se anuncia a una multitud de nodos homólogos. Anunciar puede incluir transmisión inalámbrica, transmisión de difusión o por lo menos una transmisión de unidifusión del segundo identificador. De acuerdo con algunos aspectos, anunciar incluye transmitir repetidamente el segundo identificador, que puede ser de transmisión periódica.

De acuerdo con algunos aspectos, el procedimiento también puede comunicar el primer identificador y al menos una segunda clave (diferente de la primera clave) de la multitud de claves o un conjunto diferente de claves a un segundo nodo homólogo.

Adicional o alternativamente, puede generarse un tercer identificador (o posterior) como una función del primer identificador y al menos una segunda clave de la pluralidad de claves y el segundo (o anterior) identificador puede ser invalidado. Por ejemplo, si el identificador anterior se ve comprometido o ha expirado, se puede generar la clave subsiguiente. De acuerdo con algunos aspectos, los identificadores anteriores y posteriores se derivan tanto como una función de una clave que está más alta en una jerarquía de claves.

Con referencia a La Figura 8, se ilustra un procedimiento 800 para recibir información sobre el descubrimiento de homólogos. El procedimiento 800 facilita la identificación de un grupo relacionado dentro de un entorno inalámbrico incluso aunque los homólogos relacionados anuncien su presencia utilizando un identificador temporal.

En 802, se reciben un primer identificador y al menos una clave asociada con un nodo homólogo. El nodo homólogo es un nodo destinado a ser detectable por el nodo que recibe el primer identificador y la clave. Por lo tanto, el primer identificador y al menos una de las claves pueden recibirse de un homólogo que identifica explícitamente uno o varios contactos que permiten obtener la información de presencia de homólogos. De acuerdo con algunos aspectos, el primer identificador es un identificador público.

En 804, se determina un segundo identificador en base, en parte, al primer identificador y la al menos una clave. De acuerdo con algunos aspectos, el segundo identificador se calcula o determina en base en parte al tiempo, en parte a la ubicación o combinaciones de los mismos. De acuerdo con algunos aspectos, el cálculo del segundo identificador incluye generar al menos una clave adicional. La al menos una clave adicional puede estar asociada con un intervalo de tiempo en particular, un lugar o región en particular (por ejemplo, región geográfica) o combinaciones de los mismos.

De acuerdo con algunos aspectos, la al menos una clave adicional forma una jerarquía (por ejemplo, en el tiempo o en el espacio). En un ejemplo, las claves de orden jerárquico que tienen una duración más corta se consideran claves de nivel inferior y las claves que tienen una duración más larga se consideran claves de nivel superior. De acuerdo con algunos aspectos, determinar el segundo identificador puede hacerse descifrando claves de nivel inferior en la jerarquía. La determinación puede hacerse en base a varios criterios, incluyendo el tiempo, la ubicación, los intereses, los grupos sociales o combinaciones de los mismos. Descifrar las claves de nivel inferior debe realizarse sustancialmente de la misma manera que se utilizó para cifrar las claves, mitigando por lo tanto las posibilidades de encontrar una clave actual incorrecta (por ejemplo, información no relacionada con un homólogo).

En 806, se monitoriza la recepción del segundo identificador (por ejemplo, para el descubrimiento de homólogos). De acuerdo con algunos aspectos, monitorizar puede incluir recibir transmisiones inalámbricas, recibir transmisiones de difusión, recibir al menos una transmisión de unidifusión o combinaciones de los mismos. De acuerdo con algunos aspectos, el control de recepción del segundo identificador puede incluir recibir un identificador anunciado por un nodo cercano y determinar si el identificador recibido es el segundo identificador determinado. Por lo tanto, si el homólogo relacionado está dentro de una gama geográfica específica (por ejemplo, dentro de la red punto a punto), puede detectarse la presencia de homólogos en base al segundo identificador que se está emitiendo.

De acuerdo con algunos aspectos, el procedimiento también incluye invalidar un segundo identificador. La invalidación se puede basar en la notificación de que el segundo identificador ya no es válido, en la expiración o vencimiento anticipado del segundo identificador o en otros factores (por ejemplo, el identificador se ha visto

comprometido). El procedimiento continúa mediante la derivación de un tercer identificador como una función del primer identificador y al menos una segunda clave de la pluralidad de claves.

Se apreciará que, de acuerdo con uno o más aspectos descritos en este documento, se pueden hacer inferencias respecto a la transmisión y/o recepción de identificadores. Tal y como se usa en este documento, los términos "inferir" o "inferencia" se refieren generalmente al proceso de razonamiento o inferencia de estados del sistema, al entorno y/o usuario a partir de un conjunto de observaciones capturados a través de eventos y/o datos. La inferencia puede emplearse para identificar un contexto o una acción específicos, o puede generar una distribución de probabilidad sobre los estados, por ejemplo. La inferencia puede ser, el cálculo de una distribución de probabilidad sobre estados de interés en base a una consideración de los datos y eventos. La inferencia también puede referirse a técnicas probabilísticas empleadas para la composición de eventos de mayor nivel a partir de un conjunto de eventos y/o datos. Esta inferencia resulta en la construcción de nuevos eventos o acciones de un conjunto de eventos observados y/o datos de eventos almacenados, incluso los eventos están correlacionados en estrecha proximidad temporal, y si los hechos y los datos provienen de una o varias fuentes de eventos y datos.

Según un ejemplo, uno o más aspectos presentados anteriormente pueden incluir hacer inferencias relativas a la creación de claves dispuestas en una jerarquía. De acuerdo con otro ejemplo, una inferencia se puede hacer en relación con derivar una clave de nivel más bajo en una jerarquía en base a una clave de nivel más alto. De acuerdo con otro ejemplo, una inferencia se puede hacer en relación con derivar uno o más segundos identificadores a partir de uno o más primeros identificadores. Se apreciará que los ejemplos anteriores son de naturaleza ilustrativa y no están destinados a limitar el número de inferencias que pueden hacerse o la manera en que tales inferencias se hacen en conjunto con los diversos ejemplos que se describen en este documento.

La Figura 9 ilustra un ejemplo de terminal inalámbrico 900 que puede utilizarse como uno cualquiera de los terminales inalámbricos (por ejemplo, el nodo transmisor, el nodo receptor,...), de los aspectos divulgados. El terminal inalámbrico 900 incluye un receptor 902 que incluye un decodificador 912, un transmisor 904 que incluye un codificador 914, un procesador 906 y 908 una memoria que están acoplados entre sí por un bus 910 sobre el cual los diversos elementos 902, 904, 906, 908 pueden intercambiar datos e información. Una antena 903 se utiliza para recibir señales desde una estación base y/o desde otros dispositivos acoplados al receptor 902. Una antena 905 utilizada para la transmisión de señales (por ejemplo, a la estación base y/o en otros terminales inalámbricos) está acoplada al transmisor 904.

El procesador 906 (por ejemplo, una CPU) controla el funcionamiento del terminal inalámbrico 900 e implementa procedimientos mediante la ejecución de rutinas 920 y el uso de datos/información 922 en la memoria 908. Los datos/información 922 incluyen datos de usuario 934, información de usuario 936 y la información de secuencia de asignación de información de subconjunto de tonos 950. Los datos de usuario 934 pueden incluir datos destinados a un nodo homólogo, que serán enviados al codificador 914 para codificarlos antes de su transmisión por el transmisor 904 a la estación base y/o a otros dispositivos, y los datos recibidos desde la estación base y/o en otros dispositivos, que han sido procesados por el decodificador 912 en el receptor 902. La información de usuario 936 incluye información del canal de enlace ascendente 938, información del canal de enlace descendente 940, información de ID del terminal 942, información de ID de la estación base 944, 946 información de ID de sector e información de modo 948. La información de canal de enlace ascendente 938 incluye información que identifica segmentos de canales de enlace ascendente que han sido asignados por la estación base al terminal inalámbrico 900 para usarlos cuando se transmite a la estación base. Los canales de enlace ascendente pueden incluir canales de tráfico de enlace ascendente, canales de control de enlace ascendente dedicados (por ejemplo, canales de solicitud, canales de control de potencia y canales de control de temporización). Cada canal de enlace ascendente incluye uno o más tonos lógicos, siguiendo cada tono lógico una secuencia de salto de tono de enlace ascendente. La secuencias de salto de enlace ascendente son diferentes entre cada tipo de sector de una célula y entre células adyacentes. El canal de información enlace descendente 940 incluye información que identifica segmentos de canal de enlace descendente que han sido asignados por la estación base para su uso cuando una estación base está transmitiendo datos/información al terminal inalámbrico 900. Los canales de enlace descendente pueden incluir canales de tráfico de enlace descendente y canales de asignación, incluyendo cada canal de enlace descendente uno o más tonos lógicos, siguiendo cada tono lógico una secuencia de salto de enlace descendente, que se sincroniza entre cada sector de la célula.

La información de usuario 936 también incluye información de identificación del terminal 942, que es una identificación de la estación base asignada, e información de identificación de la estación base 944 que identifica la estación base específica con la que el terminal inalámbrico 900 ha establecido comunicaciones, y el sector de la información de identificación 946 que identifica el sector específico de la celda en la que se encuentra actualmente el terminal inalámbrico 900. La identificación de la estación base 944 proporciona un valor de pendiente de célula y la información de identificación de sector 946 proporciona un tipo de índice de sector; el valor de la pendiente de célula y el tipo de índice de sector pueden utilizarse para derivar secuencias de salto de tono. La información de modo 948 también se incluye en la información de usuario 936 identifica si el terminal inalámbrico 900 está en modo de reposo, modo de espera o en modo encendido.

La información de secuencia de asignación de información de subconjunto de tonos 950 incluye información

temporal de símbolo-franja descendente 952 y la información de tono descendente 954. La información temporal de símbolo-franja descendente 952 incluye información de estructura de sincronización de trama, tales como super-ranura, ranura de baliza, información de estructura de ultra-ranura e la información que especifica si un período de símbolo dado es un periodo de símbolo-franja, y si es así, el índice del símbolo-franja, y si el símbolo-franja es un punto de reajuste para truncar la secuencia de asignación de subconjunto de tonos utilizada por la estación base. La información de tono de enlace descendente 954 incluye información que incluye una frecuencia de portadora asignada a la estación base, el número y frecuencia de los tonos y el conjunto de subconjuntos de tonos que deben asignarse a los periodos de símbolo-franja y otros valores específicos de las células y el sector como la pendiente, el índice de la pendiente y el tipo de sector.

Las rutinas 920 incluyen rutinas de comunicaciones 924, rutinas de control del terminal inalámbrico 926, y rutinas fundamentales de jerarquía 928. Las rutinas de comunicaciones 924 controlan los diversos protocolos de comunicaciones utilizados por el terminal inalámbrico 900. Por ejemplo, las rutinas de comunicaciones 924 pueden permitir la comunicación a través de una red de área amplia (por ejemplo, con la estación de base) y/o una red punto a punto de área local (por ejemplo, directamente con el(los) terminal(es) inalámbrico(s) dispar(es)). A modo de ejemplo adicional, las rutinas de comunicaciones 924 puede habilitar recibir una señal de emisión (por ejemplo, de la estación base). Las rutinas de control de terminal inalámbrico 926 controlan la funcionalidad básica del terminal inalámbrico 900 incluyendo el control del receptor 902 y el transmisor 904. Las rutinas de jerarquía de claves 928 de control de encriptación de claves dentro de una jerarquía. Las claves pueden ser una función de un primer identificador y un rango de validez. Las rutinas de jerarquía de claves 928 también puede controlar la obtención de claves de nivel inferior en una jerarquía de claves para determinar una clave actual que puede ser utilizada para descifrar un segundo identificador recibido para determinar un primer identificador situado en uno o más de sus homólogos.

Con referencia a La Figura 10, se ilustra un ejemplo de sistema 1000 para la transmisión de información de detección de homólogos. El sistema 1000 puede residir por lo menos parcialmente dentro de un nodo transmisor. Debe apreciarse que el sistema 1000 se representa como incluyendo bloques funcionales, que pueden ser bloques funcionales que representan funciones implementadas por un procesador, software o combinación de los mismos (por ejemplo, firmware).

El sistema 1000 incluye una agrupación lógica 1002 de componentes eléctricos que pueden actuar por separado o en conjunto. Por ejemplo, la agrupación lógica 1002 puede incluir un componente eléctrico 1004 para generar una multitud de claves asociadas con un primer identificador. Al menos una de las claves de la multitud de claves se asocia con un período de validez, una región geográfica o combinaciones de los mismos. Conforme a una ilustración, cada clave en la multitud de claves puede estar asociada con un período de validez diferente que tiene un punto de partida y un punto final. De acuerdo con algunos aspectos, la multitud de claves comprende una jerarquía.

El agrupamiento lógico 1002 también incluye un componente eléctrico 1006 para comunicar el primer identificador y por lo menos una de las claves de la multitud de claves. El primer identificador y las claves pueden ser transmitidos a al menos un nodo homólogo. De acuerdo con algunos aspectos, el primer identificador y las claves se comunican de forma segura. De acuerdo con algunos aspectos, el componente eléctrico 1006 comunica además el primer identificador y la al menos una segunda clave de la multitud de claves a un segundo nodo homólogo. De acuerdo con algunos aspectos, el primer identificador es un identificador público y el segundo identificador es un identificador privado. De acuerdo con otros aspectos, el primer identificador es un identificador privado y el segundo identificador es un identificador público. Además, de acuerdo con algunos aspectos, cada identificador puede tener un alcance limitado (por ejemplo, ni completamente público ni privado).

También se incluye en la agrupación lógica 1002 un componente eléctrico 1008 para derivar un segundo identificador. El segundo identificador puede derivarse como una función del primer identificador y las dos claves de la multitud de claves. También se incluye un componente eléctrico 1010 para anunciar el segundo identificador para una multitud de nodos homólogos. Anunciar el segundo identificador puede comprender una transmisión inalámbrica. Además, anunciar puede llevarse a cabo para descubrimiento de homólogos.

Además, el sistema 1000 puede incluir una memoria 1012 que retiene instrucciones para ejecutar funciones asociadas con los componentes eléctricos 1004, 1006, 1008, y 1010 u otros componentes. Aunque se muestra como externa a la memoria 1012, debe entenderse que uno o más de los componentes eléctricos, 1006, 1008, y 1010 pueden existir dentro de la memoria 1012.

Con referencia a La Figura 11, se ilustra un ejemplo de sistema 1100 que recibe la información de detección de homólogos. El sistema 1100 puede residir, al menos parcialmente, dentro de un dispositivo móvil o un nodo de recepción. Debe apreciarse que el sistema 1100 se representa incluyendo bloques funcionales, que pueden ser bloques funcionales que representan funciones implementadas por un procesador, software, o combinación de los mismos (por ejemplo, firmware).

El sistema 1100 incluye una agrupación lógica 1102 de componentes eléctricos que pueden actuar por separado o

en conjunto. El agrupamiento lógico 1102 puede incluir un componente eléctrico 1104 para recibir un primer identificador y la al menos una clave asociada con un nodo homólogo. La clave puede ser una clave temporal que tiene un período de validez que expira después de un cierto tiempo o por evento.

También se incluye un componente eléctrico 1106 para determinar un segundo identificador en base a, al menos en parte, el primer identificador y la al menos una clave. De acuerdo con algunos aspectos, el segundo identificador se determina en base a al menos en parte, el tiempo, en parte a la ubicación o combinaciones de los mismos. De acuerdo con algunos aspectos, determinar el segundo identificador puede incluir generar al menos una clave adicional. De acuerdo con algunos aspectos, la clave adicional se asocia con un período de validez específica, la región geográfica o combinaciones de los mismos. La al menos una clave adicional puede formar una jerarquía.

También se incluye en la agrupación lógica 1102 un componente eléctrico 1108 para monitorizar la recepción del segundo identificador. Monitorizar la recepción puede incluir recibir una transmisión inalámbrica. De acuerdo con algunos aspectos, el primer identificador es un identificador público y el segundo identificador es un identificador privado.

De acuerdo con algunos aspectos, la agrupación lógica 1102 puede incluir un componente eléctrico para recibir un identificador anunciado por un nodo cercano y un componente eléctrico para determinar si el identificador recibido es el segundo identificador determinado.

Además, el sistema 1100 incluye una memoria 1110 que retiene instrucciones para ejecutar funciones asociadas a los componentes eléctricos 1104, 1106, y 1108. Aunque se muestra como externa a la memoria 1110, debe entenderse que uno o más de los componentes eléctricos 1104, 1106, y 1108 pueden existir dentro de la memoria 1110.

Debe entenderse que los aspectos descritos en este documento pueden ser implementados mediante hardware, software, firmware o cualquier combinación de los mismos. Cuando se implementan en software, las funciones pueden ser almacenadas o transmitidas como una o más instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informático como medios de comunicación que incluyen cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Los medios de almacenamiento pueden ser cualquier medio disponible al que se puede acceder por un ordenador de propósito general o de propósito especial. A modo de ejemplo y no de limitación, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético o cualquier otro medio que se pueda utilizar para transportar o almacenar los medios de código de programa deseados en forma de instrucciones o estructuras de datos y al que se puede acceder mediante un ordenador de propósito general o de propósito especial o un procesador de propósito general o de propósito especial. Además, cualquier conexión se denomina correctamente medio legible por ordenador. Por ejemplo, si el programa se transmite desde un sitio web, servidor u otra fuente remota mediante un cable coaxial, cable de fibra óptica, par trenzado, línea de abonado digital (DSL) o tecnologías inalámbricas, tales como infrarrojos, radio y microondas, a continuación, el cable coaxial, el cable de fibra óptica, el par trenzado, DSL o tecnologías inalámbricas, tales como infrarrojos, radio y microondas están incluidos en la definición de medio. Disco (del inglés disk y disc), como se utilizan en la presente memoria, incluye disco compacto (CD), disco láser, disco óptico, disco versátil digital (DVD), disquete y disco “blu-ray” donde los discos (del inglés disk) generalmente reproducen datos magnéticamente, mientras que los discos (del inglés disc) reproducen datos ópticamente con láseres. También deben incluirse dentro del ámbito de los medios legibles por un ordenador combinaciones de lo anteriormente indicado.

Las diversas lógicas, bloques lógicos, módulos y circuitos ilustrativos descritos en conexión con los aspectos descritos en este documento pueden implementarse o realizarse con un procesador de propósito general, un procesador de señal digital (DSP), un circuito integrado de aplicación específica (ASIC), un matriz de puertas programable (FPGA) u otro dispositivo lógico programable, puerta discreta o lógica de transistor, componentes hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en este documento. Un procesador de propósito general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador convencional, controlador, micro-controlador, o máquina de estados. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores en conjunción con un núcleo DSP o cualquier otra configuración de ese tipo. Además, al menos un procesador puede comprender uno o más módulos operables para realizar una o más de las etapas y/o acciones descritas anteriormente.

Para una implementación software, las técnicas descritas en este documento pueden implementarse con módulos (por ejemplo, procedimientos, funciones, etcétera) que llevan a cabo las funciones descritas en el presente documento. Los códigos software pueden almacenarse en unidades de memoria y ser ejecutados por procesadores. La unidad de memoria puede implementarse dentro del procesador o externa al procesador, en cuyo caso puede acoplarse comunicativamente al procesador a través de diversos medios conocidos en la técnica. Además, al menos un procesador puede incluir uno o más módulos operables para llevar a cabo las funciones descritas en este

documento.

Las técnicas descritas en este documento pueden utilizarse para diversos sistemas de comunicación inalámbricos, tales como CDMA, TDMA, FDMA, OFDMA, SC-FDMA y otros sistemas. Los términos "sistema" y "red" se usan indistintamente. Un sistema CDMA puede implementar una tecnología radio tal como de Radio Terrestre Universal (UTRA), CDMA2000, etcétera. UTRA incluye CDMA de Banda Ancha (W-CDMA) y otras variantes del CDMA. Además, CDMA2000 cubre ES-2000, ES-95 y las normas IS-856. Un sistema TDMA puede implementar una tecnología radio tal como el Sistema Global para Comunicaciones Móviles (GSM). Un sistema OFDMA puede implementar una tecnología radio tal como UTRA Evolucionado (E-UTRA), Banda Ancha Ultramóvil (UMB), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM ®, etcétera. UTRA y E-UTRA son parte del Sistema Universal de Telecomunicaciones Móviles (UMTS). 3GPP Evolución a Largo Plazo (LTE) es un lanzamiento de UMTS que utiliza E-UTRA y que emplea OFDMA en el enlace descendente y SC-FDMA en el enlace ascendente. UTRA, E-UTRA, UMTS, LTE y GSM se describen en los documentos de una organización llamada "Proyecto de Asociación de 3ª Generación" (3GPP). Además, CDMA2000 y UMB se describen en los documentos de una organización llamada "Proyecto de Asociación de 3ª Generación 2" (3GPP2). Además, tales sistemas de comunicación inalámbrica pueden incluir adicionalmente sistemas de red punto a punto ad hoc (por ejemplo, de móvil a móvil) a menudo utilizando espectros sin licencia no balanceadas, 802.xx LAN inalámbrica, Bluetooth y otras técnicas de comunicación inalámbrica de corto o de largo alcance.

Por otra parte, diversos aspectos o características descritos en este documento pueden implementarse como un procedimiento, aparato o artículo de fabricación mediante programación estándar y/o técnicas de ingeniería. El término "artículo de fabricación", tal y como se usa en este documento, pretende abarcar un programa de ordenador accesible desde cualquier dispositivo legible por ordenador, portador o medios de comunicación. Por ejemplo, los medios legibles por ordenador pueden incluir pero no se limitan a dispositivos de almacenamiento magnético (por ejemplo, discos duro, disquetes, bandas magnéticas, etc.). Los discos ópticos (por ejemplo, discos compactos (CD), discos versátiles digitales (DVD), etc), tarjetas inteligentes y dispositivos de memoria flash (por ejemplo, EPROM, tarjetas, lápiz, unidad fundamental, etc.).Además, diversos medios de almacenamiento descritos en este documento pueden representar uno o más dispositivos y/u otros medios legibles por máquina para el almacenamiento de información. El término "medio legible por máquina" puede incluir, sin limitarse a, los canales inalámbricos y otros medios capaces de almacenar, contener y/o carga instrucción(es) y/o datos. Además, un producto de programa de ordenador puede incluir un medio legible por ordenador que tiene una o más instrucciones o códigos operables para hacer que un equipo lleve a cabo las funciones descritas en este documento.

Además, los pasos y/o acciones de un procedimiento o algoritmo descrito en conexión con los aspectos descritos en este documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo software puede residir en una memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, en registros, un disco duro, un disco extraíble, un CD-ROM o en cualquier otra forma de medio de almacenamiento conocida en la técnica. Un medio de almacenamiento de ejemplo puede estar acoplado al procesador, de tal manera que el procesador puede leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador. Además, en algunos aspectos, el procesador y el medio de almacenamiento pueden residir en un ASIC. Además, el ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario. Además, en algunos aspectos, las etapas y/o acciones de un procedimiento o algoritmo pueden residir como una o cualquier combinación o conjunto de códigos y/o instrucciones en un medio legible por máquina y/o medio legible por ordenador, que pueden ser incorporados en un producto de programa de ordenador.

Si bien la descripción anterior discute aspectos ilustrativos y/o aspectos, hay que señalar que pueden hacerse varios cambios y modificaciones en este documento sin apartarse del alcance de los aspectos descritos y/o aspectos tal como se definen mediante las reivindicaciones adjuntas. En consecuencia, los aspectos descritos están destinados a abarcar todas las alteraciones, modificaciones y variaciones que caen dentro del alcance de las reivindicaciones adjuntas. Además, aunque algunos elementos de los aspectos descritos y/o aspectos pueden describirse o reivindicarse en singular, se contempla el plural a menos que la limitación al singular se indique explícitamente. Además, la totalidad o una parte de cualquier aspecto y/o aspecto puede utilizarse con la totalidad o una parte de cualquier otro aspecto y/o aspecto, a menos que se indique lo contrario.

En la medida en que el término "incluye" se utiliza, ya sea en la descripción detallada o en las reivindicaciones, tal término pretende ser inclusivo de una manera similar a la expresión "que comprende", del modo en que "que comprende" se interpreta cuando se emplea como una palabra de transición en una reivindicación. Además, el término "o", tal y como se utiliza tanto en la descripción detallada como en las reivindicaciones está destinado a ser una " o no-exclusiva".

REIVINDICACIONES

1. Un procedimiento (700) para transmitir información de descubrimiento de homólogos, llevada a cabo por un primer nodo homólogo, que comprende:

generar (702) una pluralidad de claves asociadas con un primer identificador;

comunicar (704) el primer identificador y por lo menos una de las claves de la pluralidad de claves a un segundo nodo homólogo;

derivar (706) un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves; y

anunciar (708) el segundo identificador a una pluralidad de nodos homólogos.

2. El procedimiento según la reivindicación 1, en el que la al menos una clave de la pluralidad de claves se asocia con un período de validez, una región geográfica o combinaciones de los mismos.

3. El procedimiento según la reivindicación 1, en el que la pluralidad de claves comprende una jerarquía.

4. El procedimiento según la reivindicación 1, en el que el primer identificador y la al menos una clave son comunicadas de una manera segura.

5. El procedimiento según la reivindicación 1, que comprende además comunicar el primer identificador y al menos una segunda clave de la pluralidad de claves a un tercer nodo homólogo.

6. El procedimiento según la reivindicación 1, en el que el segundo identificador se deriva como una función del primer identificador y por lo menos dos claves de la pluralidad de claves.

7. El procedimiento según la reivindicación 1, en el que el primer identificador es un identificador público y el segundo identificador es un identificador privado.

8. Un aparato (1000) que reside dentro de un nodo transmisor (202, 302) para la transmisión de información de descubrimiento de homólogos, que comprende:

medios (206, 1004) para generar una pluralidad de claves asociadas con un primer identificador;

medios (208, 1006) para comunicar el primer identificador y por lo menos una clave de la pluralidad de claves a un primer nodo homólogo (204, 304);

medios (210, 1008) para derivar un segundo identificador como una función del primer identificador y la al menos una clave de la pluralidad de claves; y

medios (212, 1010) para anunciar el segundo identificador a una pluralidad de nodos homólogos.

9. Un procedimiento (800) para recibir información sobre el descubrimiento de homólogos, que comprende:

recibir (802) un primer identificador y al menos una clave asociada con un nodo homólogo;

determinar (804) un segundo identificador en base a, al menos en parte, el primer identificador y la al menos una clave;

monitorizar (806) la recepción del segundo identificador;

recibir un identificador anunciado por un nodo cercano; y

determinar si el identificador recibido es el segundo identificador determinado.

10. El procedimiento según la reivindicación 9, en el que el segundo identificador se determina en base al menos en parte al tiempo, en parte a la ubicación o combinaciones de los mismos.

11. El procedimiento según la reivindicación 9, en el que determinar el segundo identificador comprende generar al menos una clave adicional que está asociada con un período de validez específico, la región geográfica o combinaciones de los mismos.

12. El procedimiento según la reivindicación 11, en el que la al menos una clave adicional forma una jerarquía.

13. Un aparato (1100) que reside dentro de un nodo receptor (204, 304) para recibir información de descubrimiento de homólogos, que comprende:

medios (306, 1104) para recibir un primer identificador y al menos una clave asociada con un nodo homólogo;

medios (308, 1106) para determinar un segundo identificador en base a, al menos en parte, el primer identificador y la al menos una clave;

medios (310, 1108) para monitorizar la recepción del segundo identificador;

medios para recibir un identificador anunciado por un nodo cercano; y

medios para determinar si el identificador recibido es el segundo identificador determinado.

14. Un producto de programa informático, que comprende:

un medio legible por ordenador que comprende:

un código para hacer que al menos un ordenador lleve a cabo un procedimiento según una de las reivindicaciones 1 a 7 cuando se ejecuta.

15. Un producto de programa informático, que comprende:

un medio legible por ordenador que comprende:

un código para hacer que al menos un ordenador lleve a cabo un procedimiento según una de las reivindicaciones 9 a 12 cuando se ejecuta.

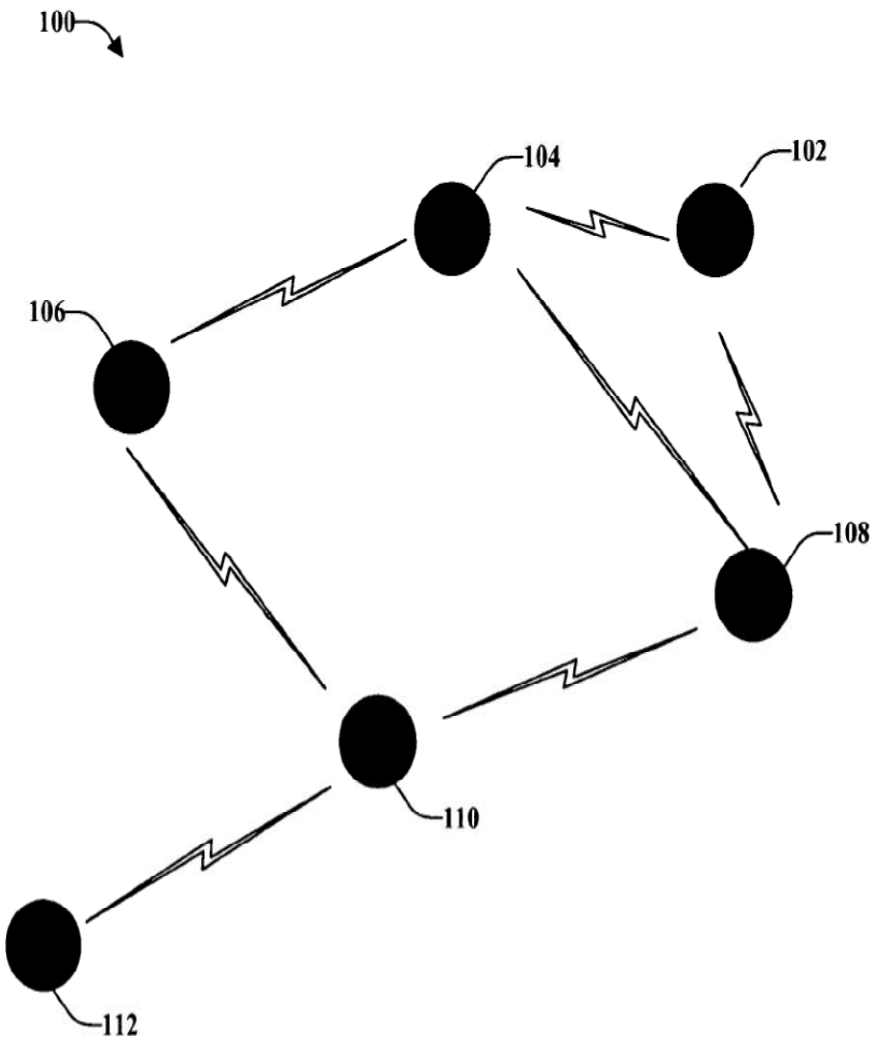

FIG. 1

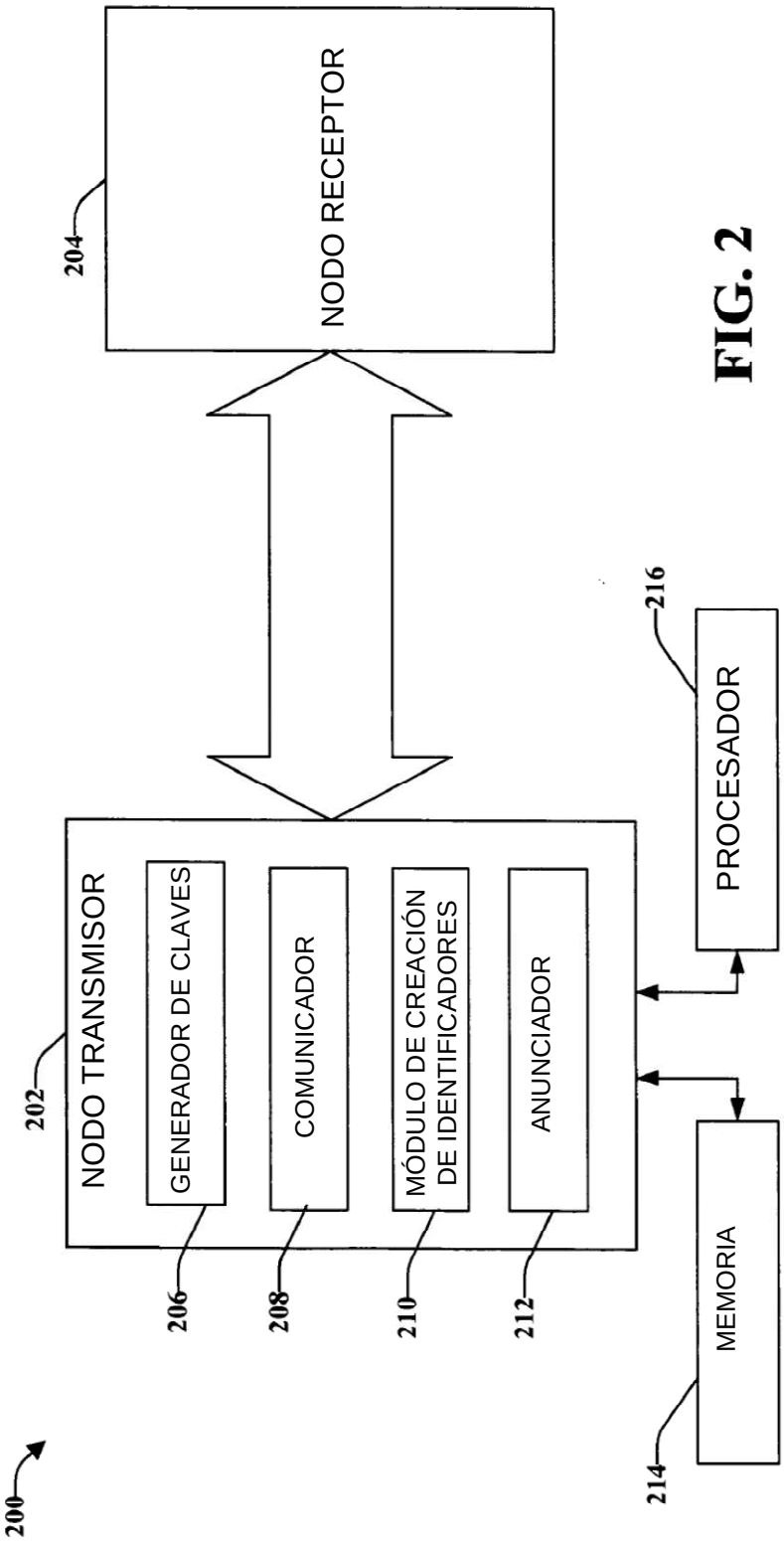
NODO RECEPTOR
204
NODO TRANSMISOR
202
GENERADOR DE CLAVES
COMUNICADOR
MÓDULO DE CREACIÓN DE IDENTIFICADORES
ANUNCIADOR
206
208
210
212
PROCESADOR
216
MEMORIA
214
200

FIG. 2

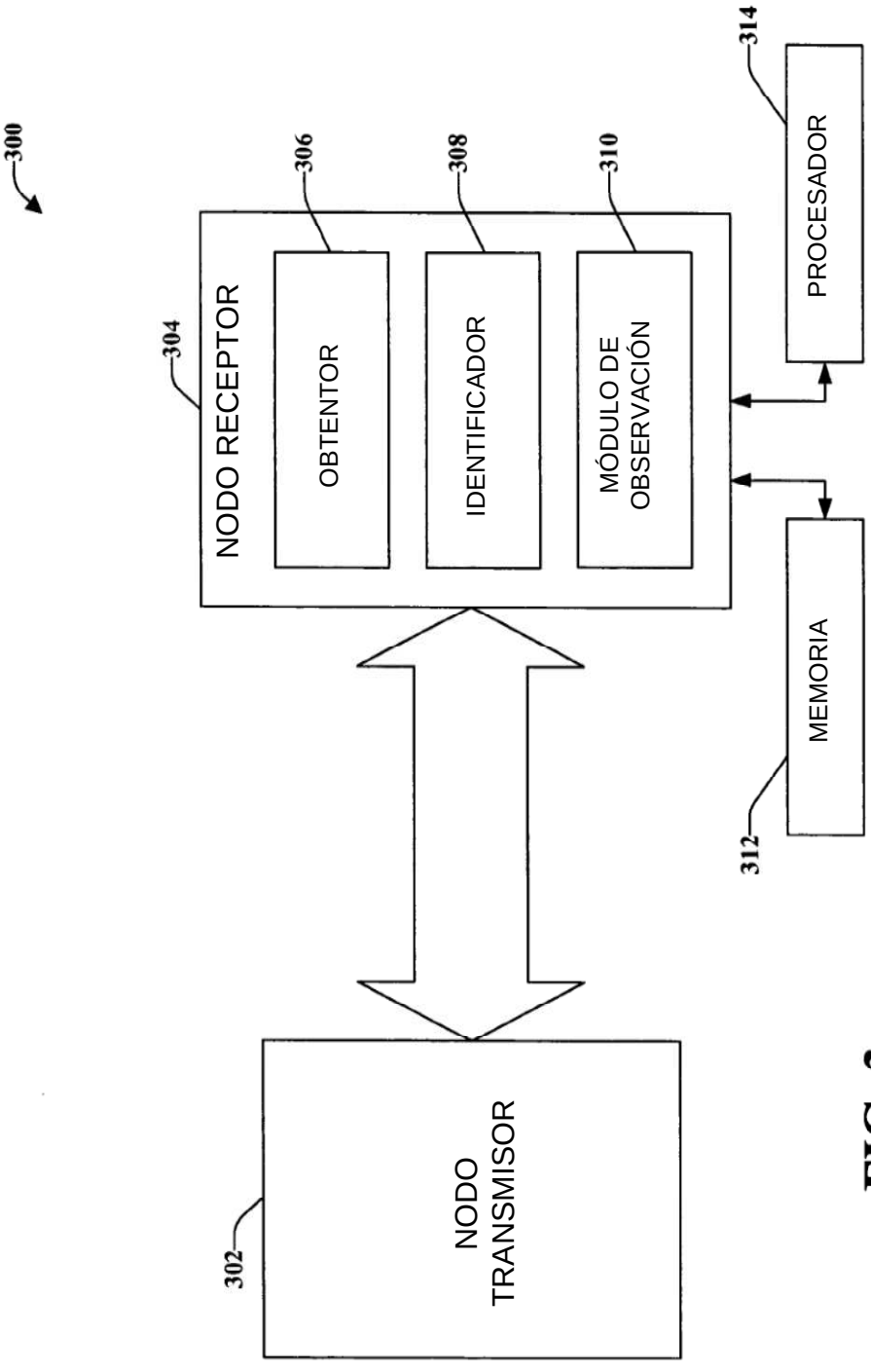
300
NODO RECEPTOR
304
OBTENTOR
306
IDENTIFICADOR
308
MÓDULO DE OBSERVACIÓN
310
PROCESADOR
314
MEMORIA
312
NODO TRANSMISOR
302

FIG. 3

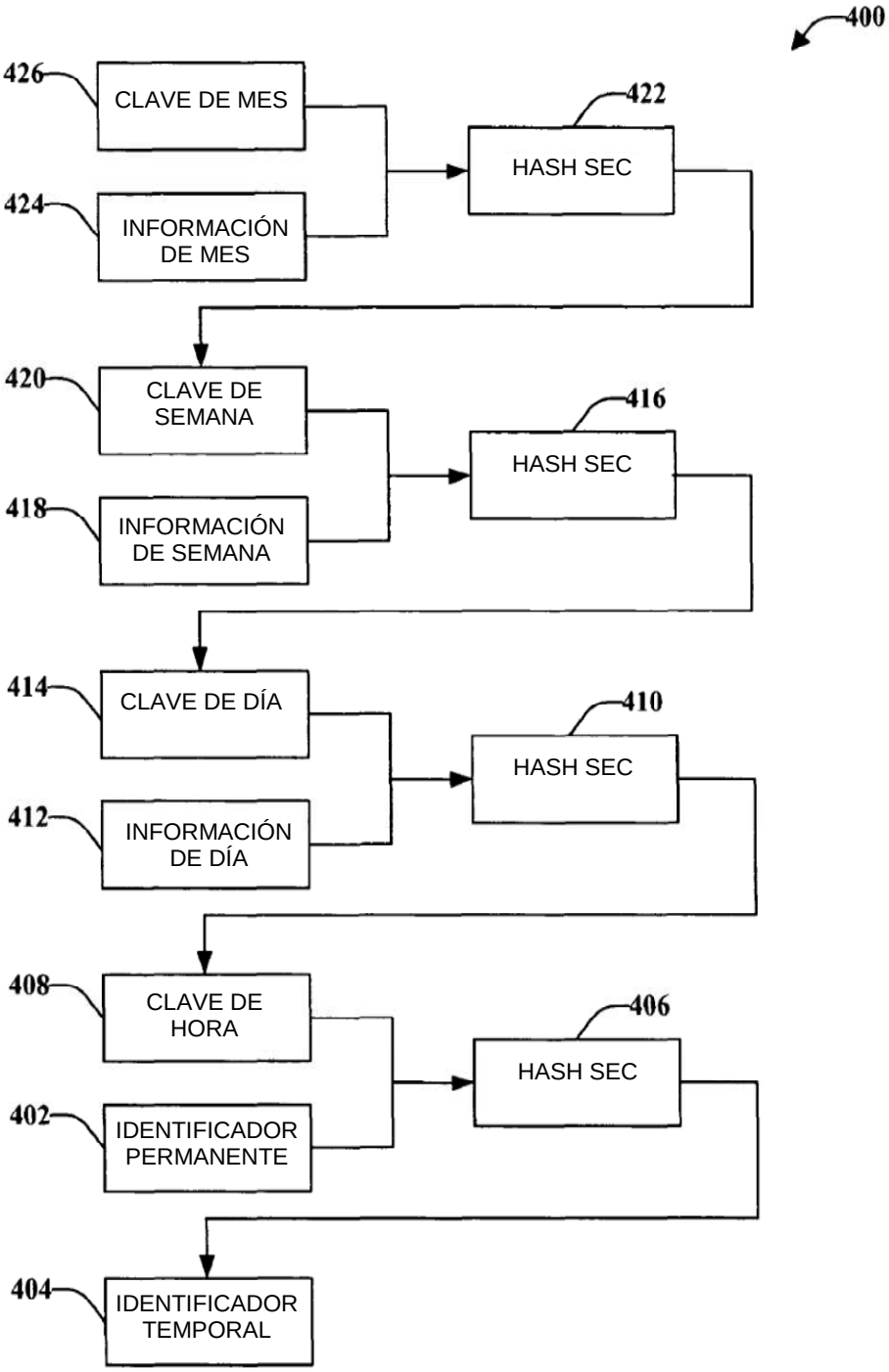
400
426
CLAVE DE MES
422
HASH SEC
424
INFORMACIÓN DE MES
420
CLAVE DE SEMANA
416
HASH SEC
418
INFORMACIÓN DE SEMANA
414
CLAVE DE DÍA
410
HASH SEC
412
INFORMACIÓN DE DÍA
408
CLAVE DE HORA
406
HASH SEC
402
IDENTIFICADOR PERMANENTE
404
IDENTIFICADOR TEMPORAL

FIG. 4

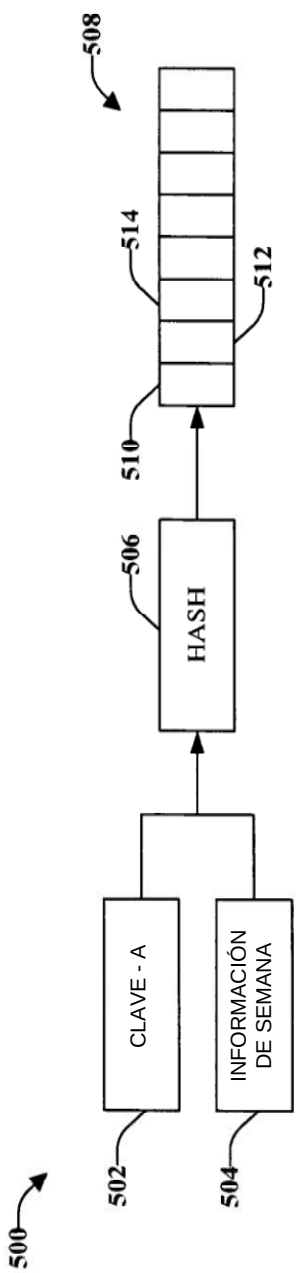
500
502
CLAVE - A
504
INFORMACIÓN DE SEMANA
506
HASH
508
510
512
514

FIG. 5

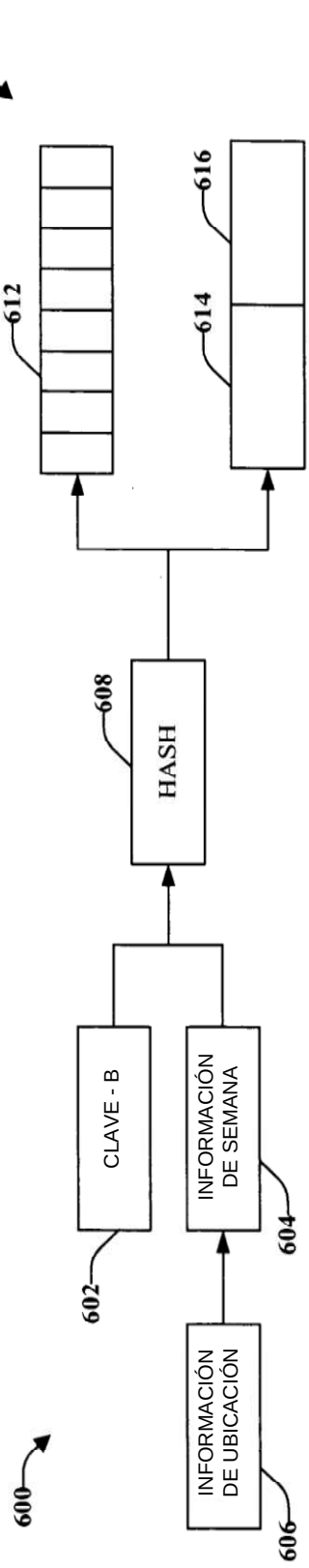
600
602
CLAVE - B
604
INFORMACIÓN DE SEMANA
606
INFORMACIÓN DE UBICACIÓN
608
HASH
610
612
614
616

FIG. 6

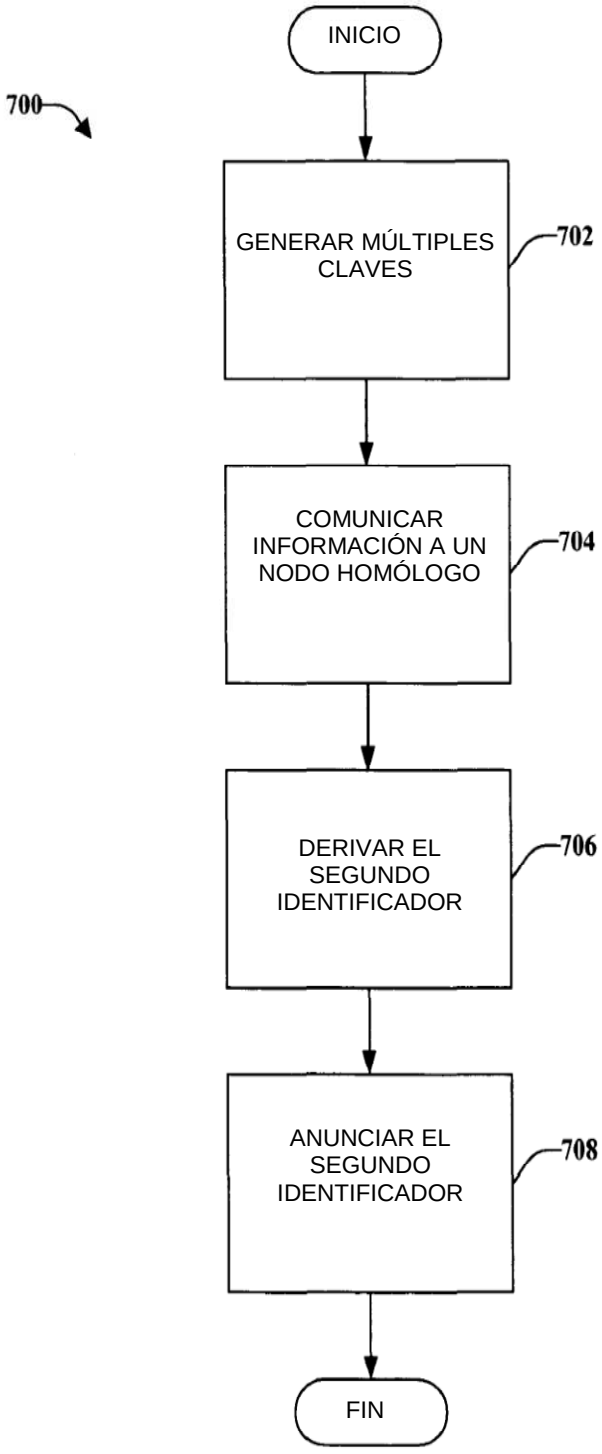
700
INICIO
GENERAR MÚLTIPLES CLAVES
702
COMUNICAR INFORMACIÓN A UN NODO HOMÓLOGO
704
DERIVAR EL SEGUNDO IDENTIFICADOR
706
ANUNCIAR EL SEGUNDO IDENTIFICADOR
708
FIN

FIG. 7

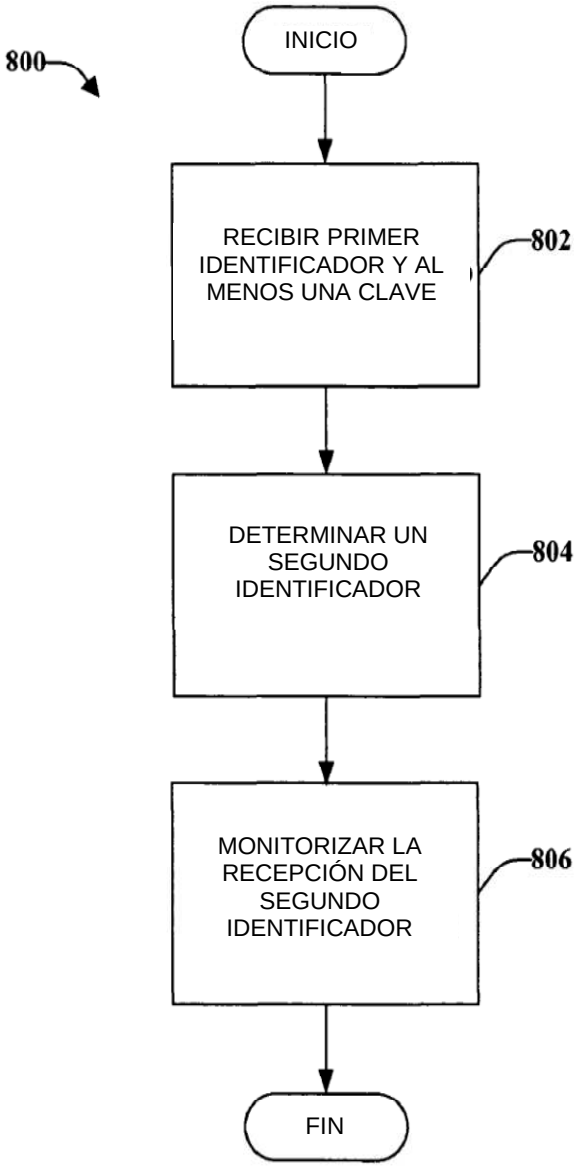
800
INICIO
RECIBIR PRIMER IDENTIFICADOR Y AL MENOS UNA CLAVE
802
DETERMINAR UN SEGUNDO IDENTIFICADOR
804
MONITORIZAR LA RECEPCIÓN DEL SEGUNDO IDENTIFICADOR
806
FIN

FIG. 8

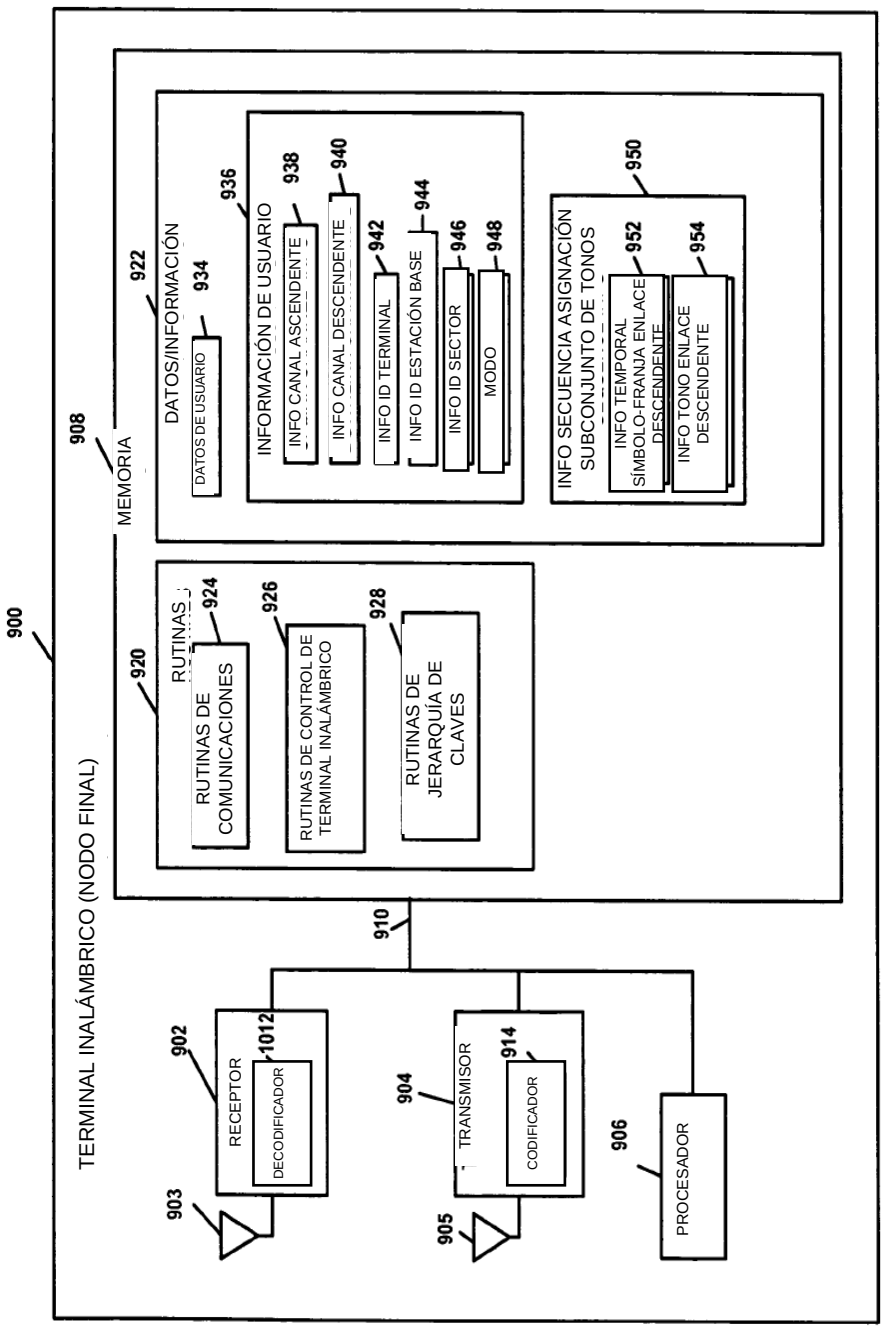
900
TERMINAL INALÁMBRICO (NODO FINAL)
908
MEMORIA
920
RUTINAS
924
RUTINAS DE COMUNICACIONES
926
RUTINAS DE CONTROL DE TERMINAL INALÁMBRICO
928
RUTINAS DE JERARQUÍA DE CLAVES
922
DATOS/INFORMACIÓN
934
DATOS DE USUARIO
936
INFORMACIÓN DE USUARIO
938
INFO CANAL ASCENDENTE
940
INFO CANAL DESCENDENTE
942
INFO ID TERMINAL
944
INFO ID ESTACIÓN BASE
946
INFO ID SECTOR
948
MODO
950
INFO SECUENCIA ASIGNACIÓN SUBCONJUNTO DE TONOS
952
INFO TEMPORAL SÍMBOLO-FRANJA ENLACE DESCENDENTE
954
INFO TONO ENLACE DESCENDENTE
910
902
RECEPTOR
1012
DECODIFICADOR
903
904
TRANSMISOR
914
CODIFICADOR
905
906
PROCESADOR

FIG. 9

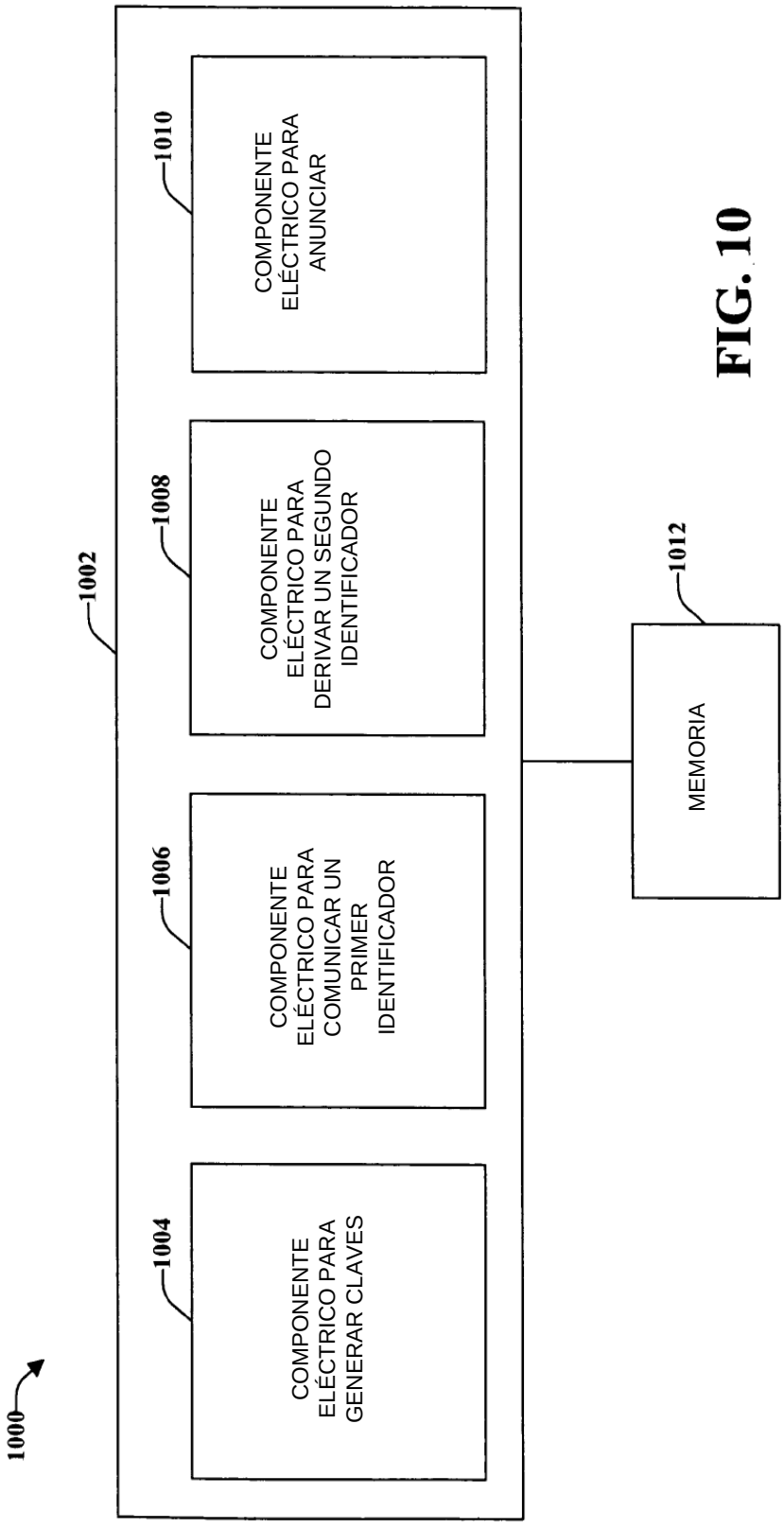
1000
1002
1004
COMPONENTE ELÉCTRICO PARA GENERAR CLAVES
1006
COMPONENTE ELÉCTRICO PARA COMUNICAR UN PRIMER IDENTIFICADOR
1008
COMPONENTE ELÉCTRICO PARA DERIVAR UN SEGUNDO IDENTIFICADOR
1010
COMPONENTE ELÉCTRICO PARA ANUNCIAR
1012
MEMORIA

FIG. 10

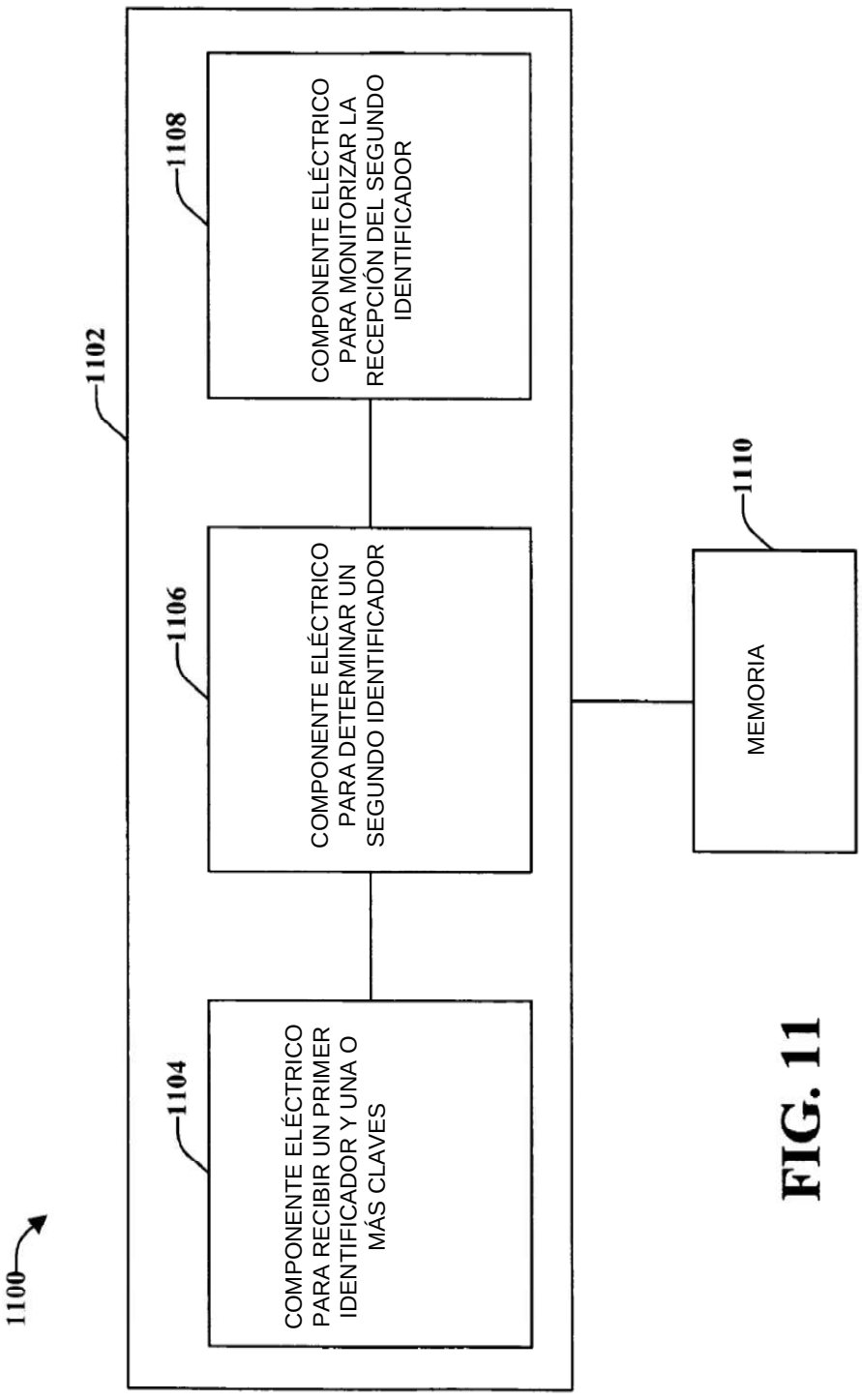
1100
1102
1104
COMPONENTE ELÉCTRICO PARA RECIBIR UN PRIMER IDENTIFICADOR Y UNA O MÁS CLAVES
1106
COMPONENTE ELÉCTRICO PARA DETERMINAR UN SEGUNDO IDENTIFICADOR
1108
COMPONENTE ELÉCTRICO PARA MONITORIZAR LA RECEPCIÓN DEL SEGUNDO IDENTIFICADOR
1110
MEMORIA

FIG. 11